# Digital Identity Roadmap Guide

# Digital Identity Roadmap Guide

**Acknowledgments**

This guide was developed by an international team of experts from a range of governmental institutions, international organizations and the private sector.

Special thanks go to the ITU and Deloitte teams who worked on this guide. In particular, from ITU, Hani Eskandar, Dorina Xhixho, Nancy Sundberg, Marco Obiso, Kemal Huseinovic and Sameer Sharma and from Deloitte, Alessandro Ortalda, Lorenzo Russo and Andrea Rigoni.

The authors would also like to thank all the experts who contributed to the development of the *Digital Identity Roadmap Guide*, including Ram Sewak Sharma (High Level Advisor), Deepti Vikas Dutt (India), Yahya Salim Rashid Al Azri (Oman), and Alphonce Malibiche (Tanzania).

**ISBN**

978-92-61-27821-2 (Paper version)
978-92-61-27831-1 (Electronic version)
978-92-61-27841-0 (ePub version)
978-92-61-27851-9 (Mobi version)

# Table of Contents

# List of Tables, Figures and Boxes

**Figures**

# Foreword

I am pleased to present the "Digital Identity Roadmap Guide" which sets out the principles, models and step-by-step recommendations to enable countries shift from paper based to digital identification systems for citizens. In today's highly connected digital environment, the ability to engage in online transactions increasingly relies on the reliability of online identity. Governments realize that delivering core services over the Internet cuts costs, streamlines efficiency, and provides valuable data for ongoing service optimization. Busy citizens, for their part, appreciate not having to make special trips to government offices to submit applications or make routine document requests. For the private sector, too, online interactions often make good business sense, allowing companies to better allocate resources where they are needed, maximizing revenues and improving overall customer experience.

Underpinning all of these benefits is the notion of trusted digital identity. Implementing a comprehensive National Digital Identity System can therefore represent a huge step forward in improving socio-economic inclusion combatting fraud and providing a solid platform for the growth of a huge range of online services, both public and private. But setting up such a system can be highly complex.

This invaluable guide presents the best of current thinking and experience in the area of National Digital Identity Frameworks, drawing on key studies, international regulatory expertise, real-world case studies and internationally-recognized technical and operational standards. It aim is to give leaders and policy makers a clear understanding of the process needed to establish a National Digital Identity Framework, outlining the choices to be made at each step; the benefits that can be leveraged through better management of public services; the potential for new partnerships with the private sector; the resource requirements for effective implementation, roll-out and maintenance; and the potential pitfalls that need to be avoided.

The guide is complemented by a comprehensive set of case studies from countries which have successful set up National Digital Identity Systems using a range of different approaches. The guide shows that there is no one-size-fits-all model; instead, governments can tailor their Digital Identity System to their own needs, ICT environment and future vision, drawing from a wide range of tested good practices.

As nations like India and Tanzania have shown, a Digital Identity System can serve as a major lever of socio-economic development. This unique guide will encourage governments around the world to consider the many benefits a Digital Identity System can bring and it will serve as an indispensable handbook for leaders and policy makers in successfully implementing such a system in their own national context.

**Brahima SANOU**
**Director, Telecommunication Development Bureau**

# Executive Summary

The *Digital Identity Roadmap Guide* is a comprehensive set of guidelines for identifying the main aspects that need to be addressed during the design, development and implementation of a National Digital Identity Framework. It is the result of a deeply collaborative multi-stakeholder effort aimed at strengthening the knowledge and expertise of professionals and policy makers working in the field digital identity and, more generally, the digitization of government services.

The value that can be derived from digital identity applications is potentially enormous and can represent a significant force in promoting a more inclusive and efficient national and transnational digital environment.

This guide introduces the main aspects to be considered by national leaders and policy makers in developing a National Digital Identity Framework, and should be considered a practical tool to guide stakeholders rather than an academic study on the topic of National Digital Identity Frameworks. It lists and describes the **overarching principles** that lay the foundations for designing, developing and implementing a National Digital Identity Framework. These principles encompass different areas ranging from economy to human rights, from operations to data protection. Each of these principles represents a fundamental part of the framework and requires careful consideration.

The guide also outlines four critical **Focus Areas**: *Governance models*, *Approaches for fostering adoption*, *Architectural models*, and *Sustainability models*. Each of these Focus Areas deals with a specific operational aspect of a National Digital Identity Framework. By building on standards, best practices and examples of implemented National Digital Identity Frameworks, this document aims to provide concrete guidance on the options available to national leaders and policy makers.

While the overarching principles and the Focus Areas will help national leaders and policy makers in designing a National Digital Identity Framework (ie., the main characteristics the framework will need to have, or need to satisfy), Section 5 illustrates a step-by-step approach that could be adopted in managing the National Digital Identity Framework throughout its entire lifecycle, from the planning phase through implementation and subsequent continuous improvement.

In order to ensure that the National Digital Identity Framework is implemented in an efficient way, the guide builds upon the experience of subject-matter experts, listing the ***main critical success factors*** that should be pursued to increase the chances of success, and the ***conflicting principles*** national leaders and policy makers should be aware of in making certain design decisions.

Lastly, the guide offers some important examples and successful case studies of National Digital Identity Frameworks, and provides a brief survey of the main technical standards available to date.

# Key messages

The Digital Identity Roadmap Guide helps leaders and policy makers identify the main aspects that need to be addressed during the design, development and implementation of a National Digital Identity Framework. A collaborative effort led by ITU, it draws on major studies by international organizations, government case studies, and world-class regulatory expertise.

- The guide identifies a set of **Overarching Principles** that need to be considered as part of initial steps to develop a national vision for a Digital Identity System. These include: a clear vision and mission statement at the outset of the project; a full audit of the national ICT landscape before decisions are made on the approach; the need to factor-in considerations related to economic and social inclusiveness and development; the need to preserve human rights in an online environment; system resilience, interoperability, sustainability, flexibility and scalability; issues of data quality; and trust, privacy and security issues.
- The guide specifies **four critical Focus Areas** that are the foundation stones of any National Digital Identity Strategy: Governance models; Approaches for fostering adoption; Architectural models; and Sustainability models. In each case, there are several models possible, and the guide makes it clear that the choices must be closely tailored to the unique national environment the National Digital Identity Framework is going to serve – there is no one-size-fits-all solution, nor a priori 'better' or 'worse' models for governance and architecture.
- The benefits of a Digital Identity System for **citizens** include: greater convenience and usability; reduced costs for government services; and improved citizen inclusion in government programmes.
- The benefits of a Digital Identity System for **governments** include: improved service delivery; reduced costs for staffing, document processing and storage; reductions in benefits 'leakage' through elimination of duplicate or fraudulent identities; better government planning through better data on the use of government services; and improved national security.
- The benefits of a Digital Identity System for the **private sector** include: new revenue opportunities through the possibility of collaborating with governments in service delivery; and reduced expenditure through centralized online service centres.
- The guide warns of **potential pitfalls** that governments need to carefully guard against when developing a National Digital Identity Framework, including: data security and privacy issues; system sustainability over the long term; and technical obsolescence.
- The guide identifies a number of **critical success factors** in the development, implementation and management of a National Digital Identity System. These include: strong professional project management skills; clearly defined organizational roles and responsibilities; strict quality management and certification; and a thorough review of the impact of a new Digital Identity System on existing legislation and regulations to identify areas which may require modification or harmonization.
- The guide includes set of country case studies spanning Canada, Estonia, India, Oman, Tanzania and the United Kingdom, which have each implemented their own country-specific – and often very different – National Digital Identity System.

# 1 Document Overview

## 1.1 Purpose

The purpose of this document is to guide governments in developing a National Digital Identity Framework, providing a comprehensive vision spanning the main elements, aspects and principles related to the notion of digital identity in a national context.

The overarching aim is to provide an understanding of the basic concepts of digital identity and how they apply in a national context. From this foundation, governments will have the competence to take concrete steps toward a wide range of initiatives in the field of digital identity, including a National Digital Identity Strategy, policies, laws and norms, technological implementation, and so on. Through such projects, governments can pursue social and economic advantages for both the private and public sectors and bring real benefits to their citizens.

This guide is a unique resource, providing a framework that benefits from a demonstrated and diverse experience of the topic and building on important prior works. As such, we believe it offers, to date, the most comprehensive overview of what constitutes successful digital identity implementation.

## 1.2 Scope

The concept of 'digital identity' represents an enormous and complex challenge that encompasses myriad aspects, touching upon governance, policy, operations, technology and law. A comprehensive understanding by national leaders and policy makers is thus essential before any effective national framework can be developed and implemented.

This guide focuses on the fundamental notions regarding digital identity to help leaders and policy makers correctly assess the national context and plan the necessary steps in developing and managing a National Digital Identity Framework.

At the same time, readers are advised that this document does not elaborate on single and specific technical aspects. The goal of this guide is not to provide a list of all available technological solutions; rather, it gives the reader the necessary theoretical tools that can be employed in designing a National Digital Identity Framework that is capable of responding to the principal and most pressing necessities all governments face.

A number of organizations have already addressed the topic of national digital identity. This guide is not intended as an alternative to these documents. Instead, it should be viewed as a companion tool to these studies, bringing additional clarity and filling the gaps that inevitably exist in such a vast and complex research area. For this reason, it is strongly recommended that leaders and policy makers read this guide in conjunction with materials that already exist; Section 8 lists some of the most prominent and well-recognized ones. However, in a field that is advancing at such a rapid pace, it will also be crucial to stay updated on the future innovations and advancements.

## 1.3 Overall Structure and usage of the guide

The content of this guide is organized as follows:

- Section 2: *Introduction* provides an overview of the subject of the guide with related definitions.
- Section 3: *Overarching principles for a National Digital Identity Framework* outlines the cross-cutting fundamental considerations to be taken into account during the development of a National Digital Identity Framework.
- Section 4: *Focus Areas* identifies the key elements and topics that should be considered during the development of a National Digital Identity Framework.
- Section 5: *Guidelines for development of a National Digital Identity Framework* details the steps required in the development of a National Digital Identity Framework during its full lifecycle.
- Section 6: *Critical success factors and conflicting principles* outlines the factors that can enhance the success of a National Digital Identity Framework and those that, conversely, have the potential to slow down the process and may necessitate decisions to exclude certain conflicting aspects in favour of others.
- Section 7: *Country Case Studies*
- Section 8: *Conclusions* provides a summary of some of the main points touched upon throughout the document.
- Appendix 1: *Standards* provides some detail on existing standardization work which has already been done in this area.
- Appendix 2: *References* provides further pointers to relevant literature that stakeholders can review.

In particular, sections 3, 4 and 5 address the principles and models for a National Digital Identity Framework, while Section 6 addresses the guidelines for the development of a National Digital Identity Framework.

## 1.4 Target Audience

This primary audience for this guide comprises policy makers responsible for developing a National Digital Identity Framework. The secondary audience constitutes all the other public and private stakeholders that might be involved in the development and implementation of a National Digital Identity Framework, such as government offices, regulatory authorities, law enforcement agencies, ICT providers, critical infrastructure operators, civil society, academia and research institutions.

We hope this guide will also prove valuable for other stakeholders, such as the international development community, which often provides assistance in National Digital Identity Framework implementation.

# 2 Introduction


## 2.1 What is a Digital identity

***Definition of Digital identity***

The International Telecommunication Union defines the concept of identity as a 'representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context'[1]. Building on this definition, we might state that a *digital* identity is the digital representation of an entity detailed enough to make the individual distinguishable within a digital context.

Identity is a crucial element for every individual as it defines *who* the individual is and identifies the main traits of each and every person. Digital identity is equally important, retaining the intrinsic characteristics that make identity such a defining factor and, at the same time, serving as an enabler for governments in achieving social inclusion, digital transformation, improvement in quality of services and so forth.

Given the primary importance digital identity can have in a national context, national leaders and policy makers should consider implementing a specific framework – a National Digital Identity Framework – which comprises all the elements necessary to operate a Digital Identity System and deliver its services to the population.

**Elements of Digital identity**

As stated above, an entity is represented through one or more 'attributes'. Strictly speaking, an attribute can be defined as a 'specific data item pertaining to an individual'[2]. These attributes can

[1] International Telecommunication Union – Telecommunication Standardization Sector, *X.1252 "Baseline identity management terms and definitions",* April 2010.

[2] International Telecommunication Union – Telecommunication Standardization Sector – Focus Group on Financial Services, *Identity and Authentication,* January 2017.

be considered the building blocks of a digital identity: they can be divided into categories such as birth-related information (name, place of birth, date of birth, etc), descriptive information (height, weight, physical traits etc), personal identifiers (eg. social security number), biometric data (fingerprint, DNA, iris scan, etc) and so on.

***Categorisation of Digital identity***

Although the concept of digital identity identifies a specific object (as defined above), we can define three main categories that can help isolate specific traits:

- A **foundational** digital identity is 'usually created as part of a national identity scheme or similar, which is based on the formal establishment of identity through the examination of qualifying ('breeder') documents such as birth records, marriage certificates, and social security documents'[3].
- A **functional** digital identity is 'created to address the specific needs of an individual sector'[4] (for instance, the healthcare or transportation sectors).
- A **transactional** digital identity is 'intended to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors'[5].

These three categories can aid our understanding of the different ways digital identities might be seen and employed by different frameworks.

## 2.2 Potential benefits and pitfalls of a National Digital Identity framework

***Potential benefits for the users***

A successfully implemented National Digital Identity Framework can open up a wide range of benefits for a state and its citizens.

- ***Improving convenience and user experience***

  *Digital* identity can effectively remove some of the barriers that make public services complex and hard to access for users, increasing both convenience and the user experience in general. Having a digital identity means users do not have to be physically present to gain access to many services, while online service delivery means users can benefit from 24/7 service availability.

  *Another* important benefit derives from the fact that users do not need to remember different usernames and passwords for each of the services they employ. This simple but critical factor exponentially simplifies authentication processes, which in turn increases the popularity of a Digital Identity System for users.

- ***Reducing cost of access to services***

  Thanks to greater convenience and flexibility, users can cut the indirect costs of accessing services. For instance, working citizens need no longer take days off work to complete bureaucratic procedures in person, and digital processing greatly reduces the amount of paper documentation required.

- ***Improving citizen inclusion***

  Thanks to digital identities, people who might not be able to obtain identity documents will be able to participate fully in their communities despite a lack of physical documentation. This

[3] Ibid.
[4] Ibid.
[5] Ibid.

means they will be able to perform important economic and social actions, such as opening a bank[6] account, getting a mobile phone connection or obtaining social security benefits.

Adopting a National Digital Identity Framework can effectively promote a new paradigm that supersedes traditional approaches based on physical identity documents.

***Potential benefits for the public sector***

- ***Improving service delivery***

  A fully functioning system of digital identity means governments can deliver services to their citizens more efficiently, helping institutions target the population with welfare and social programmes, giving governments the necessary tools to reach the least accessible and most remote areas, and ensuring that the entire community benefits and grows together. A National Digital Identity Framework can therefore deliver real improvements in the condition of society at large.

  Governments and public administration will also benefit from a reduction in leakages due to duplicates and 'ghosts' in beneficiary databases, further increasing cost-effectiveness and efficiency.

- ***Reducing the cost of service delivery***

  Thanks to Digital Identity Systems, the public sector can cut the cost of providing services to citizens[7], freeing up government resources. In addition to reducing the amount of paper documents needing to be processed and stored, Digital Identity Systems improve productivity and reduce staff costs through fewer in-person services (with no loss of service quality).

- ***Improving security***

  Digital identity can also increase the level of national security. Digital identity can serve as a powerful tool for policing and crime prosecution, and can greatly increase the effectiveness of combating certain specific crimes (such as identity fraud, tax fraud, etc).

***Potential benefits for the private sector***

- ***New revenue opportunities***

  By leveraging the digital environment created by the Digital Identity System both the public and private sectors have the potential to develop innovative revenue streams[8], kick-starting a virtuous cycle that helps the whole economy thrive and grow.

- ***Reducing the cost of service delivery***

  Private companies and entities providing services through a National Digital Identity System are also likely to benefit from a decrease in their delivery costs. Reducing personnel, physical delivery points, paperwork and the time needed to complete each user's request are just a few of the examples of measures companies can adopt to lower expenditure.

---

6 It has been demonstrated that digitalization of financial services can greatly improve their adoption, providing huge benefits. This is particularly true for poor and unbanked consumers. For more information, please refer to International Telecommunication Union, Telecommunication Standardization Sector, Focus Group on Financial Services, *Main Recommendations*, March 2017

7 This topic has been thoroughly investigated by a Group of Experts working under the purview of the Word Bank. Please refer to *Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints*, World Bank, 2018.

8 Regarding opportunities for the private sector please refer to *Private Sector Economic Impacts from Identification Systems*, World Bank, 2018.

***Potential pitfalls***

While National Digital Identity Frameworks have the potential to bring many benefits, it is important to remember that certain pitfalls can be incurred when they are not adequately designed and implemented. Some of the most critical are:

- Security and privacy: the vast amount of data required exposes the system to a number of threats from the digital world, such as hacking and data breaches.
- Sustainability: because it is a costly undertaking, a National Digital Identity Framework might easily fail if adequate resources are not planned in advance.
- Obsolescence: the initiative of building a National Digital Identity Framework will fail if the framework is not adequately future-proofed against technical obsolescence.

The next sections of this guide deal with the most important of these aspects.

# 3 Overarching Principles

This section presents cross-cutting principles, which, taken together, can help in the development of a forward-looking and holistic National Digital Identity Framework. These principles should be considered in all steps of the National Digital Identity Framework development process.

