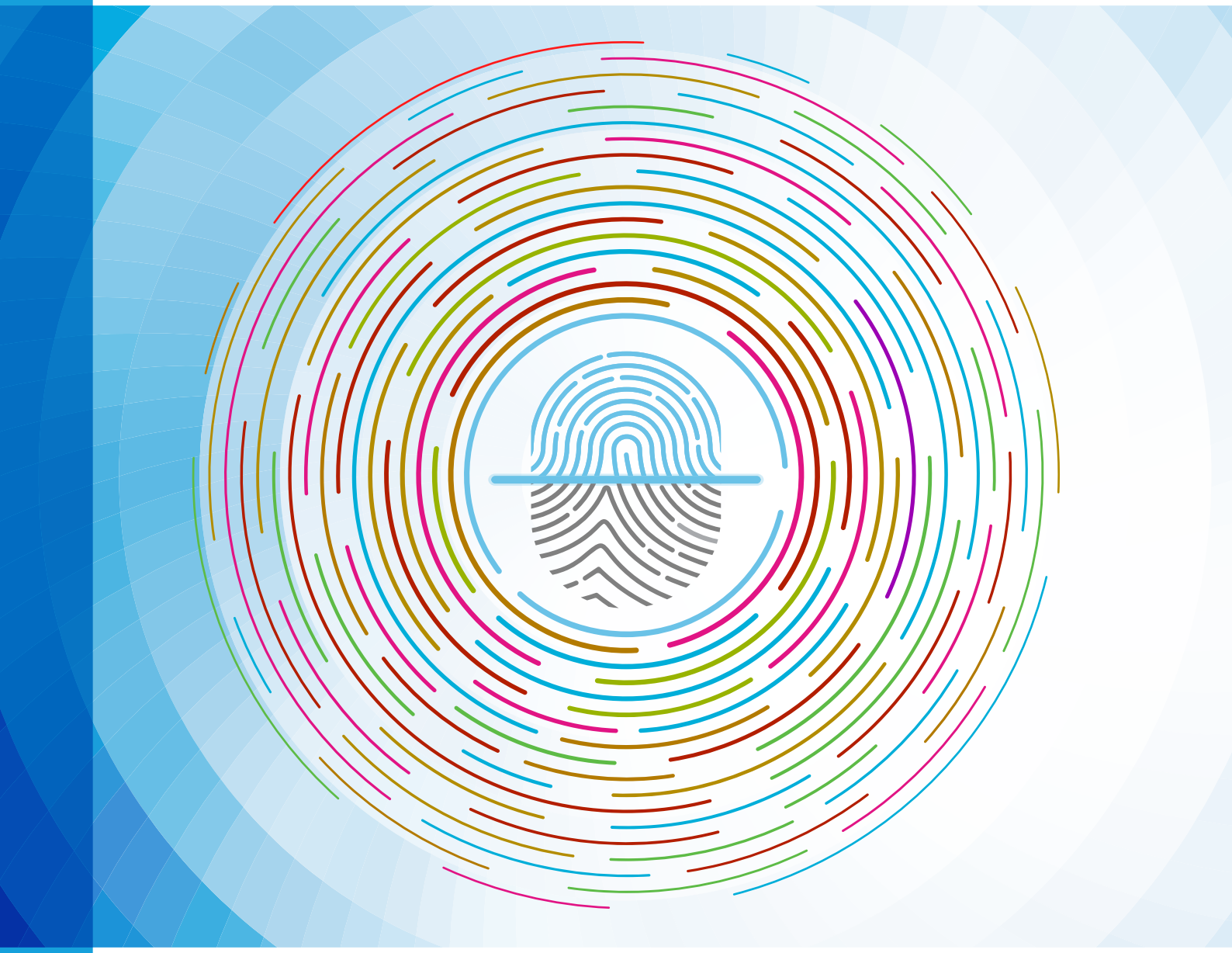
Digital Identity Road Map Guide



Digital Identity Roadmap Guide

Acknowledgments

This Guide was developed by an international team of experts from different governmental institutions and International Organisations, and private sector and included the following organizations.