The order of these principles reflects a logical narrative, rather than an order of importance.

## 3.1 Vision and Mission

***Any entity interested in developing a National Digital Identity Framework should precisely define a vision setting out the goals it aims to pursue, and a mission detailing how to reach these goals.***

In establishing a National Digital Identity Framework, a crucial success factor will be the setting out of a clear vision. This helps all stakeholders understand what is at stake and why the National Digital Identity Framework is needed (context), what is to be accomplished (objectives), as well as what it encompasses and whom it impacts (scope).

The clearer the vision, the easier it will be for national leaders and key stakeholders to ensure a more comprehensive, consistent and coherent approach. A clear vision also facilitates coordination, co-operation and implementation of the National Digital Identity Framework among involved parties. It should be formulated at a sufficiently high level and take account of the dynamic nature of the digital environment.

The vision should be complemented by an accurate mission statement. This statement provides useful information about how the government plans to pursue the changes set out in the vision. The mission statement should not be excessively detailed, but rather a broad strategy overview to ensure the flexibility required at the planning and designing phases.

## 3.2 Comprehensiveness

***The National Digital Identity Framework should result from an all-encompassing understanding and analysis of the overall digital environment, taking into consideration the country's context, circumstances and priorities.***

Managing digital identities is not only a technical challenge; it is a complex multi-faceted activity with wide ramifications for many diverse areas, such as economic development, social prosperity, law enforcement, national security, etc.

Given the broad spectrum of ramifications, it is important to understand how these might interrelate, potentially complementing or competing with each other. Based on this understanding and an analysis of the government's specific context, priorities can then be defined in line with the overall vision adopted for the National Digital Identity Framework. Priorities will allow for the setting-up of specific objectives and timelines and the allocation of necessary resources.

The priorities included in a National Digital Identity Framework will necessarily vary from country to country.

## 3.3 Social Inclusiveness

***A National Digital Identity Framework should be developed in a way that its services can be provided to the entire community of users, with particular regard for vulnerable individuals and minority groups.***

The digital environment has become an essential platform for government, business and society at large. The latter comprises a variegated set of sub-groups with very different characteristics and peculiarities. Certain of these sub-groups might be identified as particularly vulnerable or in need of protection: the elderly, minority communities and low-income families are just few examples.

A National Digital Identity Framework should be designed so that all the members of the community can benefit from its services without excluding less-advantaged individuals (who might, for instance, have lower digital literacy or less access to digital devices), and without providing grounds for any kind of discrimination.

The importance of inclusiveness is recognized by other pivotal works on digital identity. According to the World Bank, the 'identification systems should strive for continuous universal coverage from birth to death, free from discrimination and accessible to all individuals'[1].

## 3.4 Economic and Social Prosperity

***A National Digital Identity Framework should foster economic and social prosperity and maximize the contribution of the digital environment to sustainable development and social inclusiveness.***

The development of a National Digital Identity Framework will bring social and economic benefits for both the public and the private sectors.

Robust identification systems with widespread coverage can provide a number of benefits for the public sector, including reducing fraud and leakage in transfer programmes, increasing administrative efficiency, increasing tax collection, and providing additional sources of revenue.

The role of Digital Identity Systems in the private sector is equally important. The efficient, accurate and secure use of personal identity data is at the heart of most transactions, regardless of the industry

[1] World Bank, *Principles on identification for sustainable development: toward the digital age,* February 2018

in which they take place. The implementation of robust and inclusive identification systems at the national level therefore offers the potential for large financial gains for private sector companies.

Digital identity can thus generate many benefits, but it can also exacerbate the risk of isolation for poorly-connected populations including rural and remote communities, the forcibly displaced, stateless persons and other marginalized groups. Levelling the playing field requires a coordinated, sustained effort by stakeholders involved in the provision and use of Digital Identity Systems. A shared vision through a National Digital Identity Framework can contribute to robust and universal identification systems that in turn promote social and economic inclusion and sustainable development outcomes.

## 3.5 Fundamental human rights

***A National Digital Identity Framework should respect and be consistent with fundamental human rights and values.***

A National Digital Identity Framework should recognize the fact that the rights people enjoy in the physical world must also be directly translated and protected in the digital environment. The Framework should respect universally agreed fundamental rights, including, but not limited to, those found in the United Nations Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, as well as relevant multilateral or regional legal frameworks.

Attention should be paid to freedom of expression, privacy of communications, and personal data protection. In particular, the National Digital Identity Framework should avoid facilitating the practice of arbitrary, unjustified or otherwise unlawful surveillance, interception of communications and unauthorized processing of personal data.

In balancing the needs of the state with those of the individual, the Framework should ensure that, where applicable, surveillance, interception of communications, and collection of data is conducted within the context of a specific investigation or legal case, authorized by the appropriate national authority, and pursued on the basis of a public, precise, comprehensive and non-discriminatory legal framework enabling effective oversight, procedural safeguards and remedies.

Ensuring people's rights are respected in the digital environment is crucial to ensuring that trust is established and maintained between governments and citizens. Respecting fundamental human rights and promoting their protection in every aspect of government activities reinforces the idea that institutions exist to safeguard the population, creating a trust relationship that will ultimately promote quicker and more effective adoption of digital identity by citizens.

## 3.6 Resilience

***A National Digital Identity Framework should enable an efficient risk management approach and ensure an appropriate level of resilience.***

While a National Digital Identity System entails a great number of advantages and benefits for a state and its citizens, there are many associated risks, especially in an environment as fluid and complex as cyberspace, where the 'threat landscape' is in continuous evolution. These risks can be of an economic and financial nature, but also relate to the particular sensitivity of the processed data if we consider, for example, the health sector.

For this reason, a National Digital Identity Framework should be designed in a proactive manner, should focus on a resilience-oriented approach, and should be aimed at limiting the risks that may originate from identity data management.

## 3.7 Trust, privacy and Security

***A National Digital Identity Framework should ensure adequate safeguards for the privacy of users and guarantee an appropriate level of information security in order to gain a high level of trust among users and stakeholders.***

A National Digital Identity Framework should define clear and effective privacy and data protection regulatory measures. The whole process of data collection, integration and management should be underpinned by legal frameworks and procedures that clearly specify the treatment of different sets of data and under which conditions, ensuring that users retain adequate control over their personal information. The Framework should also include robust security measures to guarantee data protection.

These aspects are vital to building trust among users; without that trust, the framework is bound to fail. This is all the more important considering the prominence privacy and data security are currently enjoying in public debate[2].

Adequate and effective governance, especially regarding privacy, security and respect for human rights in general, has the power to enable situations in which governments can foster an increased level of trust among their citizens. As the World Bank correctly states, the governance of 'identification systems must be built on a legal and operational foundation of trust and accountability between government agencies, international organizations, private sector actors and individuals. People must be assured of the privacy and protection of their data, the ability to exercise control and oversight over its use, and processes for independent oversight and the redress of grievances'[3].

Furthermore, opportunities provided by robust and inclusive systems may extend beyond a strictly economic dimension. Generally, well-run and transparent identification systems that protect privacy while offering clear benefits increase trust in the government overall, with a variety of benefits. For example, a trusted identification system may reduce the likelihood that election results are disputed, thereby decreasing the risk of post-election violence and its associated human and financial costs.

## 3.8 Sustainability and cost optimisation

***The National Digital Identity Framework should be developed keeping into consideration the economic sustainability of the system.***

As public and private service providers increasingly transition into the digital realm, the ability for individuals to prove who they are will be essential for accessing benefits and services via digital platforms. This move toward digital platforms can increase efficiency of service delivery and create significant savings for citizens, governments, and businesses by reducing transaction costs, as well as drive innovation.

Obviously enough, the system requires certain costs to be operated and managed. Therefore, it is important for States to assess and anticipate such costs, so that the generated benefits can be directed to ensure the sustainability of the system on the long term.

## 3.9 Flexibility and scalability

***A National Digital Identity Framework should be operated in a flexible and scalable manner and must be able to be promptly and efficiently modified or updated when necessary.***

---

[2] The topic of trust in digital systems, with a specific focus on digital identity, is thoroughly explained in International Telecommunication Union, *Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security,* ITU 2018.

[3] World Bank, *Principles on identification for sustainable development: toward the digital age,* February 2018

The need for flexibility and scalability is important for many reasons. The number of governments with National Digital Identity Frameworks will increase over time, while the population coverage within a single country will, initially at least, be progressive, especially in case of countries with large populations. At the same time, the conditions of application and use of digital identity will necessarily evolve, driven by technological evolution and social progress.

For these reasons, a National Digital Identity Framework should provide a high degree of flexibility so that it can be updated and modified over time, as well as adapted to very different contexts, while maintaining common and shared guidelines.

## 3.10 Interoperability

***A National Digital Identity Framework should take into account the role of interoperability to ensure the ability of different systems to exchange information and queries.***

Interoperability between identification systems with sufficient coverage and robustness can reduce or eliminate some redundant aspects of the identity ecosystem, avoiding duplicate data collection and eliminating obsolete databases or credentials.

Moreover, a high level of interoperability contributes to lowering operating costs within a government's identity ecosystem, since an identification system with sufficient population coverage and interoperability can centralize functions and replace a number of previously disparate systems.

## 3.11 Speed of deployment

***The implementation and deployment of a National Digital Identity Framework should follow a swift roll-out schedule.***

A National Digital Identity Framework should be quickly and steadily deployed across the entire area/perimeter that the framework has to cover. This is of the utmost importance in order to guarantee an adequate and universal application of digital identity, underpinning the overall effectiveness of the services associated with it.

## 3.12 Identity as a platform

***A National Digital Identity Framework should foster the development of digital ID as a platform, so that users can plug it into any domain and use it.***

Whenever possible, a National Digital Identity Framework should be of a foundational nature. A foundational approach ensures that digital identity is not just an asset or an attribute of a citizen – which opens the possibility of employing the digital identity environment as a platform for aggregating a variety of different and interrelated services, greatly improving the speed of adoption.

This can also lead to savings when governments are able to create a foundational identification system with enough coverage and interoperability or integration to eliminate duplicative functional systems. Using foundational registers and credentials to underpin voter lists, for example, reduces the cost of voter registration and/or eliminates the need for separate voter ID cards; in the same way, a foundational unique identity linked with the tax database can help improve taxpayer identification, potentially broadening the tax base and improving compliance.

## 3.13 Uniqueness of IDs

***A National Digital Identity Framework should ensure that people are able to get only one digital identity.***

Robust identification systems must not only be able to establish the existence of individuals in a given jurisdiction, but also their uniqueness (noting that the ability of individuals to prove who they are will be essential for accessing benefits and services via digital platforms as public and private Service Providers increasingly transition into the digital realm).

Unique identifiers – which uniquely identify a person or entity within a given population – are therefore needed. An identifier is unique if no two individuals in the system share the same value of the identifier. Although this will be different according to the means of identification employed, uniqueness of ID should be pursued and ensured (ie. users should not be able to register in the system multiple times or under multiple names), thus avoiding duplication and 'ghost' users.

The creation of a unique identifier for each individual within the population can increase transaction efficiency and is essential to minimizing opportunities for fraud.

## 3.14 Robustness and future-proofing technology

***The technologies and systems described in the National Digital Identity Framework and used for the creation of digital identities should be robust, scalable and future-proof.***

The level of robustness in the identification system is a crucial condition for savings and revenue generation. Robustness refers to the accuracy, integrity, and security of system assets and processes. Savings and revenue potential is limited where systems are non-robust, and maximized when systems are statistically error free and highly resistant to fraud or theft. Interoperability between databases with inaccurate records will be less useful for identifying ineligible beneficiaries than databases that are relatively complete and error free. Similarly, if digital authentication procedures rely on ID cards with weak security features or identity records that were not thoroughly proofed, the system may be more vulnerable to identity theft and impersonation.

In parallel, systems development planning and the technologies adopted need to stand the test of time and not be prone to obsolescence, in order to assure the continuity of the entire process.

## 3.15 Data quality

***A National Digital Identity Framework should serve as the base for other programmes of national importance; it is thus critical that steps are taken to ensure data quality at multiple levels.***

Data quality and accuracy are first of all assured by establishing a unique identifier – a unique ID number – via biometric deduplication or another method, so that Identity Providers can directly reduce administrative errors and increase the efficiency of identity records management over time and across different agencies using the identifier. When integrated into other systems, unique IDs can help deduplicate data records, serve as the key for communication and queries across databases, and provide a credential for secure verification and authentication procedures. They therefore help facilitate integration and interoperability, and typically strengthen the robustness of digital authentication processes and services.

# 4 National Digital Identity Framework Focus Areas

Digital identity affects many areas of socio-economic development and is influenced by several factors within the national context. This section introduces the elements that will ensure appropriate levels of comprehensiveness and effectiveness of a National Digital Identity Framework, while allowing for a tailor-made design to fit each system's unique national environment.

These *good practices* are grouped into four distinct focus areas (governance, adoption approaches, architectural models and sustainability), representing the overarching themes of a National Digital Identity Framework. While both the Focus Areas and the elements they comprise have been put forward here as examples, it is particularly important that the latter are viewed in their own national context, as some may not be relevant to another country's specific situation. Countries should identify the models that support their own objectives and priorities in line with their vision.

It is also important to stress that the order of the individual Focus Areas and/or elements below should not be seen as indicating a level of importance or priority.

## 4.1 Focus Area 1 – Governance Model

This Focus Area introduces good practice elements to be considered when addressing the governance of a National Digital Identity Framework.

Essentially, three different models can be adopted:

**1)** The government is directly involved as Identity Provider

**2)** The government only acts as Regulator and is not involved as Identity Provider

**3)** The government acts as Regulator and Identity Broker, Clearing House

Selecting a specific model is a choice that cannot be made upon predefined criteria. Analysis of existing digital identity frameworks shows that several factors are usually considered, however it is not possible to define a specific rule. For instance, in some cases governments have leveraged initiatives associated with the issuing of identity cards – combining this with the issuing of a digital identity. Others have adopted options that leverage third parties capable of bringing in millions of already-verified and active identities or capable of managing digital identities thanks to their prior experience and capabilities.

This section focuses solely on the role of government, regardless of the number of other stakeholders involved (eg. the number of Service Providers).

***The Government is directly involved as Identity Provider***

The governmental approach to digital identity can be either 'buy' or 'make'. Both approaches offer a secure and convenient digital identity to citizens. This section explores the scenario usually defined as 'make'.

In this scenario the government has a primary role in the National Digital Identity Framework, acting as Regulator and Identity Provider at the same time. On one hand, its role as Regulator implies providing guidance and control on the National Digital Identity Framework, producing specific laws, regulations, criteria, conditions, procedures, and controls for the management of digital identities. On the other hand, acting as an Identity Provider requires a direct responsibility in terms of operation of the digital identity lifecycle, from identity proofing to credential management, authentication of identities, integration with Service Providers, and revocation of digital identities.

This option has both benefits and disadvantages. While the government might be able to leverage certain advantageous factors such as a local presence throughout the territory, other programmes/initiatives already in place (for example, a national identity card programme), and more direct control over the whole system, it also holds true that this approach does not take advantage of the considerable experience in managing digital identities gained over the years by third parties such as telco operators or banks, or the ability to deploy systems in a rapid manner leveraging experience, capabilities, and even user base.

Estonia is one of the great success stories in the adoption of this model. The system introduced by the government in 2002 currently has coverage close to 98% for a total population of 1.3 million[1]. It is based on the use of an electronic ID card, which is used as a comprehensive proof of identity in a digital and physical context. There are currently countless uses, both in the public and private sectors: for instance, the card can be employed as proof of identity when accessing bank accounts, to apply digital signatures, and to access public administration services (eg. access to medical records, taxation records, etc).

Other prominent examples of this approach are India and Tanzania. In India, through its *Aadhaar* programme, the government acts as Identity Provider. In less than five and a half years the government has amassed 1.2 billion digital identities. In these cases, since digital identity is provided directly by the government, it is regarded as a reliable and trusted digital identity for everyday use across multiple governmental services and other service sectors such as banking and telecoms.

It is important to point out that the option to act as Identity Provider in the National Digital Identity Framework does not completely exclude any kind of private sector involvement, allowing governments to take advantage of the experience and capabilities of system integrators as identity management providers. A government can develop and implement the system by itself, or, more commonly, can engage third parties for deployment of the technical solutions, maintaining *de facto* its Identity Provider role.

[1] Source https://e-estonia.com/solutions/e-identity/id-card/

This governance model is very commonly associated with a foundational Digital Identity System, as the government (or an authorized third party) operates and manages a central repository that effectively constitutes the main registry of citizens.

***The Government only acts as Regulator and is not involved as Identity Provider***

This section explores the scenario in which the government acts as Regulator of the National Digital Identity Framework and buyer of digital identity provision services. The model implies that other entities are engaged in managing the digital identities of citizens. This model is commonly referred as the 'buy' model, since it requires subsidies from the government to remunerate third parties for costs sustained and services offered.

In this scenario the government has, on one hand, the role of regulating and controlling the National Digital Identity Framework, issuing laws, regulations, criteria, conditions, procedures, and controls for the management of digital identities and for accrediting the entities that act as Identity Providers. These activities require specific attention as, in order to distribute its services, the government requires a high level of identity proofing – indeed, usually the highest, ie. 'proofing in person'. This requirement is due to the level of assurance governments must guarantee in accordance with international and national laws and regulations, ensuring identity proofing conforms to the same strict criteria that applies to the issuance of physical identity documents (for example, a national passport).

Leveraging a service provided by third parties, in particular with regard to accessing public digital services, requires subsidies from the government aimed at compensating the third parties involved for the service provided (eg. proofing of identities on behalf of the government, managing of credentials, etc) and related costs (personnel, facilities, technologies, etc). Mostly the third parties involved are private operators with proven expertise and capability in the field.

The Canadian government's initiative is one of the success stories in the adoption of this model. Named *SecureKey Concierge*, the initiative saw the creation of a system consisting of an Identity Broker and a set of Identity Providers. These were selected among entities which had a considerable number of identities already verified with a high level of assurance, and which were already equipped with digital authentication solutions (eg. banks).

Canada's goal was to provide a method of identification and authentication – an alternative to the one already offered by the government – to access public services, based on a 'bring your own credentials' (BYOC) model where users are enabled to use credentials they already have and use in other contexts.

The government signed a contract with an Identity Broker, SecureKey, a consortium comprising some of Canada's largest banks (at the system's inception there were three; at time of writing there are five) which have already verified the identities of their customers and provided them with a tested and secure means of authentication.

Often, when the government is not directly involved as Identity Provider, the system takes the shape of a multiple Identity Provider system. In this scenario, identities are usually collected to satisfy the specific needs of each Identity Provider. No single centralized registry is created, and the system can be considered as functional, rather than foundational.

***The Government acts as Regulator and Identity Broker/Clearing House***

This section explores the scenario in which the government acts as regulator of the National Digital Identity Framework and as a digital Identity Broker/Clearing House. This model is very similar to the previous one but adds an active role for government in the management of the relations and the economic relationship between citizens, Identity Providers and Service Providers. This has been simplified through the creation of an Identity Broker as an intermediary between Service Providers and Identity Providers. The advantages of this model are:

- The ability to simplify the integration of Service Providers with multiple Identity Providers.

- The guarantee of greater privacy for users. Service Providers do not trace the Identity Providers to users, and vice versa.

The English initiative, *GOV.UK Verify*, part of the larger *Identity Assurance Program*, is one of the success stories in the adoption of this model. In 2012, five Identity Providers were selected through a European tender. The selection was repeated in 2015, extending the maximum number of operators to ten, for a duration of three years with an option for a further year. Currently the number of Identity Providers is eight. This model requires that the government make use of and repay digital Identity Providers, which in turn allow citizens access to the digital services of the public administration. Access to public services is intermediated by the government acting as Identity Broker, facilitating communication between Service Providers and Identity Providers by placing itself in the middle.

## 4.2 Focus Area 2 – Approaches for fostering adoption

The success of a National Digital Identity Framework is gauged by the level of adoption among relevant stakeholders. The term *level of adoption* refers generically to multiple objectives: the percentage of citizens who have a digital identity; the number of public and private services able to offer services through the use of digital identity; and the number of accesses to digital services.

To achieve the challenging goal of universal or near-universal adoption, it is crucial to address the needs and expectations of the two primary entities involved in any Digital Identity System: users (citizens) and Service Providers. The system is a *de facto* classic example of a two-sided market where the needs and demands of these two entities are completely different and antagonistic. Users demand a wide, secure and simple use of digital identities on as many services as possible. Service Providers, conversely, require as large a user base as possible. Being able to successfully manage these different needs creates a virtuous circle, where more demand from one group stimulates demand from the other.

The next sections describe the most important elements to be considered in fostering/promoting the participation of citizens and Service Providers.

***Approaches for fostering adoption citizen-side***

*Value of digital identity for users*

One of the most critical drivers for citizens' adoption is the real value in terms of public and private services that can be accessed with a digital identity. Even if a sizeable percentage of users has an issued digital identity, the success of the initiative will be measured by the services that can be accessed by citizens and the number of accesses completed.

For this reason, governments should consider proactively promoting participation in the system by the many different public service departments so that real value can be provided to citizens. A nation's public administration should be capable of offering secure, easy, and convenient access to a series of public services with a unique digital identity such as, but not limited to:

- Demographic services
- Health services
- Welfare services
- Taxation services
- Pension services.

Access to this range of services through a unique digital identity can represent a key driver of citizen adoption. At the same time, extending the range accessible services to include private sector services can further increase citizens' interest in using digital identity. Estonia, for example, allows the use of digital identities for a huge number of providers, both public and private.

Governments should define a comprehensive strategy and roadmap for Service Provider involvement, and align this to the vision that underlies the National Digital Identity Framework. The outcome, represented by a Service Catalogue, needs to be defined in advance and be constantly updated.

A different strategy sees the government compelling the user to adopt a digital identity as a mandatory means of accessing digital public services. This approach has the potential to provide a major boost to adoption. In Oman, for example, the Omani Information Technology Authority has achieved extensive adoption, leveraging the mandate of the highest authority, the Ministers' Cabinet, which requires access to digital public services through the National Digital Identity Framework. The same approach has been adopted in Tanzania, where adoption has been encouraged thanks to a policy that has made it mandatory to access a series of public services via digital identity such as:

- Obtaining a Tanzanian Passport
- Opening or registering a new company.

*Convenient enrolment process*

Citizens have to be able to complete the digital identity enrolment process in a convenient way, through a system that limits the complexity and effort required. One decisive aspect is the level of identity proofing required. Identity proofing is the method used to certify user authenticity prior to providing the credentials necessary to access digital services. Identity proofing has four different Levels of Assurance (LoA), commonly identified through international standard ISO/IEC DIS 29115 as:

- LoA1 (Low Proofing) – Self-asserted
- LoA2 (Medium Proofing) – Proof of identity through use of identity information from an authoritative source
- LoA3 (High Proofing) – Proof of identity through use of identity information from an authoritative source + verification with the authoritative source
- LoA4 (Vey High Proofing)- Proofing in person in addition to LoA3 requirements.

Government initiatives generally require a very high level of identity proofing – usually LoA4, 'proofing in person'. This requirement is due to the level of assurance that governments have to guarantee in accordance with international and national laws and regulations, corresponding to the same proofing level as the issuance of government-certified physical identity documents such as national passports. High levels of identity proofing, however, require more controls and, often, the need to visit a government office or authorized agency. For this reason two main aspects need to be defined in advance:

- Level of identity proofing requested
- Process and technicalities for proofing.

With respect to the process and technicalities for proofing, there are different approaches to the identification adopted as 'in-person identification' versus 'remote identification'. In the first case, government-authorized entities (eg. public officials) verify the identity of the citizen *de-visu*. This approach offers a greater level of assurance, but entails certain complexities for citizens and Identity Providers alike. Citizens have to physically go to an office, and the Identity Provider has to set-up multiple offices to complete the identity proofing. The second case – remote identification – is commonly associated with the notion of an inherently lower level of assurance. There are a number of solutions and technologies that can be deployed to safeguard the level of assurance for remote identification (eg. facial recognition, video anti-tampering), even though there is as-yet no consensus among experts on the comparison in terms of assurance between the two approaches. That said, remote identification is clearly considerably more efficient than in-person identification.

*Issuing of digital identity: voluntary vs mandatory*

Another driver of adoption is related to the voluntary or mandatory nature of having a digital identity. This represents a determining element – perhaps not the most decisive among those that can decide the success or otherwise of an initiative, but certainly among those that can foster adoption.

Essentially, two different approaches can be adopted for the issuing of digital identities: voluntary-based or mandatory-based:

- **Voluntary-based**:the decision whether or not to have a digital identity is left to citizens themselves. In this scenario, citizens need to be encouraged to request a digital identity because it represents their key to accessing a series of valuable services. India, through its Aadhaar programme, has adopted this approach. Citizens are not forced to hold an Aadhaar-issued digital identity, however, they must own one in order to participate in certain specific, national or governmental welfare or social programmes (for example, social benefits).
- **Mandatory-based**: this approach does not allow the citizen to decide whether or not to request a digital identity. It is usually adopted in combination with initiatives where the enrolment of a digital identity is created in parallel with another ID document, such as a physical ID card. Forms of mandatory possession of digital identity become decisive for promoting adoption, but they do not guarantee use of that identity if it is not combined with an extensive service offering. Estonia has established a system that provides state-issued digital identities to almost the entirety of its citizenry (current figures stand at around 98% adoption). Citizens can access a broad suite of services, such as e-government, healthcare, security and safety, business and finance, and educational services.

  While this method has been extremely successful for Estonia, it can be challenging for countries which do not already have a national ID card or which would find it challenging (politically, logistically) to manage the two identities – digital and physical – together.

*Levering other digital identities systems*

In many cases, citizens already have digital identities that they routinely use – for example, to access banking services, telecommunications providers, energy suppliers, and so on. To obtain and use these identities they have already been verified and own authentication tools that they regularly use. Banks and telco operators in particular manage identities that require higher levels of trust – often equivalent to that required by governments – due to the type of service offering (mortgages, loans, etc.) or due to sector-specific compliance laws (for example, anti-money laundering or SIM registration). For this reason, governments wishing to do so can partner with private entities to allow citizens access to government services via their familiar online sign-in process, leveraging an identity already verified.

Such an approach can yield multiple benefits:

- Governments leverage a significant number of already verified active users
- User convenience is enhanced as the risk of forgetting credentials is minimized. Citizens typically don’t access government services online on a daily basis – yet we know that users forget passwords for sites they don’t visit regularly. Conversely, banking, telecommunications or other private services are often accessed very regularly. Leveraging the same digital identity reduces the overhead of re-verifying lost credentials and simplifies the number of credentials users have to manage.
- Governments reduce the effort and costs related to credential management.

The Canadian government's initiative – already presented in the previous section – is a unique collaboration between the private and the public sector. By letting customers use a single set of credentials for banking and government access, the Canadian government helps citizens maintain fewer higher-quality passwords than before, simplifying the customer experience. The government is willing to involve other entities for authentication services that it can't provide, simply because users visit

its sites too rarely. In addition, trusted private sector entities could provide new services based on credential management.

*Usability*

A National Digital Identity Framework should aim at achieving the highest level of usability possible. A system that users find complex to operate will have far less chance of garnering the full participation of a country's citizenry.

To make a National Digital Identity Framework effective, the design of its processes, components and systems should take into account the principles of simplicity and immediacy of access. No advanced skills should be required of users and an adequate level of support should be provided to guide adopters. This is particularly important for people who might not be familiar with the digital environment, such as people with a low level of digital literacy, the elderly, or persons with disabilities.

Extending the concept to interoperability, users see value in identity recognition across multiple platforms and / or domains without the burden of having to enter more credentials or use multiple authentication tools.

*Security and privacy*

Citizens demand simple, convenient and secure use of their digital identity. Protection of that identity from abuse, compromise and fraud through certified solutions and services with proven reliability is a crucial driver of adoption. At the same time, guaranteeing transparency in terms of data processing is an important goal.

Security is a complex, multi-faceted aspect that touches upon many different elements. Defining specific security-related and privacy-based objectives at the very start of any digital identity programme will ensure that security and privacy considerations are integrated across the entire digital ecosystem.

Governments should adopt specific actions aimed at ensuring that citizens and Service Providers benefit from the maximum achievable level of security. There are multiple security risks related to different phases of a digital identity lifecycle which need to be thoroughly analyzed through an accurate threat profile, starting from core processes such as:

- Identity proofing and enrolment of digital identity
- Use of digital identity.

Because multiple stakeholders are involved – citizens, Identity Providers, Service Providers, Identity Brokers, etc. – national leaders and policy makers should adopt a security-by-design approach, which ensures the Digital Identity System is adequately secured against both external attacks and internal abuses. The consequences of a security breach can have a very destructive impact on stakeholders' level of trust in the system.

Another crucial element having a direct impact on the level of trust accorded to any Digital Identity System is the safeguards protecting user privacy. The recent introduction of norms such as the European Union General Data Protection Regulation[2] reveals the high degree of attention this issue is attracting from legislators and society in general.

Since the use of services that rely on digital identity entails the sharing of a certain amount of personal data, sometimes of a very sensitive nature (such as biometric data), national leaders and policy makers should make every effort to reassure users that privacy is respected and protected at each

[2] See *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

step of the process. This can be achieved through a sound legal and regulatory framework and, more generally, by complying with the privacy-by-default principle.

There are different ways of ensuring that data privacy is adequately managed and maintained. Each of these approaches entails potential benefits and disadvantages that need to be carefully considered. Canada, for instance, adopted a specific approach based on the adoption of an Identity Broker. In the Canadian Digital Identity System, *SecureKey Concierge* acts as an intermediary, connecting credential subscribers to credential providers (in this case, Canadian banks). The service is triple-blind to protect privacy: users can be confident that banks cannot see what they are doing online; the government cannot see users' banking details; and the *SecureKey Concierge* service is not aware of users' identities.

Promoting an open and transparent approach about how data are processed, stored, deleted and shared, and about the rights users have in relation to the management of their personal data, is therefore critical to the success of a National Digital Identity System.

Generally speaking, there are a number of safeguards that can be adopted to ensure a higher level of both data protection and data privacy:

- Information is stored securely
- Information is shared with third party only when strictly necessary
- Information is managed transparently, with clear communication about how it is used and shared
- The Identity Provider does not have access to or knowledge about the services the user is adopting.
- The government does not have access to or knowledge of the Identity Provider the user decided to adopt (applicable only when multiple Identity Providers are present).
- All Identity Providers and Service Providers have to meet government and international standards for security and data protection.

*Communication and citizen awareness*

Governments need to constantly promote the digital identity initiative and its benefits to their citizens, taking into account the needs and concerns of different target audiences when designing an overall communication strategy. Suffice to say that this is an often overlooked element that, when not correctly managed, can gravely impair the success of the initiative.

***Approach for fostering adoption service providers-side***

*Promoting or mandating public administration participation*

The success of a National Digital Identity Framework is measured by the number and extent of services that citizens can access, both public and private. Government action should aim at involving public and private digital Service Providers, according to their Digital Identity Strategy and related objectives.

Actions to involve various public service departments in digital identity adoption can be facilitated by government's role as Regulator for specific sectors. Governments can either make participation mandatory for certain departmental services, or actively promote the benefits of using new digital identity services over traditional services.

Governments might decide to request that certain digital public services be exclusively accessed via digital identities. This requires Service Providers to employ the identity management system used by the government at the national level. What might appear to be a simple operation at first glance, however, requires careful designing of the Digital Identity Systems employed. The design will need to focus on integration and interoperability, taking into account technical and other standards that can facilitate this. It will also require meticulous planning in terms of deployment, in the light of the central

role played by the identity system. Examples of success stories here include Oman and Tanzania, where the state provides public services that can be accessed only by users who have a digital identity.

Other countries have adopted different approaches where there are no services that can *only* be accessed via digital identity, with traditional identity systems offered in parallel. Even if Service Providers' participation in the identity system is mandated by the government, this approach usually slows citizen adoption.

*Engaging with private sector operators*

Service providers play a crucial role in the success of a National Digital Identity Framework. Extending the service offering to the private sector can be a compelling driver for accelerating citizen adoption. Since private providers will decide on their participation in the system based on a cost-benefit analysis, a crucial part of facilitating the participation of private Service Providers in the National Digital Identity Framework will be to provide real advantages and / or cost reductions.

As already stated, a National Digital Identity Framework encompasses high levels of identity proofing (ie. in-person verification) to the benefit of public Service Providers. As highlighted in Figure 1, private Service Providers have different requirements in terms of levels of identity proofing. Consequently, the price they are willing to pay for identity services is different from that of government departments. Simple e-commerce operators do not have the same needs (eg. self-declared identity for payments for which a credit card is appropriate) as banks and financial or telecoms operators, which have more critical transactions (eg. opening accounts, requests for mortgages or loans) and compliance obligations (for instance, anti-money laundering or SIM registration). While this certainly holds true for entities with highly polarized needs (eg. online commerce vs banks), it is also true that each private entity will prefer a specific identity proofing approach according to its specific business model (see Figure 1).

Figure 1 – Comparison of two options for identity proofing

| | Option 1 - Private Operators Leveraging Highly Trusted Identity | Option 2 - Private Operators Leveraging "Self Asserted" Identity |
|---|---|---|
| **Identity Proofing Level** | High | Low |
| **Authentication recom.** | Strong and Weak Authentication | Weak Authentication |
| **Identification of the Target Market Segments** | Banking, Insurance, Telecommunications, Public services and Health care | Media and Web 2.0 Communication |
| | Traditional production (Automot.), Retail, E-commerce, Online info / entertaimt., Utilities, Transport. | |
| | **Private sector operators that requires identities with high level of proofing as enabling factor for their business value proposition.** | **Private sector operators that leverages a "Self Asserted" identity as enabling factor for a better customer insight or completing micro payments** |

Several drivers should be considered in any cost-benefit analysis:

- Contribution to value:
  - Leverage a larger user base faster
  - Improve the user experience: users can access new services more quickly and with less effort because they can share trusted information that has already been vetted (eg. single sign-on One Click to Purchase)
  - Take advantage of additional services such as payments, logistics and shipping services that can be offered by Identity Providers
  - Customize user experience through qualifying attributes
  - Enhance focus on core offering, eliminating the need for involvement in non-core services.

- Cost reduction:
  - Reduce costs associated with identification proofing processes
  - Reduce costs associated with credential management
  - Reduce costs for starting and managing new services.

*Introducing an Identity Broker*

The majority of initiatives with multiple Identity Providers envisage the implementation of an Identity Broker. The Identity Broker is an intermediary that connects Identity Providers and Service Providers, providing further protection for privacy and working as a clearing house for costs and revenues among participants.

This element is a key facilitator, especially when there are multiple Identity Providers that need to be integrated with multiple Service Providers. This is even more crucial when small and medium public or private providers are willing to be engaged.