The team included Ram Sewak Sharma (India), Deepti Vikas Dutt (India), Yahya Salim Rashid Al Azri (Oman), Alphonse Malibiche (Tanzania), Kemal Huseinovic (ITU), Marco Obiso (ITU), Hani Eskandar (ITU), Nancy Sundberg (ITU), Dorina Xhixho (ITU), Andrea Rigoni (Deloitte), Lorenzo Russo (Deloitte), Alessandro Ortalda (Deloitte).

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

Boxes

Preface

The Digital Identity Roadmap Guide is a comprehensive guideline useful 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 and thorough multi-stakeholder effort aimed at strengthening the knowledge and the expertise of the audience working with digital identity and, more generally, digitalisation of governmental and State services.

The value that can be derived from digital identity applications is potentially enormous, and can be a significant force in promoting a more inclusive and efficient national and transnational digital environment. The objective of this Guide is to provide a specific support to all national leaders and policy makers during the creation lifecycle of the Framework.

1 Document Overview

1.1 Purpose

The purpose of this document (hereinafter, also the "Guide") is to guide national leaders and policy makers in developing a National Digital Identity Framework. In order to achieve said goal, this Guide provides a comprehensive vision about the main elements, aspects, and principles related to the notion of digital identity in a national context.

By reading this documents, national leaders and policy makers will obtain the knowledge to understand the basic concepts of digital identity and how they apply in a national context. From this premise, they will have the competence to take concrete steps toward a wide range of initiatives in the field of digital identity, pursuing different outputs such as a National Digital Identity Strategy, policies, law and norms, technological implementation, etc. Through these projects, States can pursue social and economic advantages for both the private and the public sector, and bring deep benefits to their citizenship.

The Guide is a unique resource, as it provides a framework that benefits from a demonstrated and diverse experience in this topic area, and builds on prior works in this space. As such, it offers the most comprehensive overview of what constitutes successful digital identity meaning to date.

1.2 Scope

Digital Identity is an enormous and complex challenge that encompasses multiple aspects. It touches upon areas such as governance, policy, operation, technology, and law. Therefore, it is necessary that national leaders and policy makers deeply understand the topic.

This Guide focuses on to transfer the fundamental notions and overarching principles regarding digital identity in order to help correctly assess the context in place and plan the necessary steps to develop and manage a National Digital Identity Framework.

At the same time, the reader is advised that the present document does not elaborate on single and specific technical aspects. The goal of the Guide is not to provide a list of the technological solutions available. Rather, it gives the reader the necessary theoretical tools that can be employed to design a National Digital Identity Framework capable of answering the main and most pressing necessities of States.

There are a number of organisations that already addressed the topic of national digital identity. The present Guide is not intended as a concurrent tool to these documents. Rather, it aims at positioning itself together with these other efforts, bringing clarity and filling the gaps that inevitably exist in such a vast and complex research area. Therefore, it is strongly suggested to read this Guide in conjunction with other materials that already exists. Section 7 of the document lists some of the most prominent ones. However, it is worth mentioning that this field of study is advancing at a quick pace. It is therefore crucial that readers remain updated on the main innovations and advancements in the field.

1.3 Overall Structure and usage of the guide

This Guide is intended as a resource to help national leaders and policy makers in developing a National Digital Identity Framework. As such, the content is organised as follow:

- 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 in the development of a National Digital Identity Framework during its full lifecycle;
- Section 6, Critical success factors and conflicting principles, enunciates the factors that might enhance the success factor of a National Digital Identity Framework, and those that, instead, have the potential to slow down the process forcing national leaders and policy makers to exclude certain conflicting aspects in favor of others;
- Section 7, Supporting Reference Materials, provides further pointers to relevant literature that stakeholders can review as part of their drafting effort.

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

The Guide can be valuable for different stakeholders as well, mainly in the international development community, who provide assistance in National Digital Identity Framework.