The primary benefits of introducing an Identity Broker are:

- Identity Providers and Service Providers only have to define and sign a single agreement with the Broker/s, instead of bilateral agreements with all the entities involved. Moreover the Identity Broker can act as a clearing house, logging the transactions or use of identity and the proceeds with the invoices to Service Providers and the payment of Identity Providers.
- Easy technical integration with just one entity – the Identity Broker – reducing effort and time.
- Extended privacy assurance through the triple-blind mechanism. Service Providers can forward the authentication request to the Identity Broker, unaware of which Identity Provider the user is signed-in on; Identity Providers see the request coming from the Identity Broker but are not informed as to which Service Provider the user is accessing; and, finally, the Identity Broker is not aware of the identity of the user.

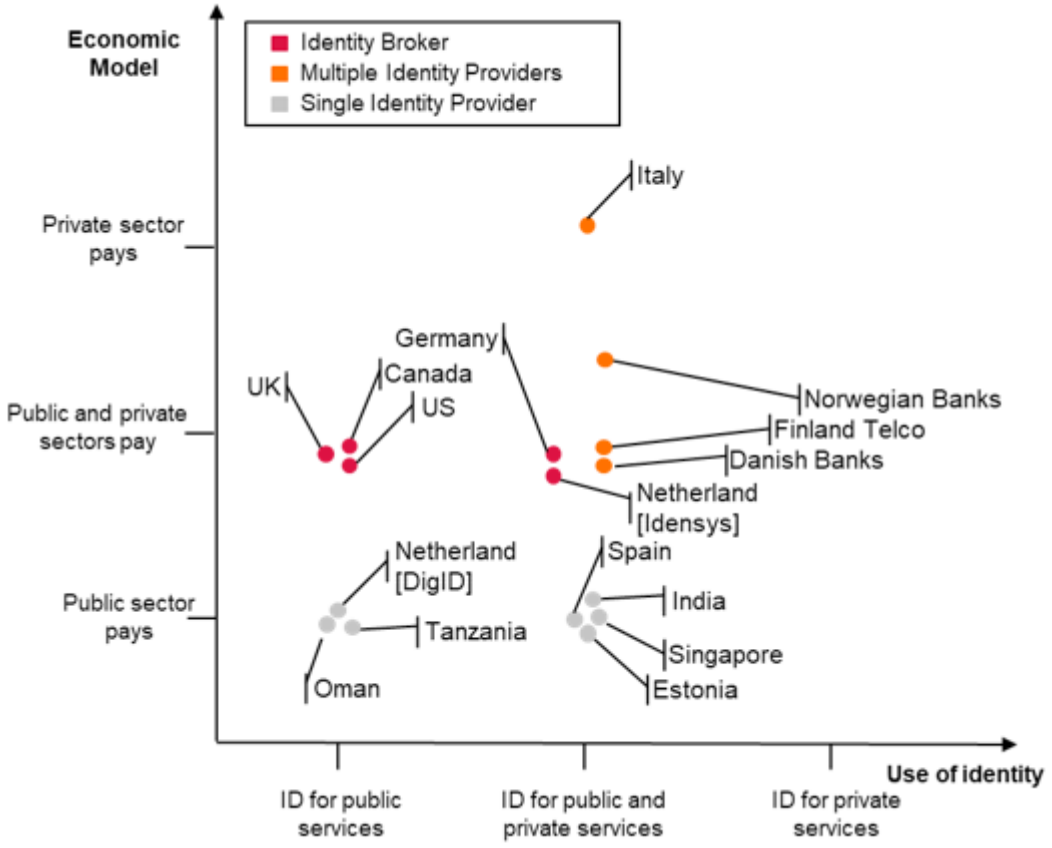
Success stories related to the adoption of Identity Brokers can be found in the UK, Germany, Canada and the US, where in each case one Identity Broker is implemented (see Figure 2). In the Netherlands, the revisited National Digital Identity Framework, *Idensys*, even posits multiple Identity Brokers at the national level.

*Fostering Federation of Identity Providers*

As already anticipated, one of the key drivers of the involvement of Service Providers is the opportunity to access a large user base. Governments can leverage this goal in different ways. One option is the involvement of private operators as Identity Providers after a selection process based on criteria defined by the government.

There are several successful international cases, particularly in Europe, that have seen federations of banks and telco operators acting as Identity Providers. These entities are to be preferred, as they already have a significant user base that has been properly verified and that already has robust authentication credentials.

Figure 2 – Distribution of Identity Provider/Broker models




## 4.3 Focus Area 3 – Architectural model

This Focus Area introduces good practice elements to be considered when addressing the architectural model for the National Digital Identity System.

Essentially, architectural models are differentiated by the number of Identity Providers involved and the approach governing the interactions between the different stakeholders involved.

Three different architectural models are possible:

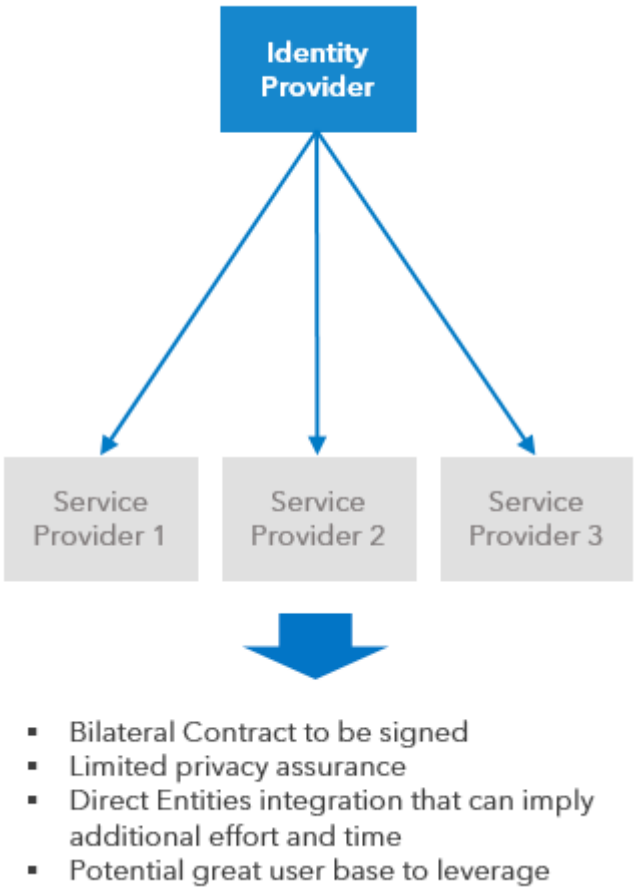
- One unique Identity Provider
- Multiple Identity Providers
- Identity Broker/s with multiple Identity Providers.

Clearly enough, there is a correlation between governance models and architectural models, as described in the previous sections. However, these should not be seen as rigidly intertwined.

***One unique Identity Provider***

This section explores the scenario in which only one entity is authorized to provide digital identities.

Figure 3 – Single ID Provider architectural model




In centralized identity systems, a single entity acts as an Identity Provider, authenticating users to Service Providers and transferring their attributes. These systems are often designed to streamline service delivery, enable data aggregation and provide a single view of users across multiple Service Providers.

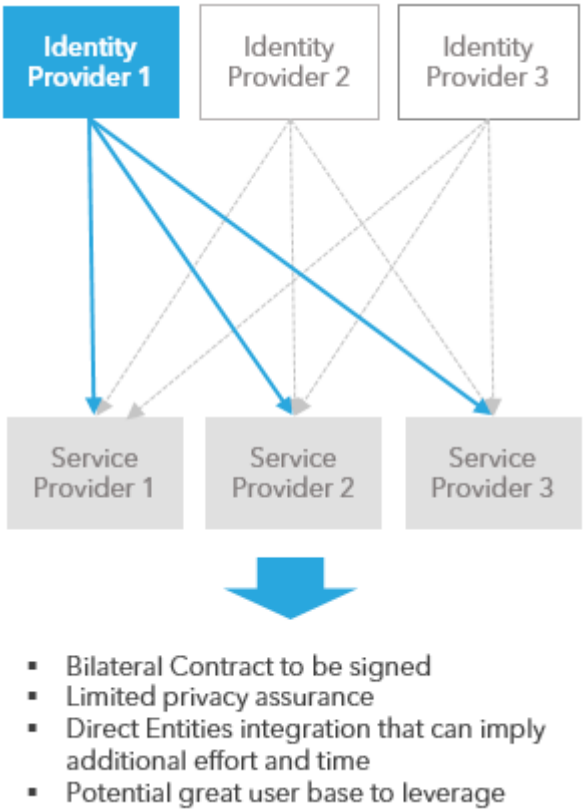
The main characteristics of this approach are:

- A unique Identity Provider accountable for the identity proofing of citizens. This entity holds users' credentials and attributes.
- The Identity Provider is accountable for the authentication of users that are allowed to access digital services across multiple Service Providers, public and private. A set of defined attributes is transferred to Service Providers to enhance the personalization of services and efficiency of processes.
- Private Service Provider participation is allowed subject to criteria compliance and fee payment.
- Privacy is limited compared to other systems, as the Identity Provider is aware of the services the user is accessing.

**When this architecture is adopted the government is directly involved as Identity Provider.**

India is a well-known example of this approach. The Aadhaar programme is world's largest digital identity programme and has adopted a centralized Digital Identity System.

Figure 4 – Multiple Identity Provider architectural model




Another example is Finland. The Finnish Population Registry is a good illustration of the single Identity Provider scenario. The Population Registry is a national database owned and maintained by the Finnish government. The government acts as Identity Provider, transferring attributes to public and private Service Providers. The purpose of the system is to collect data that can be used for elections, tax filing, judicial administration, and so on. Private Service Providers may also access this data, subject to criteria compliance and fee payment.

In the same fashion, *DigID* is a digital authentication system for Dutch residents who access government services online. Individual attributes are held in a national citizen registry. These attributes are used to authenticate users when they apply for a *DigID*. Individuals can then use their *DigID* username and password to authenticate themselves to government agencies, with their national identifier number transferred from the national citizen registry to the relevant Service Provider/s.

Estonia also represents a successful case in which the government operates as unique Identity Provider. The Estonian model is based on an electronic identity card, called simply *ID-card*, which is used as definitive proof of identity in both a digital and physical context. There are innumerable uses spanning both the public and private sectors: bank account identification access, digital signatures, access to public services (such as medical records and tax profile). Since the launch of *ID-card* a *Mobile-ID* mobile solution has also been introduced, allowing citizens to use their mobile phones as a secure form of digital identity. Both *ID-card* and *Mobile-ID* are government regulated: *ID-card* is issued by the Police and Border Guard, which is also responsible for establishing the identity of users through *Mobile-ID*, though *Mobile-ID*-compliant SIM cards are issued by mobile network operators.

*Multiple Identity Providers*

This section explores the scenario in which multiple entities are authorized to provide digital identities.

In distributed identity systems, multiple Identity Providers collect, store and manage user credentials and attributes, interacting with multiple Service Providers. These systems leverage multiple Identity Providers' capabilities and differentiators for completion of identity processes, and in particular for identity proofing. Extensive experience in managing identities, having identity solutions already in place, and maintaining local branch offices that facilitate interaction with citizens, are all key elements for selecting this scenario. This architecture allows users to choose between different Identity Providers.

The main characteristics of this approach are:

- Multiple Identity Providers are accountable for the identity proofing of citizens, and respectively hold users' credentials and attributes. It is possible for the user to own different identities.
- Service Providers have to provide an option for users to select between different Identity Providers.
- The Identity Provider is accountable for the authentication of its 'own' users, who are then allowed to access the digital services of multiple Service Providers – public, but also private. A set of defined attributes can be transferred to Service Providers to enhance the personalization of services and efficiency of processes.
- Private Service Provider participation is allowed subject to criteria compliance and fee payment.
- Privacy is limited compared with other systems, as the Identity Provider is aware of the services that the user is accessing.

**When this architecture is adopted, the government is responsible for defining criteria and completing the accreditation of Identity Providers. It represents a sort of 'federation of providers' regulated by the government.**

An example of a multiple Identity Provider system is offered by the Italian *SPID*, which was launched in March 2016 with the aim of providing digital identities to Italian citizens to allow access to public administrative services as well as private digital services. The *SPID* system requires identities to be issued and managed by a set of Identity Providers, not limited in number, but bound to an accreditation process defined and managed by the Agency for Digital Italy (AgID).

*Identity Broker/s with Multiple Identity Providers*

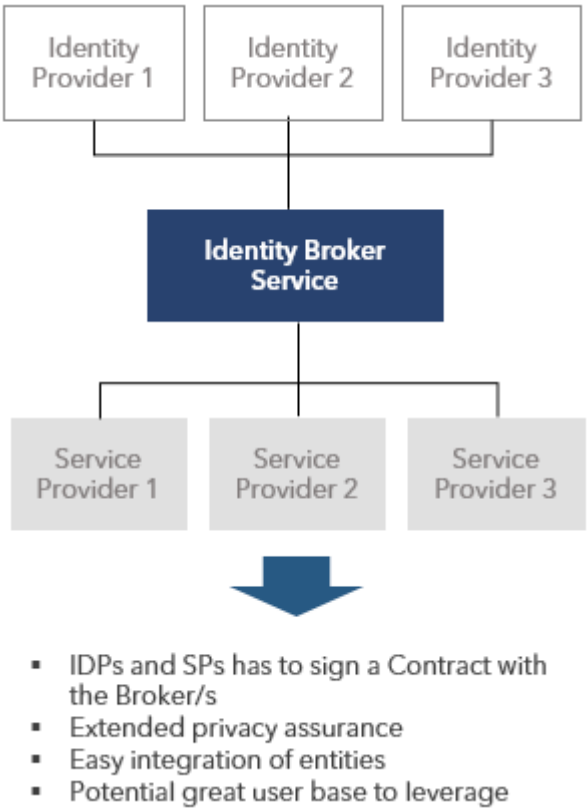
This section explores the scenario in which multiple entities manage digital identities, while interacting with one or more Identity Broker.

The majority of initiatives with multiple Identity Providers envisage the implementation of a Broker as an intermediary that connects Identity Provider and Service Provider. The objective is to intermediate communication between Service Provider and Identity Provider, placing the Broker between these two entities. The main advantages of this approach relate to the possibility of simplifying the integration of Service Providers with multiple Identity Providers. The approach also guarantees greater privacy for users, preventing Service Providers from tracing back to Identity Providers accessed by users, and vice versa.

The main characteristics of this approach are:

- Multiple Identity Providers are accountable for the identity proofing of citizens, and respectively hold users' credentials and attributes. It is possible for the user to own different identities.
- Service Providers only need to connect with the Identity Broker, which is responsible for presenting users with the option to use different Identity Providers.
- The Identity Provider is accountable for the authentication of its 'own' users, who are then allowed to access the digital services of multiple Service Providers – public, but also private. A

Figure 5 – Identity Broker with multiple Identity Providers architectural model




set of defined attributes can be transferred to Service Providers to enhance the personalization of services and efficiency of processes.

- Private Service Provider participation is allowed subject to criteria compliance and fee payment.
- Privacy is higher compared with other systems, as the Identity Provider is not aware of the services that the user is accessing and Service Providers are not aware of the Identity Provider selected by users.

**When this architecture is adopted the government is responsible for defining criteria and completing the accreditation of identity providers. It represents a sort of federation of providers regulated by the government. At the same time, the government might deploy and operate the Identity Broker or mandate this role to an external entity.**

As previously outlined, the introduction of an Identity Broker can simplify Service Provider adoption, facilitating participation by those who have reduced capacity both in economic and technical terms. This also makes it possible to reduce integration times and tasks, especially in the case of the integration of new Identity Providers in the future.

As noted, the presence of an Identity Broker is also useful as it can act as a clearing house for the management of costs and billing associated with identity services; under current systems, it is very difficult if not impossible for Service Providers to invoice each of the accredited Identity Providers.

A clear example of the role of an Identity Broker is provided by the GOV.UK Verify programme, which is an external authentication system that allows UK citizens to access government services online. Users verify their identity online with one of up to ten Identity Providers. Once users are authenticated through one of these providers, they are granted access to the government service they wish to

access. The programme uses a 'hub' (Broker) that allows Identity Providers to authenticate identities to reliant parties without:

- The government centrally storing an individual's data
- Privacy being breached by exchanging unnecessary data
- Either transacting party openly sharing user details.

***Other architectural models***

Distributed ledgers might represent a future alternative architecture for identity management, and is certainly worthy of evaluation by governments looking to establish a National Digital Identity Framework. This architecture accommodates multiple Identity Providers interacting with multiple Service Providers, as in other architecture models, the difference being in what is called the process of 'identity attestation'. In practice this means that identity credentials are attested by users and third-parties via a decentralized database.

However, the role of the government in this architecture is crucial. When this model is not properly implemented, there is a risk of relinquishing control to the benefit of third parties (such as corporations) or completely shifting control to users.

## 4.4 Focus Area 4 – Sustainability model

The sustainability of a National Digital Identity Framework is one of the main concerns that national leaders and policy makers should bear in mind when designing a framework. Even the most efficient, effective and innovative solution does not stand much chance of success if it is not economically sustainable.

Managing user identities entails certain costs, in the main related to the two processes of user verification and authentication. The first one is 'the process of identifying an individual [...], and formally establishing the veracity of that identity'[3], while the second one represents 'the process of validating the assertion of an attribute associated with an identity previously established during identification'[4]. These processes provide different levels of guarantee based on the controls and safety techniques applied. In particular, European regulation 910/2014 (eIDAS) defines three levels of guarantee for the electronic identification means (ie. authentication).

To summarize, high authentication tools are to be expected following high identity checks. An analogous approach has been adopted by the standard ISO/IEC DIS 29115, which adopts the Levels of Assurance already described in section 4.2 regarding user convenience in terms of the enrollment process. Figure 7 displays the relationship between the different Levels of Assurance for identity verification and authentication, as indicated in eIDAS Regulation Article 8, above.

The relations presented here should be considered as a non-binding guideline. The choice to adopt a specific relation should be driven by cost-benefit considerations. For instance, providing the maximum level of authentication regardless of the identity proofing level might end up having a negative impact on implementation and maintenance costs.

[3] International Telecommunication Union – Telecommunication Standardization Sector, *X.1252 "Baseline identity management terms and definitions",* April 2010.

[4] Ibid.

Figure 6 – eIDAS Regulation Article 8[5]

***eIDAS Regulation Article 8 - Assurance levels of electronic identification schemes***

*1 - [...]*

*2 - The assurance levels low, substantial and high shall meet respectively the following criteria:*

*(a) - assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;*

*(b) - assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;*

*(c) - assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.*

The process that is likely to have the highest impact on the sustainability of the framework is the verification of user identity. Given its particular economic importance, there is a strict correlation between the adopted verification approach and the business model of choice.

The sustainability model of a National Digital Identity Framework is a product of the combination of two different aspects:

- How identities are employed
- Who pays in the system

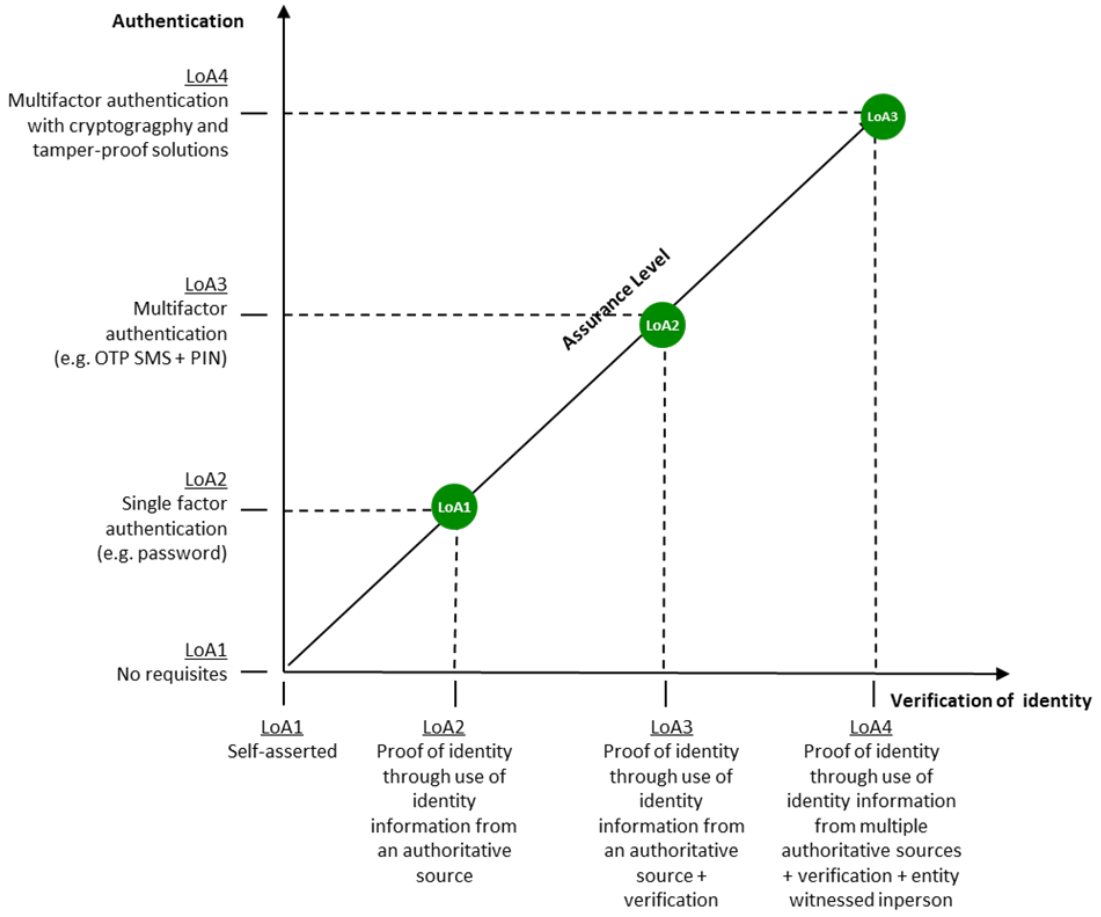
*Use of identity*

In the context of a National Digital Identity Framework, we can identify three different approaches to how an identity can be employed by users:

- Identity for public services: In this case, the identity can be employed exclusively to access services offered by the government or public administration. Examples of this approach include the United Kingdom, Canada, the United States of America, India, and Oman.
- Identity for private services: In this case, the identity can be employed exclusively to access services offered by private third parties. Although it might be possible to envisage a system relying on this service model, this option currently belongs only to private initiatives. No governments have adopted such an approach to date.

[5] See https://www.eid.as/home/

Figure 7 – Level of Assurance of ISO/IEC DIS 29115




- Identity for public and private services: In this case, the identity can be employed to access services offered by both private entities and the public administration. This is by far the most common model, accounting for the majority of systems currently in use.

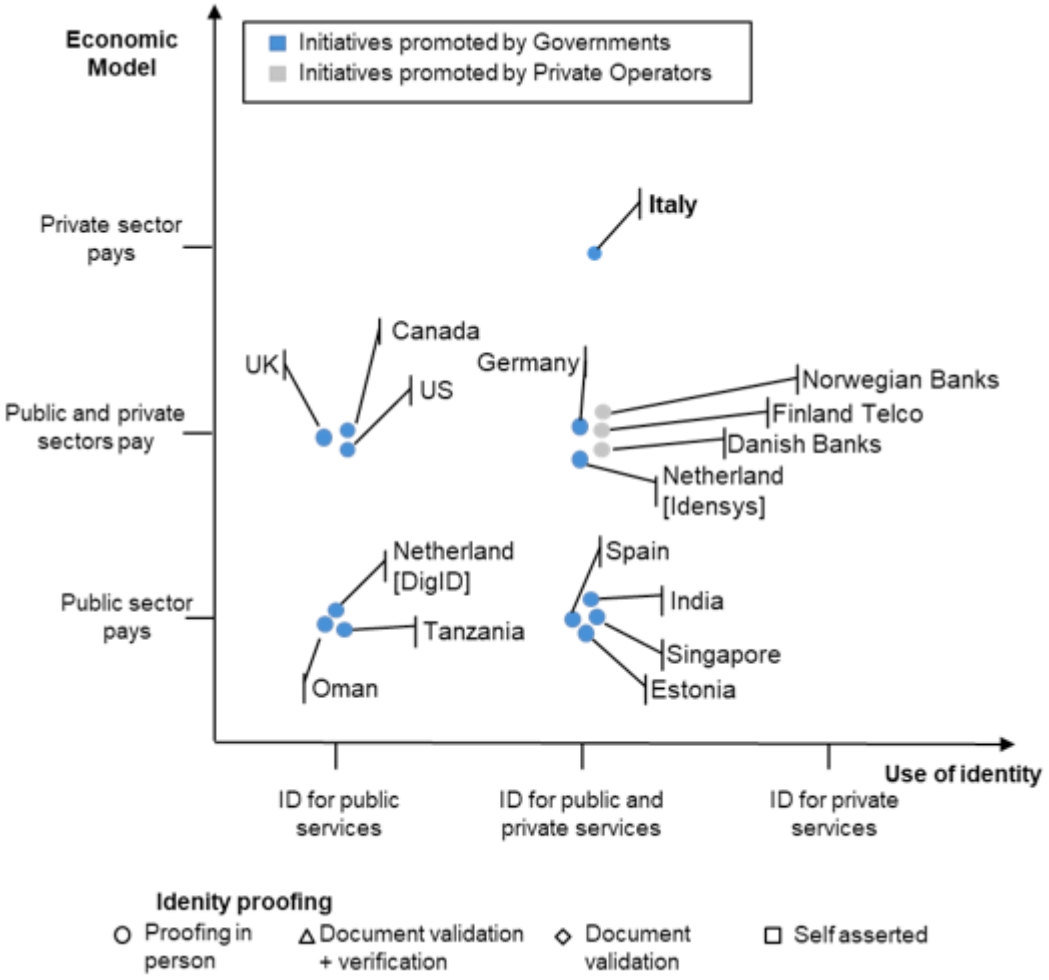
***Economic models***

In the context of a National Digital Identity Framework, we can identify three different approaches to how the system is financed:

- Financing by the public sector pays: In this case, the public sector fully sustains the costs of the Digital Identity System. Estonia is the most prominent example of this approach.
- Financing by the public and private sectors: In this case, both the public sector and the private sector sustain the costs of the system. This is a well-established model, and many examples can be found.
- Financing by the private sector: In this case, the private sector fully sustains the costs of the Digital Identity System. This is a very uncommon way to sustain a National Digital Identity Framework, and there are very few examples. The Italian National Digital Identity System (Sistema Pubblico di Identità Digital, *SPID*) falls into this category. Despite the fact that is employed by the public administration (and therefore requires an approach with highest level assurance, in-person verification) it is still private entities (playing the role of Identity Providers) that pay the costs of managing the system. The choice is primarily motivated by the fact that promoting public services has been considered the best strategy to increase the use of the system among citizens. Private entities accepted the burden of the costs while waiting for the full opening of the system to private services.

Figure 8 identifies how these three approaches distribute across a series of case studies.

Figure 8 – Distribution of economic models



# 5 National Digital Identity Framework development


This Section provides an overview of the various phases necessary to develop a Digital Identity Framework.

This section provides an overview of the phases necessary to develop a National Digital Identity Framework, defined as:

- Analyze
- Define strategy
- Implement system, and
- Operate & continuously improve.

## 5.1 Phase 1 – Analyse


Prior to planning and drafting a National Digital Identity Framework, the parties and stakeholders involved in the development of the framework should carefully assess the context and situation in which they will have to operate. This is necessary in order to establish the correct baseline that will subsequently ensure the correct implementation and operation of the framework.

***Context analysis***

*Identification of national specifics and peculiarities*

One of the first aspects to be taken into consideration is the unique characteristics that shape the environment in which the National Digital Identity Framework will operate.

National culture, traditional models, the accessibility of digital infrastructure and devices, trust in the government – these are just a few of the influencing elements that can impact the implementation and operation of a National Digital Identity Framework. Because of their potential significant impact on the effectiveness of the framework, these influencing elements must be identified at the outset of the development process so that appropriate countermeasures can be investigated beforehand. For instance, a country with a large elderly demographic might decide to emphasize simplicity and accessibility, rather than efficiency. On the other hand, a nation with a relatively young population might prefer to opt for a National Digital Identity System that seamlessly integrates into the digital fabric of citizens' already hyper-connected lives.

The choices that govern each implementation must be tailored to each specific situation. There is no one-size-fits-all approach, so it is crucial that planners correctly assess national characteristics and peculiarities.

*Benchmark of Digital Identity Strategy*

Many governments and organizations worldwide are now equipped with, or are developing, specific systems for digital identity management. Their experiences constitute an invaluable repository of information that can be used to gather relevant lessons-learned to build upon.

Any review of digital identity strategies should be focused on the broad objectives of the government concerned in developing its strategy and the targets it ultimately seeks to attain, as well as on the main elements of the plan the government has developed to realize its vision.

A comprehensive review of relevant and comparable initiatives on digital identity developed by other countries can be performed through a structured approach based on the following phases:

- Case Selection: cases to be analyzed are selected from the public and private sectors based on a series of defined criteria; it is important to ensure a good balance in terms of geography,

population size, layers of government, diversity of cultures and styles of government. A sample of different stages of advancement with respect to development and implementation of digital identity initiatives should be considered, from preliminary investigation or early development stage through to full deployment.

- Case Analysis and Classification: each selected case is analyzed and classified according to a well-defined set of criteria which facilitate understanding of the different approaches followed during the design and implementation phases, the primary objectives, the tools (laws, plans, actions, etc.) developed to implement the strategy, and the outcomes achieved.
- Case Evaluation: once the analysis is complete, good practice elements are derived to support objectives and priorities in line with the vision defined in the National Digital Identity Strategy.

*Identification of primary objectives*

Once the entity developing the National Digital Identity System has clearly identified the environment and the context in which the system will operate, and once a review of comparable initiatives has been performed, it is of the utmost importance to clearly articulate the objectives the National Digital Identity System must satisfy.

At this point, a set of goals and objectives should already exist, as the decision to implement a National Digital Identity System most likely rests on specific needs. Careful identification of objectives and principles is crucial in providing a reliable guide for further phases.

## 5.2 Phase 2 – Define strategy


The purpose of this phase is to develop the National Digital Identity Strategy by engaging key stakeholders from the principal entity involved. Public consultations and working groups involving the public sector, private sector, and civil society could also be established, depending on the complexity of the initiative. This group of stakeholders will be responsible for defining the overall vision and scope of the strategy, setting high-level objectives, taking stock of the current situation, prioritizing objectives in terms of impact on society and citizens, and ensuring the necessary financial resources. Coordination of the initiative by a Lead Project Authority is desirable. During this phase, the primary objectives and principles and the good practice elements that emerged from the benchmarking activities conducted during Phase 1 should be taken into account.

***Definition of Digital Identity Strategy***

The Digital Identity Strategy should set the overall digital identity direction for the country, expressing a clear vision and scope, setting objectives to be accomplished within a specific time frame, and prioritizing these in terms of impact on society, the economy, and infrastructure. The strategy should also identify possible courses of action, incentivize implementation efforts and drive the allocation of

required resources to support all these activities. The drafting of the strategy could involve dedicated working groups, either focused on specific topics or charged with drafting different sections of the strategy.

The strategy needs to put forward a clear governance framework that defines the roles and responsibilities of key stakeholders. This includes the identification of the entity responsible for the management and evaluation of the strategy, as well as an entity responsible for its overall management and implementation, such as a central authority. In the same vein, it also needs to define or confirm the mandate of all the entities responsible for operating the initiative, and how all of these entities interact with each other and with the central authority.

In the final step of strategy development, its formal adoption has to be ensured. Its broad availability will ensure that the general public is aware of the government's priorities and objectives for the introduction of digital identity, and also support any other efforts to raise awareness. This official adoption process will vary by country and be based on how the strategy is defined within the legislative framework. Furthermore, it is vital that the strategy is not only developed with approval from the highest levels of government, but that this commitment continues throughout its implementation phase.

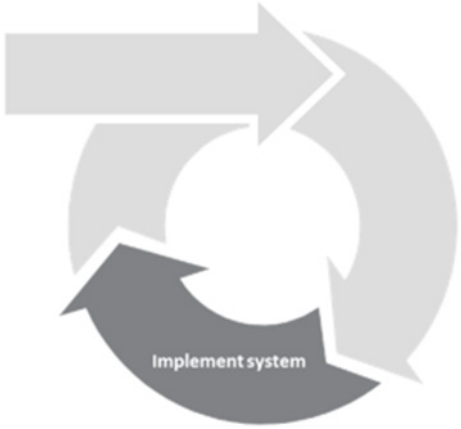
***Definition of implementation roadmap***

A structured approach to implementation, supported by adequate human and financial resources, is critical to the success of the Digital Identity Strategy and needs to be considered a part of its development. The implementation phase should be centred on an Action Plan, which can support the effective implementation of the strategy and guide the various activities envisioned.

In the Action Plan specific initiatives are identified and detailed within each focus area that will help meet the objectives and achieve the outcomes, as well as coordinate efforts and pool resources. The timeline, dependencies between tasks, and efforts needed for the implementation of different initiatives should be prioritized in accordance with their criticality, to ensure that limited resources are appropriately allocated.

As part of the definition of the implementation roadmap, specific metrics and key performance indicators should be identified to facilitate ongoing evaluation of the efficiency and effectiveness of the initiatives during and after their completion.

## 5.3 Phase 3 – Implement system




The goal of this phase is to define and implement the single core elements and characteristics that form the basis of the National Digital Identity Framework.

***Implement governance model***

Governments have to carefully implement the governance models and supporting tools. Once the government has selected which role it will play in the National Digital Identity Framework (eg., just Regulator, or Identity Provider, etc) it is important to define the entire set of processes, roles and responsibilities that need to be put in place for the government to efficiently play the role it has decided to adopt. This comprehensive, clear set of processes, roles and responsibilities must be formalized and distributed among all relevant stakeholders.

***Define and review regulations and laws***

In most countries, existing legislation that would impact digital identity is scattered throughout many different legal acts and regulations, including those pertaining to electronic communication and commerce, electronic signature, data protection and privacy. For this reason a detailed review of potential issues arising from existing national regulations and laws should be investigated in advance, and a set of proper measures instituted.

During the review of laws and regulations, attention should also be given to the country's broader ICT policies and regulatory environment. Digital identity is an integral element of the national ICT landscape and could benefit from policies that aim, in the long term, to promote modern and effective ICT infrastructure in a country.

Examples of how the National Digital Identity Framework development can be positively affected include policies that aim to improve connectivity, access, and education and training. National incentives for the private sector to participate in the development of ICT infrastructure may also be of benefit.

***Design architectural model***

The architectural model can follow different approaches: a centralized system with a single Identity Provider that collects and manages all information and data; a distributed system with multiple Identity Providers; or a system with intermediaries between Identity Provider(s) and the other elements that serve specific verification or control functions. Depending on the selected architectural model, a Digital Identity System will be built by selecting and implementing several technology solutions/options.