2 Introduction

2.1 What is a Digital identity

2.1.1 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, it is possible to state that a digital identity is the digital representation of an entity, detailed enough to make the individual distinguishable within the digital context.

Identity is a crucial element for each individual as it defines and identifies the main traits of each and every person. Obviously enough digital identity is equally important. It retains the intrinsic characteristics that make identity such a defining factor and, at the same time, can be seen as a tool that States and Governments can leverage on to meet the demands of their citizens, or to improve their overall efficiency.

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

2.1.2 Elements of Digital identity

As stated in the definition 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 be considered as the building blocks of a digital identity. They can be divided into different categories such as birth-related information (name, place of birth, date of birth, etc.), descriptive information (height, weight, physical traits, etc.), personal identifiers (e.g. social security number), biometric data (fingerprint, DNA, iris, etc.), etc.

2.1.3 Categorisation of Digital identity

Although the concept of digital identity identifies a specific object (as defined above), this can be categorised into three main categories that can help to 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 the 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].

---

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.
3 Ibid.
4 Ibid.
5 Ibid.

These three categories can help to understand 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

A successfully implemented National Digital Identity Framework has the potential to introduce a wide range of benefits for the State and its citizens.

2.2.1 Potential benefits for the users

2.2.1.1 Improving the convenience for users

One of the most prominent benefits that users can have from participating into a National Digital Identity Framework is the great improvement in their convenience. Digital identity represents the means through which users can effectively remove some of the barriers that often make public services complex and difficult to be accessed. First of all, with the capabilities offered by their digital identities, users do not have to be physically present in most of the cases. Secondly, by adopting online-service delivery approaches, users are likely to benefit from 24/7 availability of services.

2.2.1.2 Reducing costs of the access to services

Thanks to the higher convenience and flexibility, users will have the chance to cut the indirect costs of accessing to the services. For instance, working citizens will be relieved by the burden of taking days off in order to complete bureaucratic procedures, they will have to manage a considerably lower amount of paper personal documentations, etc.

2.2.1.3 Improving inclusions for citizens

Thanks to digital identities, people who might not be able to obtain identity documents will be able to participate fully to their communities, despite the lack of physical documentation. Therefore, they will be able to perform actions such as opening of bank account, getting a mobile connection or getting social security benefits.

2.2.1.4 Service delivery improvement

One of the most important benefits that can derive from a National Digital Identity Framework is the improvement of the condition of the society at large and citizens. A fully functioning system of digital identity means that States will be able to more efficiently deliver their services to the citizenship. In particular, it will help institutions to target the population with welfare and social programs. The system will effectively empower Governments with the necessary tools to timely and efficiently intervene in the least accessible and most remote area, ensuring that the entire community benefits and grows together.

Moreover, Governments and the public administration will see a reduction in leakages due to duplicates and ghosts in beneficiary databases of various social assistance programs, further increasing their effectiveness and efficiency.

2.2.1.5 Reducing cost of service delivery

Likewise the reduction of costs for the private sector, the public sector benefits of costs cut as well. Together with a better and more efficient service delivery it comes a reduction of the costs necessary to perform services for the community. The adoption of digital identity is a prominent aspect of the digitalization of the public administration. This leads to cut in expenses that will free resources for the

Government. For instance, it will help to greatly lower the amount of paper documents employed, or it will increase the productivity of the public administration thanks to the fact that less in-person services will be delivered (without lowering the quality of the services offered).

2.2.1.6 Improving security

Digital identity can also increase the level of security of the State. Indeed, this can be a power tool for policing and crime prosecution, and can greatly increase the effectiveness of combating certain specific crimes (such as identity frauds, tax frauds, etc.).

2.2.2 Potential benefits for the private sector

2.2.2.1 New revenue opportunities for public and private

By leveraging on the digital environment created by the digital identity system, both the public and the private sector might be able to come up with new and innovative revenue streams, kickstarting a virtuous cycle that will help the whole economy to thrive and grow thanks to this new assets.