National technology strategy thus plays a crucial role in the development of a digital identity; dimensions that come into play include cost, capacity, interoperability, usage, security, privacy, and long-term viability. Many of the technical components revolve around identity data, including technology for capturing, encrypting, transmitting, storing and using these data to identify and verify the identity of individuals.

An important part of any national technology strategy is an assessment of the country's underlying, enabling technology infrastructure. High-speed Internet is often a necessary requirement for online identity solutions, but many developing countries are still working to develop and deploy broadband networks. The degree of penetration of smart devices in a country – in the form of smartphones and tablets – determines the potential for mobile identity and mobile applications. A strong domestic IT industry is needed to provide the human capacity and the products and services that can benefit from digital identity. Electronic banking and financial services require the availability of a financial infrastructure – such as a national payments system, POS devices, ATMs, agent networks, and payment networks – to benefit from digital identity.

For these reasons, the architectural choices – including the identification of functional and non-functional requirements, the selection of platform components, the definition of interfaces, and other technical specifications – should carefully take into account the importance of creating the right environment in which technical boundaries and dependencies can be effectively managed.

Finally, the definition of a pilot scope and use case (for example, a government sector) could help in identifying functional and infrastructure adjustments in terms of architecture scalability that need to be addressed in the future.

***Implement adoption model***

The digital services accessed by a generic entity require the implementation of an end-to-end process throughout the whole lifecycle of digital identity, which spans the following phases:

- Collection: information collection for the definition of the digital identity.
- Certification: verify the match between the information collected and the real identity.
- Provisioning: creation and assignment of user, access credentials and rights for digital identity.
- Data update facility: given that many data attributes are likely to change during the life time of an individual, it is critical to establish mechanisms through which citizens can update their data in a secure yet convenient manner. Without a proper data update mechanism, the data related to the digital identity will become obsolete, rendering it useless.
- Authentication: perform a check of access credentials input during the access phase to the digital service.
- Authorization: perform a compliance check between the privileges assigned to digital identity and those necessary to the specific service.
- De-provisioning: removal of accounts, credentials and/or privileges based on specific request, events or rules.

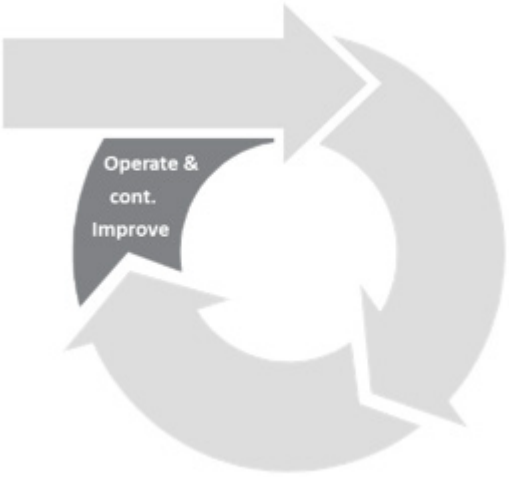
***Implement sustainability model***

Sufficient, consistent, and continuous funding is the foundation of an effective digital identity initiative. Based on the governance model established for the National Digital Identity Framework, the allocation of dedicated and appropriate resources for its implementation, maintenance, and revision should be defined and specified in terms of financials (ie., dedicated budget), people and material, as well as the relationships and partnerships and continued political commitment and leadership required for its successful execution.

Digital Identity Systems can require high investments and costs (especially for sizeable populations), both in terms of up-front setup as well as ongoing operation and maintenance. The types of pricing and cost-distribution models selected are vital to ensuring a sustainable National Digital Identity System. Governments can leverage potential revenue flows by offering identity services to offset the costs of digital identity development to help promote overall operational sustainability.

Public-private partnerships can provide an avenue to relieve the financial burden, and have proved a successful strategy in many countries. A financial and economic model, with detailed expected costs and potential revenue streams, needs to be developed up-front and implemented accordingly.

## 5.4 Phase 4 – Operate and continuosly improve




During this phase, all the tasks related to the operational side of the digital identity lifecycle are to be performed, and a formal process to monitor and evaluate the implementation progress and efficiency of the strategy should be defined and applied. In the monitoring phase, the government should ensure that the strategy is implemented in accordance with its Action Plan. In the evaluation phase, the government/competent authority should assess whether the strategy still reflects the government's objectives and what adjustments might be necessary.

Continuous assessment of the implementation plan (ie., what is going well and what is not) helps inform the Digital Identity Strategy. Good governance mechanisms with regards to the strategy implementation should also clearly delineate the accountability and responsibility for ensuring successful execution. Furthermore, the allocation of budgets should match the levels of ambition and complexity of the desired impact.

The establishment of baseline metrics will enable better monitoring of actions and highlight areas for potential improvement. This approach will ensure that the relevant stakeholders are held accountable for the commitments set, as well as identifying any implementation challenges early on. In turn, this allows the government to either rectify the situation or adapt its plans accordingly, based on the lessons learned during the implementation process.

In addition to assessing progress across the agreed-upon metrics, it is important to also periodically evaluate the outcomes and compare them with the objectives set. This is critical for understanding whether the objectives of the strategy are being realized or whether different actions should be considered.

Once a digital identity platform is operational, monitoring for fraud management also becomes critical. Some types of fraud can be managed through the technology design of the Digital Identity System; other types of fraud will need to be monitored during ongoing operations, such as data updates and authentication.

# 6 Critical success factors and conflicting principles

As has become clear, designing and implementing a successful National Digital Identity Framework involves a huge number of factors, considerations and complex decisions. But among all the factors that influence the process some can be viewed as critical enablers that, when correctly implemented, greatly increase the chance of success of the National Digital Identity Framework and its underlying system.

In addition, there are several principles having a considerable impact on the advancement of the project that, by their nature, may conflict with one another, particularly in terms of the priorities of users versus the priorities of Service Providers. These sets of paired principles are nonetheless an invaluable tool in helping governments decide how to characterize their National Digital Identity Frameworks; they narrow the choices, and create increased focus and clarity about what needs to be achieved.

## 6.1 Critical success factors

The following critical enablers retain their importance in the overall success of the project across different situations and contexts.

***Organization structure and capacity building***

The design and implementation of a National Digital Identity Framework will greatly benefit from being developed within solid organization that provides a pool of structured expertise from appropriate and diverse skill sets.

The areas of competence most relevant are:

- Government processes
- Technology
- Programme management
- Legal and regulatory expertise
- Media, communication and civil society outreach.

***Project management***

An appropriate project management approach is crucial to the success of the design and implementation processes of a National Digital Identity Framework. In particular, a rigorous approach comprised of lab testing, field Proof-of-Concept, pilot projects and full scale roll-out (with statistically significant data at each stage) can keep everything under control and help ensure a speedy deployment.

***Quality and standardization***

Quality management and certification should be taken into consideration at all levels, throughout the entire project, and for every aspect (people, process, technology).

***Regulatory framework***

How the digital identity programme will fit within the regulatory framework of the country needs to be defined, and will dictate stakeholders' engagement.

## 6.2 Conflicting principles

While certain factors can be seen as useful aids in the development of a National Digital Identity Framework, others present certain constraints. In many cases these constraints are unavoidable, as they originate from the inherent conflicts that arise when certain principles have to be incorporated into the design of the Digital Identity System.

***National security vs social service delivery***

The first conflicting principle directly derives from the goals established for the Digital Identity System. There are two primary reasons a government might be interested in developing a system for managing digital identity. On one hand, there is the border/national security rationale. Digital identities can be a powerful tool in combating crime, patrolling borders, ensuring citizens' security, etc. For this reason, governments might be willing to primarily employ their Digital Identity System to meet security needs. On the other hand, governments might decide to implement a Digital Identity System to enhance the service offering to their citizens (eg. increasing the efficiency of welfare and social services), rather than strengthening government control capabilities. This latter aspect in particular poses the risk of anti-government feeling, as citizens might feel they are falling under a surveillance regime, weakening trust in public institutions.

The two approaches mentioned above cannot be equally implemented in a National Digital Identity Framework, as the first (national security) requires a broader approach to the monitoring of individuals and their information, while the second will be best implemented using a 'data minimization' regime (meaning that only the data necessary to a specific purpose will be collected and processed). Since these scenarios have distinctively different characteristics, it is extremely complicated to strike a balance between them. For this reason, National Digital Identity Systems tend to favour either one scenario or the other, rather than attempting to embrace both.

It is important to note that both approaches entail their own specific sets of risks. For instance, adopting a 'data minimization' regime might preclude the possibility of extending the Digital Identity System to new social services when these require different subsets of data. The approach based on national security, meanwhile, raises the serious risk of new levels of citizen surveillance. When a great deal of data about individuals are managed (or at least can be accessed) by a single authority, citizens can find themselves facing situations that might be perceived as a major violation of their privacy and freedom.

This risk can reach critical levels when such data can be accessed by authorities with governmental power or law enforcement capacity, especially in the context of polarizing issues (eg. internal conflicts

among racial and ethnical groups). However, this also holds true when private actors enjoy a similar level of access (for instance, profiling people for commercial purposes).

These concerns might heavily influence the trust citizens have in the authorities in charge of the National Digital Identity Framework and compromise the success for the framework. For these reasons, governments willing to pursue the implementation of a National Digital Identity Framework focused on national security need to take special pains to reassure citizens. This can be done through appropriate governance countermeasures, such as independent reviews and normative frameworks, so that the process of implementation is not negatively affected by the chosen approach.

***Data security vs citizen convenience***

When managing user data, and especially when those data are sensitive (as in the case of data regarding identity), security must be one of the top system priorities. However, tight security measures can greatly affect the success of the system. Users might not appreciate the real benefits of operating in a secure environment, but instead only perceive the inconvenience they have to suffer in order to use the system (eg. time spent to authenticate multiple times, physical authentication devices that have to be carried around, etc.).

This is a challenge that governments implementing a National Digital Identity System have to face. Finding the correct balance requires a careful analysis of the risks and the benefits.

***Building a de novo identity database vs building on an existing identity database***

The creation of database for digital identities can be approached in two different ways. The first option is a Digital Identity System fully populated with newly-created digital identities. One benefit is a very good level of data consistency, since a standardized data entry approach can be adopted from inception. On the other hand, since within the framework of services offered by national entities and governments it is likely that some sort of digital identification means already exist, the second option is to leverage this existing capability to build an identity database.

This second approach can offer certain advantages, such as a potentially lower cost of implementation, but it also brings with it a number of problems, mainly related to the fact that existing systems and identification means may not suit a nationwide system for managing digital identity. For instance, some existing identity databases might not provide universal coverage (eg. an electoral identity database covers only people who have reached voting age; a driver's licence database covers only those who have a licence). In addition, since existing databases are unlikely to share a common data entry standard, the efforts and costs required to normalize the database (ie. complete partial identities with the correct attributes and acquire new identities that are not already digitized) might actually be higher than simply creating a *de novo* database.

***Minimal citizen data vs full citizen data register***

The degree of data collected and associated with each identity can greatly influence the design decisions related to a Digital Identity System. An approach that favours a wide range of attributes is likely to cost more than a simple one, both in terms of computing resources necessary to manage attribute-rich entries, and managing the resources necessary to keep the database updated. However, deciding on a minimal data collection approach rather than a full one can also substantially impact the range of services the government will be able to provide.

One option sees the Digital Identity System as an opportunity to capture an ID number associated with all social and government services in which a citizen participates (eg. voter ID card, income tax ID, passport number, census data, etc). The positive side of this approach is that it gives government a '360 degree' view of the citizen, which can serve two purposes:

1) Know the citizen better and improve services to citizens;

2) Eliminate frauds and duplicity of services. For example, if someone is availing of 2 scholarship programs or has availed services under 2 programs with conflicting eligibility criteria, that could be detected very easily.

The negative side of this approach is that it can be criticized as giving governments too much control; for example, by enabling them to easily profile citizens and use this knowledge against communities on the basis of political affiliations or other reasons. The approach also increases the complexity and time involved in enrolling citizens, as different local areas or regions might run different welfare programmes with little standardization of data formats (this particularly holds true for larger countries).

***Token-less identity vs token-based identity and digital authentication***

One of the purposes of issuing digital identities is that the holders are able to authenticate themselves at the point of service delivery. Authentication happens in any of the following ways (or a combination of these): 'What I know', 'What I have' and 'What I am'.

'What I know' will include things like username, password or PIN; 'What I have' will include factors like possession of a smart card; and 'What I am' will include biometrics (like fingerprint or iris scan). Typically, two-factor authentication is used for various transactions – for example, the use of a card along with PIN for a debit/credit card transaction.

Keeping these practices in mind, there are two approaches to the distribution of digital identities to their holders. The first is that identities are distributed as smart cards with authentication attributes on a chip, and the second is to not provide a smart card but instead keep the identities in the cloud. The first approach has the advantage that citizens can carry their card/s and can authenticate themselves as needed anytime/anywhere via a smart card reader, typically using the card and the PIN. Many countries have used this approach. Disadvantages include the relatively high cost of smart cards and the challenge of securely communicating PINs to their holders. Furthermore, life-cycle cost and maintenance of smart cards (replacement in the case of lost /damaged / compromised cards etc.) tends to be higher.

In an increasingly connected world where smartphone use is rising rapidly, smartphones can replace smart cards. One-time-password (OTP) functionality can become a powerful authentication tool when a user's smartphone is linked to his/her digital identity. This scenario enables token-less digital identities, where identities exist in the cloud and an individual is able to access the identity database for the purpose of authentication either through biometrics (fingerprints or iris scan) or OTP to a linked smartphone. This approach has been adopted by India, where there is no smart card, where the digital identity is a unique identity number generated, and where authentication is carried out directly through the identity repository on the cloud. This approach is cost effective, as it eliminates the need for producing and distributing smart cards, communicating PINs and having card readers at point of service delivery. However, the system obviously requires ubiquitous connectivity for authentication.

When deciding on the issue, each county needs to carefully evaluate the cost, processes involved, uniqueness attribute and citizen convenience in the complete life-cycle of identity management.

# 7 Country Case Studies

Case studies offer invaluable lessons about how National Digital Identity Frameworks are designed, implemented, and operated in different nations.

The following list comprises some of the most relevant case studies to date.

## 7.1 CANADA

*SecureKey Concierge* is an authentication network for conveniently connecting people to critical online services using banking credentials they already have and trust. *SecureKey Concierge* is configured to be 'triple-blind', ensuring that no party receives sensitive or personal information from other parties.

*SecureKey Concierge* is based on a system consisting of a single Identity Broker and a set of Identity Providers. The contract amount is CAD 41 million for three years.

***What was the goal in developing a Digital Identity System?***

The goal of Canadian government was to provide a method of identification and authentication – an alternative to the one already offered by the government – to access public services, based on a 'bring your own credentials' (BYOC) model, where users can leverage identity credentials that already exist and that they already use.

***Who is the Identity Provider?***

The Canadian government has chosen SecureKey as the Identity Broker, and five of the country's major banks as the Identity Providers. These have provided an existing large pool of users (their customers) and secure means of authentication.

***How are users identified?***

People can connect to critical online services using a banking credential they already have and trust.

***What is the government's role?***

The Canadian government selected SecureKey as Identity Broker via tender.

***What can digital identity be used for?***

*SecureKey Concierge* ensures people can connect to a range of important and useful online services using their banking credentials.

***What are the adoption enablers (eg. Support to citizens or service providers)?***

By adopting already existing credentials and promoting the convenience of users, the Canadian government has been able to push for a steady adoption of the system.

***How is identity proofing completed?***

Users are already registered in the Identity Providers' databases as (banking) clients. New users can be identified with an identity document at banks that are recognized as Service Providers.

***What are the authentication methods?***

Authentication is assured through instruments already defined by the Identity Providers (banks) based on a 'bring your own credentials' (BYOC) model.

***What is the level of adoption?***

In 2014, two years after the launch of the initiative, the number of digital identities had reached one million.

## 7.2 ESTONIA

Estonia has by far the most highly-developed national ID card system in the world. The mandatory national card also provides digital access to all of Estonia's secure e-services.

The digital identity system, called *e-Estonia*, was introduced in 2002, and is one of the most successful systems in terms of adoption with almost the entire citizenry enrolled in the programme.

***What was the goal in developing a Digital Identity System?***

To create an advanced digital society building an efficient, secure and transparent ecosystem that saves time and money. The electronic identity card, *ID-card*, is used as definitive proof of identity in both digital and physical contexts.

***Who is the Identity Provider?***

The Estonian government.

***How are users identified?***

The chip on the card carries embedded files, and using 2048-bit public key encryption, it can be used as definitive proof of ID in an electronic environment.

In 2007, a *Mobile-ID* mobile solution (dependent on SIM) was introduced, which allows citizens to use mobile phones as a form of digital identity, avoiding the need for a card reader.

***What is the government's role?***

The government is the Identity Provider.

***What can digital identity be used for?***

Countless uses in both the public and private sectors, such as:

- Proof of identification for accessing bank accounts
- Digital signatures
- Access to public administration services such as medical records or tax classification.

***What are the adoption enablers (eg. support to citizens or service providers)?***

The fact that all Estonian citizens need to hold a digital identity greatly promoted the quick and steady adoption of the system, which as of today has almost complete coverage of the Estonian population.

***How is identity proofing completed?***

Identity verification is completed by validating the identification documents (eg. passport, driver's licence).

***What are the authentication methods?***

Estonia has adopted an authentication method based on the physical ID-card, which has the digital identity embedded into it, combined with a card reader (either via the mobile device or integrated into a laptop/desktop device).

***What is the level of adoption?***

All Estonian citizens and everyone with a valid residence permit are required to hold a digital identity. The Digital Identity System has a current coverage close to 98% on a total population of 1.3 million.

## 7.3 INDIA

The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar Act of 2016. UIDAI was created with the objective of issuing Unique Identification numbers (UID), named as *'Aadhaar'*, to all residents of India in order to:

- Eliminate duplicate and fake identities
- Verify and authenticate identities in an easy, cost-effective way.

*Aadhaar* is a cradle-to-grave online-authenticable digital ID which is essentially a 12-digit random number generated after biometric data (fingerprint & iris) deduplication. The first UID number was issued on 29 September 2010. The Authority has so far issued more than 1.2 billion *Aadhaar* numbers to the residents of India.

Any individual who resides in India, irrespective of age or gender, can voluntarily enrol to obtain his or her *Aadhaar* number. Each person seeking to enrol has to provide demographic and biometric information during the enrolment process, which is totally free of cost. An individual needs to enrol for *Aadhaar* only once; uniqueness is achieved through the process of biometric deduplication.

UIDAI is responsible for *Aadhaar* enrolment and authentication, including the operation and management of all stages of the *Aadhaar* life cycle, developing the policy, procedures, and system for issuing *Aadhaar* numbers to individuals, and performing authentication. It is also required to ensure the security of identity information and the authentication records of individuals.

***What was the goal in developing a Digital Identity System?***

The goal was to issue Unique Identification numbers (UID) to all residents of India and to empower residents of India with a unique identity and a digital platform that enables the Government of India to

directly reach residents to deliver various subsidies, benefits and services by using only the resident's *Aadhaar* number. Two of the most critical goals of India's Digital Identity System are the uniqueness of identities and social inclusion.

- **Uniqueness of identities:** The most important motivation for ensuring uniqueness is to eliminate leakages which take place in the delivery of services and benefits to residents in various government programmes. It has been estimated that there are substantial leakages due to existence of duplicates and 'ghosts' in the set of beneficiaries of every programme. Another reason for ensuring uniqueness is to create a citizen-centric view of benefits and services which various programmes cover.
- **Inclusion:** The Aadhaar Strategy Overview [1] document observes: "In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals with services. But to date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence." This approach was especially unfair to India's poor and underprivileged residents, who usually lacked documentation, and found it difficult to meet the costs of multiple verification processes required to avail themselves of various social services.

***Who is the Identity Provider?***

Unique Identification Authority of India (UIDAI) acts as Identity Provider in partnership with the Registrars. Registrars collect demographic and biometric data from residents through Enrolment Agencies and send this data to UIDAI. UIDAI carries out the required back-end quality check and deduplication process to generate *Aadhaar* and communicate this identity to residents.

***How are users identified?***

People enrolled are identified through a 12-digit ID random number issued by the UIDAI.

***What is the government's role?***

The government owns and manages the identity platform. In addition, the government is also one of the biggest users of the digital identity platform to deliver social services to citizens.

***What can digital identity be used for?***

*Aadhaar* is a strategic policy tool for social and financial inclusion, public sector delivery reform, increasing convenience and promoting hassle-free people-centric governance.

- ***Aadhaar* as a database cleaner:** One of the key goals of *Aadhaar* is the uniqueness of identity. The most important motivation for ensuring uniqueness is to eliminate leakages which take place in the delivery of services and benefits to residents through various government programmes. This objective is achieved by adding the *Aadhaar* number of the beneficiary to the respective records in the programme databases. For example, in a scholarship programme, all students are asked to get their *Aadhaar* added to their student record. Since one student can have only one *Aadhaar*, all fakes and duplicates due to impersonation are eliminated from the database. 'Aadhaar seeding' is the necessary first step in the Government of India's Direct Benefit Transfer (DBT) programme, which now covers over 430 schemes across 55+ ministries[2].
- ***Aadhaar* as a financial address:** For all programmes whereby the Government of India provides subsidies and support to citizens, *Aadhaar* is the financial address that is used to send money to the bank account through the Aadhaar Payments Bridge (which translates the *Aadhaar* number

1 Unique Identification Authority of India (UIDAI) Planning Commission, Govt. of India, UIDAI Strategy Overview. Creating a Unique Identity Number for Every Resident in India, April 2010

2 See https://dbtbharat.gov.in/

to the bank/ bank account). Such programmes include student scholarships, pension schemes, livelihood support, food distribution, cooking gas subsidies, health care schemes etc. This system is referred to as Direct Benefit Transfer (https://www.dbtbharat.gov.in).

- ***Aadhaar* as proof of presence:** Online biometric authentication is often used as proof of presence for services that require a person to be present at the point of service delivery. Common use cases include:
  - Confirming beneficiary before delivery of services such as food grain delivery to Public Distribution System beneficiaries, health service delivery to beneficiaries of different health programmes.
  - Attendance tracking for programmes related education, government employment etc. An example is the biometric attendance system for all employees of Central Government[3].
- ***Aadhaar* for eKYC:** The eKYC service[4] enables a resident to share his/her demographic information and photograph with a UIDAI partner organization in an online, secure, auditable manner with the resident's consent. *Aadhaar eKYC* is being extensively used by the banking system to open new accounts and to issue credit products, as well as by telcos for issuing SIM cards to customers and by various government programmes to add beneficiaries. Over 250 agencies are using the eKYC service. On an average, about nine million eKYC transactions are carried out every day[5].

*What are the adoption enablers (e.g. support to citizens or service providers)?*

*Aadhaar* has been designed as a platform that can be used by any public service delivery programme to reengineer its services. Leveraging *Aadhaar* (both adding *Aadhaar* to service delivery databases and online authentication) benefits both residents (convenience and portability) and Service Providers (cheaper, faster, and ensures targeted service delivery).

The scale that *Aadhaar* has been able to achieve is a result of some conscious policy decisions taken during the design phase. Key decisions included:

- A self-incentivized ecosystem that enables the field-level team to drive speedier adoption; there has been a very conscious effort at UIDAI to ensure a very large ecosystem of partners for all aspects of ID lifecycle management, such as:
  - Enrolment – registrars, enrolment agencies, device kit providers, biometric service providers
  - Data updates – enrolment ecosystem + online self-service mechanisms
  - Authentication – biometric device providers, network providers, user agencies.
- An open, standards-based interoperable platform to allow easy plug-and-play for various service delivery/support systems. This was supported by well-defined (and published) Application Programming Interface (APIs) and standards for ecosystem partners to leverage while building their solutions.
- Multiple service providers to ensure required quality while containing costs and minimal dependency on a single vendor.
- Centralized control and definition of quality, technology and processes to ensure a robust backbone and adequate quality of data in the system.
- A focused project management-based approach, well designed proof-of-concept studies (PoCs) and pilots, followed by large scale roll-out.

---

[3] See https://www.attendance.gov.in/
[4] Unique Identification Authority of India (UIDAI), AADHAAR E-KYC API Specification. Version 2.5, March 2018
[5] See https://www.uidai.gov.in/aadhaar_dashboard/ekyc_trend.php

***How is identity proofing completed?***

Biometrics are at the heart of *Aadhaar*, to ensure uniqueness of identity. Aadhaar is generated in a 2-step process:

- ***Aadhaar* enrolment**: An offline field-level activity that includes residents visiting an Enrolment Centre, filling in the enrolment form, getting demographic and biometric data captured, submitting proof of identity and address documents, before collecting an acknowledgement slip containing an Enrolment ID. The data is then sent to the UIDAI data centre where *Aadhaar* generation process begins.
- ***Aadhaar* generation**: A back-end process that involves activities such as quality checks, packet validation, demographic and biometric deduplication etc. *Aadhaar* is generated successfully only if:
  - The quality of enrolment data meets prescribed standards laid down by UIDAI.
  - The enrolment packet passes all the validations done in CIDR.
  - No biometric duplicate is found.

  If any of the above conditions is not satisfied, then *Aadhaar* number will not be issued and the enrolment gets rejected. UIDAI has also set up exception processes for handling challenges associated with biometric technology such as false reject and residents with poor or no biometrics such as leprosy patients.

***What are the authentication methods?***

*Aadhaar* authentication[6] is the process whereby the *Aadhaar* number, along with the attribute to be verified (demographic/biometrics/OTP) is submitted to UIDAI's database for verification; the system verifies whether the data submitted matches the data available and responds with a 'yes/no'. The purpose of authentication is to enable residents to prove their identity and for Service Providers to confirm that residents are 'who they say they are' in order to supply services and accord access to benefits.

*Aadhaar* provides online authentication[7] through the following means:

- Demographic data
- Fingerprint
- Iris
- OTP.

***What is the level of adoption?***

Some statistics (as of August 2018) provide an overall picture of the project's success:

- Number of *Aadhaar* identities issued: >1.2 billion
- Number of authentication transactions carried out: About 22 billion
- Number of eKYC transactions carried out: >6 billion
- DBT beneficiaries under different schemes in financial year 2017-2018: 1.24 billion
- Amount transferred under DBT scheme: >USD 65 billion

[6] See https://uidai.gov.in/authentication/authentication-overview/authentication-en.html
[7] Unique Identification Authority of India (UIDAI), AADHAAR E-KYC API Specification. Version 2.5, March 2018

*Aadhaar* has caused many paradigm shifts. In a country where a large number of people had no way to establish their identity, they have leapfrogged from no identity at all to a state-of-the-art online identity. Some of the social benefits include:

- The creation of the largest service delivery reengineering programme in the world. As an online identity, any service that needs to use *Aadhaar* needs to be in online format. Adoption by various service delivery programmes has expedited the long-pending process transformation and digitization of most government programmes.
- The need to prove identity only once during *Aadhaar* enrolment and subsequent *Aadhaar*-based eKYC usage by Service Providers has substantially brought down transaction costs for providing services. Using *Aadhaar eKYC*, banks are now able to provide no-frills bank accounts to the underprivileged that requires zero minimum balance.
- The delivery of social welfare programmes has been transformed by bringing in populations that were previously cut off from such benefits through lack of identification. For example, over 50 million poor households have been provided cooking gas connection under a scheme that uses *Aadhaar* to identify beneficiaries and manage subsidies[8].
- The government has been able to shift from indirect to direct benefits transfer. In financial year 2017-2018, the Government of India transferred subsidies worth over USD 26.2 billion directly to beneficiaries' bank accounts[9].

A single, universal identity number has been transformational in eliminating fraud and duplicate identities. This has resulted in significant savings to the state. As per estimates, in financial year 2017-2018, the Government of India has saved over USD 14 billion through the *Aadhaar*-based Direct Benefit Transfer (DBT) scheme. Over 27.5 million fake, duplicate or non-existent records were eliminated in the food distribution programme[10].

## 7.4 OMAN

The Sultanate of Oman's Information Technology Authority (ITA) aims to consolidate government policies to transform the Sultanate into a knowledge-based economy, bringing social and economic benefits to Omani society by using technology to support policies of economic diversification and sustainable development. In order to support Oman's Digital Society initiatives, substantial legal protection for the various entities in the use of ICT for official and personal communications and transactions is required. ITA has begun the formulation of an 'e-Legislation' project for Oman to increase both citizens' and businesses' trust in electronic transactions. The goal is to establish the required infrastructure to implement the applications needed to support the delivery of electronic and Internet-based services.

ITA launched the National Public Key Infrastructure (Oman National PKI) in order to support the use of e-services and to spearhead the implementation of an e-services infrastructure. Oman National PKI is owned and operated by ITA as the National Digital Certification Centre (NDCC). NDCC provides PKI services to government entities, companies, citizens and residents. The Oman National PKI uses the National Digital Identity System to provide strong and secure authentication to applications and websites by providing a trusted digital identity.

One of the most important components of the National Digital Identity System is the digital certificate. A digital certificate is the mechanism used to associate a public key with a collection of components, allowing for unique identification of the claimed owner. Citizens and residents who use electronic services request a digital identity certificate (authentication certificate), a credential that contains the

[8] See http://www.pmujjwalayojana.com/
[9] See https://www.dbtbharat.gov.in/
[10] Prasanta Sahu, Direct Benefit Transfer: Savings up 58% to Rs 32,984 crore in FY18, June 2018, https://www.financialexpress.com/economy/direct-benefit-transfer-savings-up-58-to-rs-32984-crore-in-fy18/1193744/

public key for an individual along with other identity information. The certificate is created and signed by the Oman National PKI as the trusted Certificate Authority. When the CA signs the certificate, it binds the individual's identity to a public key and the CA itself owns liability for the authenticity of that individual. In addition to the authentication certificate, Oman National PKI issues an electronic signature certificate, which is used to digitally sign documents and transactions and is legally binding.

***What was the goal in developing a Digital Identity System?***

In order to support Oman's Digital Society initiatives, Oman National PKI uses the National Digital Identity System to provide strong and secure authentication both government and private sector applications and websites by providing a trusted digital identity.

***Who is the Identity Provider?***

ITA acts as the Identity Provider in Oman to provide strong authentication and digital signature.

***How are users identified?***

For the digital identity incorporated in both National and Resident Cards, citizens and residents are identified and confirmed physically by Royal Oman Police (an accredited Registration Authority).

For Mobile ID, citizens and residents are identified and confirmed by the Mobile Network Operator registration officer using the National or Resident Card. The SIM card will not be registered in the system if the ID card is not inserted.

***What is the government's role?***

The government of Oman, through the National PKI, issues digital identity certificates to citizens and residents. It also acts as the Identity Provider.

***What can digital identity be used for?***

To date, 24 government and private entities have integrated the national digital identity gateway or Mobile ID (Mobile PKI) system into their websites, applications and mobile apps. Those entities provide online services by authenticating citizens and residents securely using the digital identity in the ID card or Mobile ID.

***What are the adoption enablers (eg. support to citizens or service providers)?***

1) The National eOman Strategy acts as an umbrella for the government's electronic transformation initiative, where unlimited support is provided to transfer traditional services to electronic services.
2) Solid PKI services, including reliable and highly available systems for authentication, electronic signing, Time Stamp, Electronic Stamp, CRL, OCSP, and signature verification.
3) Legislation availability
4) Oman e-Transaction Law.
5) Integration of the National ID card registration system with the National Digital Identity System.
6) Integration of the telecommunication registration systems with the National Mobile PKI Identity System.
7) Enforcement to provide government services via PKI services. In Oman, the enforcement is achieved using a mandate by the highest authority, the Ministers' Cabinet. Online services are **only** provided by PKI services.
8) Awareness-building strategies and campaigns for the entities and the public.

***How is identity proofing completed?***

- The National ID Card (eID) is owned, issued and managed by the Royal Oman Police (ROP). ROP is accredited as a Registration Authority (RA) by Oman National PKI. ROP performs certification registration duties by establishing and confirming the identity of citizens or residents (birth certificate, form), initiating the certification process with Oman National PKI on behalf of citizens and residents. ROP does not issue certificates, but acts as a broker between citizens and residents and Oman National PKI, and then embeds the certificates in the eID chip, an advanced system with high security features. The enrollment process is mandatory. Citizens and residents acquire the digital ID the moment they obtain an ID card in all Civil Status Centers in all governorates. The activation is performed immediately after receiving the ID card by entering a 6-digit PIN via the PIN pad provided by ROP. It is necessary to activate the identity before it is ready to be used in order to secure it against illegal use.
- PKI-enabled SIM cards are provided by Mobile Network Operators (MNOs), and these entities are also accredited as RAs for Oman National PKI. The digital identity certificates are registered by the MNOs and issued by Oman National PKI. The digital Identity is embedded in the SIM card in a PKI certificate. The enrolment process is optional. Citizens or residents may ask the MNO for a PKI-enabled SIM card the moment they obtain a SIM card. Activation is provided via the portal **www.oman.om/tam** after receiving the registered SIM card and entering a 6-digit PIN via the phone. The identity is proofed by ID card, with strong authentication in the portal.

***What are the authentication methods?***

Secure two-factor authentication using the ID card+PIN or a PKI-enabled SIM card+PIN.

***What is the level of adoption?***

- **Certificates Issuance: 100%**

  From July 2013- July 2018: **7.1 million** digital identity certificates have been issued via ID cards and Mobile ID for Oman's 4.5 million population.

- **Number of Transactions**

  From July 2013- July 2018: **14.1 million** electronic transactions by citizens and residents using digital identity.

- **Integrated Entities**

  Oman provides hundreds of services that are delivered only to users who have a digital identity. A total of 24 government and private entities are integrated into the National Digital Identity System. The services offered include commercial services, manpower services, health care services, financial services, customs services, social insurance services, SME services, election services, and municipal services.

## 7.5 TANZANIA

The National Identification Authority (NIDA) was established under Section 2(1) of the National Identification Authority (Establishment) Instrument, 2008. NIDA identifies and registers citizens, legal residents, and refugees and maintains a National ID Database for the purposes of enhancing the security and socio-economic development of the country. NIDA is a government institution under the auspices of the Ministry of Home Affairs of Tanzania.

Ongoing digitization of its activities saw NIDA launch its first electronic identity card in 2016. The *Tanzania National (e)ID card* is a smart card that can be used to access both governmental and

non-governmental services. The chip on the card allows the electronic identification of the owner through specific sets of data:

- Biographical data:
  - National ID number
  - Name of cardholder
  - Gender
  - Date of birth
  - Place of birth (district)
  - Pace of issue
  - Place where card printed (ie. Dar Es Salaam)
  - Birth certificate number
- Photo
- Fingerprints – both right and left fingerprint templates of the cardholder
- Residential address
- Personal reference information.

Each individual who registers with the National Identity Authority (NIDA) is associated with a number called a National Identification Number (NIN). The NIN is assigned to an individual at the time of initial registration with NIDA. The NIN is associated with a single set of biometric attributes of the individual holding the NIN, can never be changed or altered in any form, and cannot expire.

To avoid duplications or mistakes, NIDA adopts the Automated Fingerprint Identification System (AFIS). AFIS is a national ID application subsystem designed to automatically match one or many unknown fingerprints against the samples in the National ID Database registry. All new applicants' records must go through an AFIS check for verification as to whether their records exist in the National ID Database or they have been blacklisted.

All processed information is centrally stored in a state-of-the-art data centre which conforms to recognized international standards (ISO 27001 and ISO 9001). The data centre is equipped with a Disaster Recovery Site, a mirror site that, in case of disaster at the main data centre, can be used to operate the national ID System. NIDA requires nationwide ICT access services to connect all District Registration Offices to the data centre.

To register and obtain an ID card, citizens must send information to the central processing centre for verification purposes. Information is subject to vetting by the AFIS system to remove duplicates. Once information is verified, IDs are printed. All printed IDs are subjected to a physical and electronic quality check.

***What was the goal in developing a Digital Identity System?***

NIDA was established with the following core objectives:

1) Registering people living in Tanzania aged 18 years and above, including citizens, legal residents, and refugees.
2) Building a database of registered persons and sharing data with all relevant stakeholders and beneficiaries.
3) Producing and issuing ID cards to all registered people to serve as an identification document for various transactions wherever identification is requested.

4) Fostering good governance.

***Who is the Identity Provider?***

NIDA is the only institution vested with mandate of preparing and issuing national ID cards.

***How are users identified?***

In Tanzania an individual gets a digital identity at the moment she or he obtains an ID card. The issuance of both physical and digital identities, therefore, happens at the same moment.

***What is the government's role?***

The government is directly involved in the Digital Identity System as manager and as Identity Provider through NIDA.

***What can digital identity be used for?***

The national ID system has led to several benefits for the Tanzanian government, from the elimination of 'ghost' workers in the Government Payroll System to assistance in identification for national social security schemes. The ID system is also used by financial institutions when evaluating individuals for loans, or to solve problems when identifying potential beneficiaries of student loans. The National Identification System is expected to significantly reduce the financial resources required by other government systems through harmonization of the identification of persons, as well as being used to increase the security of border control and to fight crime.

***What are the adoption enablers (eg. support to citizens or service providers)?***

In Tanzania adoption has been encouraged thanks to government action making it mandatory to access a number of public services using digital identity, such as:

- Obtaining a Tanzanian passport
- Opening or registering a new company.

***How is identity proofing completed?***

To register and obtain the ID card, citizens must send information to the central processing centre for verification purposes. All information then passes through different approval processes. All information is run through the AFIS system to remove duplicates. Once information is verified, the ID cards, pass through quality control, and then are bundled for issuance.

***What are the authentication methods?***

In Tanzania the following authentication methods are in place:

- Fingerprint or PIN matching against central database through Common Interface Gateway and APIs
- Fingerprint matching against smart card
- Secure web portal to access demographic data (NIN + PIN)
- PKI for authentication when online services[11].

***What is the level of adoption?***

- 15.2 million people registered, equating to around 56% of the adult population
- 5.2 million national ID cards issued

[11] See http://www.id4africa.com/2018_event/Presentations/PS2/1-2-2_Tanzania_Alphonce_Malibiche.pdf

- 53 institutions have agreed to access Common Interface Gateway for authentication services through API
- Registration Offices established in all 150 Districts.

## 7.6 United Kingdom

*GOV.UK Verify* is the name of the UK's digital identity project, which was started in 2012 as part of the government's Identity Assurance Service.

The government has made efforts to ensure that *GOV.UK Verify* becomes the national authentication scheme, and not just one used for public sector services, and dialogue has been initiated with banks, insurers and retailers to this end.

The commitment of the British government has been substantial. The budget made available was GBP 150 million for three years of service.

Other features of *GOV.UK Verify* include the capacity to mediate between Identity Providers and Service Providers, thanks to the introduction of an Identity Broker, which offers important benefits:

- Simplification of the integration of Service Providers with multiple Identity Providers.
- Privacy guarantees for users: Service Providers are not able to trace the Identity Provider a user has accessed, and vice versa.

***What was the goal in developing a Digital Identity System?***

To spread the use of digital identity among citizens for access to public services and increase the effectiveness and efficiency of service delivery capabilities of public institutions within the scope of the British National Digital Identity Framework.

***Who is the Identity Provider?***

In UK, the Identity Providers were chosen via tender. To date, eight different Identity Providers exist. The government set the maximum number of Identity Providers at ten, for a duration of three years with an option to increase the service for a further year.

***How are users identified?***

Identity verification is completed online by validating multiple identification documents (eg. passport, drivers license).

***What is the government's role?***

The government chooses the digital Identity Providers by means of public tenders.

***What can digital identity be used for?***

GOV.UK Verify supports the use of digital identities in public services such as:

- Tax services offered by Her Majesty's Revenue and Customs (HMRC)
- Pension services offered by the Department for Work and Pensions (DWP)
- Services offered by the Driver and Vehicle Licensing Agency (DVLA)
- Requests for a basic Disclosure and Barring Service (DBS) check
- Updating of details of rural payments with the Department for Environment, Food and Rural Affairs (Defra).

***What are the adoption enablers (eg. support to citizens or service providers)?***

The UK Government has encouraged the use of digital identity by making it mandatory to access a range of public services such as:

- Tax services
- Pension services
- Services offered by the Driver and Vehicle Licensing Agency

***How is identity proofing completed?***

Identity proofing is performed following a Level of Assurance that requires a claimed Identity to be proofed by virtue of evidence (document validation) supporting the actual existence and said identity. Citizens can register with more than one Identity Provider.

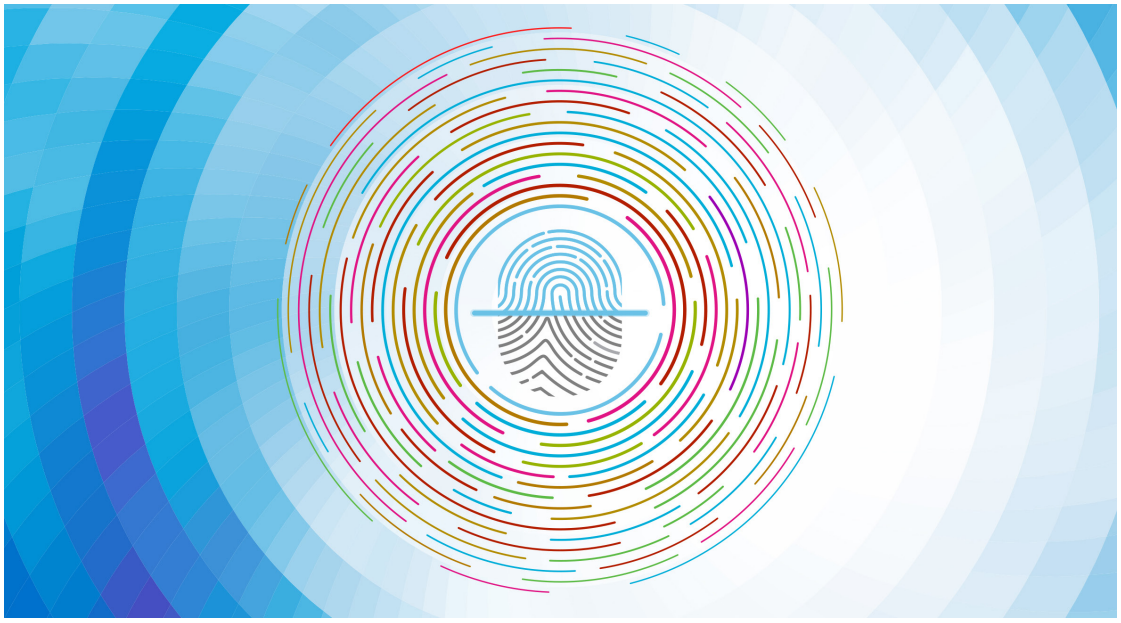
***What are the authentication methods?***

Several methods of authentication are employed: user/password, PIN, biometric, hardware/software token.

***What is the level of adoption?***

In April 2016, when the system became fully operational, there were about 30 services available. The government plans to integrate additional services in the future.

# 8 Conclusions



The discourse around Digital Identity is enjoying a great deal of attention at both the national and international level, and many important global entities – including the United Nations and the World Bank – are developing discussions aimed at promoting Digital Identity Systems.

This document, along with previous studies, demonstrates the value in particular of adopting a national Digital Identity System, which can have powerful beneficial effects on national development – and this is especially true for the least economically advanced nations, where the digitization of services can greatly enhance citizen welfare.

The first step towards adopting an effective nationwide Digital Identity System is the development of a clear, implementable framework. Of the utmost importance, this National Digital Identity Framework provides the structure around which the entire Digital Identity System is planned, designed, implemented, and operated – and can subsequently be improved.

There are a number of different options that governments can adopt, and each has its specific peculiarities. Precisely defining the role the government will play is therefore absolutely fundamental: as governments are, *de facto*, the most involved stakeholders, it is critical that their position is clear from the inception of the programme.

An assessment should therefore be conducted on the basis of the context in which the system will have to be operated. Many elements can influence this assessment, including, among others, demography, the existence (or lack) of previous experience in the field of digital identity, the goals national leaders and policy makers intend to satisfy, and what approach they prefer to pursue (ie. functional or foundational).

Once a government has decided its role, it should take measures to ensure that the Digital Identity System will be adequately adopted. This can be done by leveraging specific elements that promote the use of the system by both citizens and Service Providers. While Service Providers in the public sector can effectively be compelled to adopt the system, the situation for citizens and private companies is less straightforward. Governments can, in certain cases and with limitations, impose adoption on the former; but for the latter the best strategy is to identify the business needs of the necessary actors and help private entities satisfy these needs through adoption of the National Digital Identity Framework.

The approach taken by governments will need to take into account a number of factors, including the number of citizens expected to use the System, how often they might do so, and the total number of services comprised within the System. Success will depend very much on the correct assessment of these factors.

Governments are likely to be confronted by the complex interaction between users and Service Providers. These represent the two main pillars of the Digital Identity System, but they stand on opposite sides of the National Digital Identity Framework, and have opposite and conflicting needs that they expect the System to satisfy.

For users, the System is expected to add value in terms of convenience and the number of services offered – and it is this second aspect in particular that represents the pivotal point behind users' willingness to participate in the System. Governments therefore need to ensure that an appropriate number and an adequate coverage of services can be provided through the National Digital Identity Framework.

For Service Providers, and especially private entities, on the other hand, the opposite is true: before they agree to participate in the System with their services, they want to be reassured there will be enough users to justify the associated technology and human resource costs.

This is a typical example of a two-sided market. Each group benefits from the participation of the other, but one has to initiate the cycle. Governments therefore need to facilitate the situation, by providing support where needed and ensuring that potential inconveniences are minimized. They may, for example, subsidize costs for service providers, or perhaps promote a gradual transition from a fully-governmental service offering to a more variegated one with private service providers.

The functional architecture that national leaders and policy makers decide to adopt is therefore of great importance, and directly influences the stakeholders and actors involved in the system. For this reason, governments need to carefully evaluate their options and pursue models that suit their specific approaches or needs.

Finally, economic aspects need to be considered. For a National Digital Identity Framework to be successful a realistic sustainability goal needs to be set and pursued. Governments therefore need to plan in advance how the framework will be sustained – for instance, internally by generated revenues, or externally by government subsidies.

Ultimately, it is not possible to identify one single model for a National Digital Identity Framework that is better than the others – there is no one-size-fits-all solution, as each country has its own unique characteristics, needs and goals. These elements directly shape how the state approaches the implementation of its National Digital Identity Framework.

Since it is not possible to identify a common implementation strategy *a priori*, governments are strongly advised to consult this guide to obtain the necessary tools to help them evaluate the myriad aspects and elements necessary to design a roadmap toward the implementation of a National Digital Identity Framework. The knowledge provided by this document is the result of in-depth analysis of real cases, enriched by the informed opinion of experts in the field.

The guide provides a summary of the main elements of some sufficiently mature National Digital Identity Frameworks which represent an invaluable source of information that can be consulted to draw lessons-learned about different approaches adopted throughout the world. However, governments should define specific benchmarks according to their own needs.

In conclusion, this guide aims to be a useful support tool giving a general understanding about National Digital Identity Frameworks; on the one hand efficiently informing policy making decisions, and on the other providing operational support during the planning, design, implementation, operations, and subsequent improvements of National Digital Identity Frameworks.

# Appendix 1: Standards

As of today, the topic of national digital identity continues to be widely debated. Various organizations have already tackled certain issues, producing a set of tools that can be very useful when designing and implementing a National Digital Identity Framework.

In the process of developing this guide a stocktaking of existing guides and best practices was conducted. This allowed for the identification of materials already available to support countries in developing their own National Digital Identity Framework, such as technical standards. The list below is a comprehensive, but not exhaustive, catalogue of relevant standards.

**ISO/IEC 29115**

The *ISO/IEC DIS 29115 – Information technology – Security techniques – Entity authentication assurance framework* provides a framework for managing entity authentication assurance in a given context. In particular, it:

- Specifies four levels of entity authentication assurance (LoAs).
- Specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance.
- Provides guidance for mapping other authentication assurance schemes to the four LoAs.
- Provides guidance for exchanging the results of authentication that are based on the four LoAs.
- Provides guidance concerning controls that should be used to mitigate authentication threats.

The Entity Authentication Assurance Framework (EAAF) defines four levels of assurance (LoA) for entity authentication. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity claiming a particular identity (ie., the entity) is in fact the entity to which that identity was assigned.

The actors involved in the EAAF include entities, Credential Service Providers (CSPs), Registration Authorities (RAs), relying parties (RPs), verifiers, and trusted third parties (TTPs). These actors may belong to a single organization or separate organizations. There may be a variety of relationships and capabilities provided by a number of organizations, including shared or interacting components, systems, and services.

The Entity Authentication Assurance Framework (EAAF) provides a model with specific phases and processes; organizations adopting this Framework must establish policies and procedures that provide the necessary supporting processes and fulfil requirements set forth in the Framework. For the content of the document, refer to standard ISO/IEC DIS 29115:2011.

**ISO/IEC 24760-1**

*The ISO/IEC 24760-1 – Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts:*

- Defines terms for identity management.
- Specifies core concepts of identity and identity management and their relationships.

ISO/IEC 24760-1 is applicable to any information system that processes identity information.

**ITU-T X.1253 Recommendation: Security guidelines for identity management systems**

Recommendation ITU-T X.1253 proposes security guidelines for identity management (IdM) systems. The scope of this Recommendation is as follows:

- General IdM system models and services.

- IdM system related security threats and risks.
- Security guidelines for the deployment of IdM systems.
- Security guidelines for the operation of IdM systems.
- Privacy considerations in IdM systems.

The security guidelines describe how an IdM system should be deployed and operated for secure identity services in a next generation network (NGN) or cyberspace environment. The security guidelines focus on providing official advice on how to employ various security mechanisms to protect a general IdM system and also provide the required proper security procedures when two IdM systems are interoperated.

The Recommendation mainly focuses on multi-domain-based identity management services. However, the guidelines are also applicable to a centralized identity management system.

**ITU-T X.1254 Recommendation: Entity authentication assurance framework**

Recommendation ITU-T X.1254 represents the main work upon which the international standard 'ISO/IEC DIS 29115 – Information technology – Security techniques – Entity authentication assurance framework' was built. It is a crucial document, as it represents the first organized attempt to structure specific levels of authentication assurance with their related framework.

**ITU-T X.1255 Recommendation: Framework for discovery of identity management information**

The purpose of Recommendation ITU-T X.1255 is to provide an open architecture framework in which identity management information can be discovered. The core component of the framework include: 1) a digital entity data model, 2) a digital entity interface protocol, 3) one or more identifier/resolution systems and 4) one or more metadata registries.

# Appendix 2: References

**International Telecommunication Union publications**

International Telecommunication Union, *Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security*, ITU 2018.

International Telecommunication Union – Telecommunication Standardization Sector, *X.1252 "Baseline identity management terms and definitions"*, April 2010.

International Telecommunication Union – Telecommunication Standardization Sector – Focus Group on Financial Services, *Identity and Authentication*, January 2017.

International Telecommunication Union – Telecommunication Standardization Sector – Focus Group on Financial Services, *Main Recommendations*, March 2017.

**Other documents**

Prasanta Sahu, *Direct Benefit Transfer: Savings up 58% to Rs 32,984 crore in FY18*, June 2018, https://www.financialexpress.com/economy/direct-benefit-transfer-savings-up-58-to-rs-32984-crore-in-fy18/1193744/.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)".

Unique Identification Authority of India (UIDAI) Planning Commission, Govt. of India, *UIDAI Strategy Overview. Creating a Unique Identity Number for Every Resident in India*, April 2010.

Unique Identification Authority of India (UIDAI), *AADHAAR E-KYC API Specification*. Version 2.5, March 2018.

World Bank, *Principles on identification for sustainable development: toward the digital age,* February 2018.

World Bank, *Private Sector Economic Impacts from Identification Systems*, 2018.

World Bank, *Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints*, 2018.

**Web links**

https://dbtbharat.gov.in/

http://oman.om/

https://www.attendance.gov.in/

https://www.eid.as/home/

http://www.pmujjwalayojana.com/

https://www.uidai.gov.in/aadhaar_dashboard/ekyc_trend.php

https://uidai.gov.in/authentication/authentication-overview/authentication-en.html

International
Telecommunication
Union
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-27831-1

Published in Switzerland
Geneva, 2018