2.2.2.2 Reducing cost of service delivery

Private companies and entities providing services through a National Digital Identity System are likely to benefit from a decrease in the costs they have to sustain in order to delivery said services. Reducing personnel, physical delivery points, paperwork, and the time needed to complete each user's request are just a few of the examples of cost-cutting initiatives that can be launched by companies with the aim at lowering their expenditures.

2.2.3 Potential benefits for the Government

2.2.4 Potential pitfalls

While National Digital Identity Frameworks carries the potential of many benefits, it is important to remember that they might incur in certain pitfalls, when not adequately designed and implemented. Some of the most critical pitfalls are:

- Security and privacy: the vast amount of data required exposes the system to a number of threats coming from the digital world, such as hacking and data breaches;
- Sustainability: as a costly feat, a National Digital Identity Framework might easily fail if no adequate resources are 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 the document touch upon the most relevant 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 a 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 the goals it aims to pursue, and a mission detailing how to reach said goals.

One of the most crucial success factor for a National Digital Identity Framework is to set a clear vision associated to it. This helps all stakeholders to understand what is at stake and why the National Digital Identity Framework is needed (context), what it is to be accomplished (objectives), as well as what it is about and who 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 amongst the relevant stakeholders. It should be formulated at a sufficiently high-level and consider 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 organisation plans to pursue the changes set out in the vision. However, a mission should not be excessively detailed in order to avoid losing the necessary flexibility required by 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 but a complex multi-faceted activity. It has ramifications into many and different areas such as the development of the economy, social prosperity, law enforcement, national security, etc.

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

The priorities included in a National Digital Identity Framework will vary State to State.

3.3 Social Inclusiveness

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

The digital environment has become critical to Governments, businesses, and the society in general. This last group comprises a variegated set of sub-groups with very different characteristics and

peculiarities. Among these sub-groups, certain individuals might be identified as particularly weak or in need of protection. Elderly people, minorities, and low-income families are just few examples.

A NationalDigital Identity Framework should be designed so that all the members of the community can benefit of its services, without excluding weak individuals (who might have, for instance, a lower digital literacy or access to digital devices).

3.4 Economic and Social Prosperity

The National Digital Identity Framework should foster economic and social prosperity and maximise the contribution of digital to sustainable development and social inclusiveness.

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

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

The role of digital identification 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 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.

This can generate many benefits, but 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 the identification 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

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

The National Digital Identity Framework should recognise the fact that rights of people must be directly translated and protected also in a digital environment. It should respect universally agreed fundamental rights, including, but not limited to, the ones 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 or processing of personal data.

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

3.6 Resilience

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

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

For this reason, the National Digital Identity Framework should be designed in a proactive manner and 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

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

Clear and effective privacy and data protection measures should be defined within the National Digital Identity Framework. The whole process of data collection, integration and management should be underpinned by legal frameworks and procedures that clearly specify the treatment of the different sets of data and under what conditions, ensure that users retain adequate control over their data, and include robust security measures to ensure data protection.

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 may be able to increase trust in government, with a variety of benefits. For example, a trusted identification system may reduce the likelihood that election results are disputed, thereby decreasing risk of 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

The National Digital Identity Framework should be operated in a flexible and scalable manner and ensure that it can be promptly and efficiently modified or updated when necessary.

The need of flexibility and scalability could be relevant in many cases. The number of States involved will increase over time and the same coverage within a single State will be progressive, especially in

case of States with large populations. In the same way, conditions of application and usage of digital identity will evolve, driven by technological evolution and social progress.

Thus, the 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

The National Digital Identity Framework should take into account the role of interoperability as the ability of different systems to talk to each other, exchanging information and queries.

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

Moreover, a high level of interoperability contributes to reduce operating costs within a State's identity ecosystem and foster administrative savings when countries are able to create an identification system with enough coverage and interoperability aimed to rationalize duplicative functional systems.

3.11 Speed of deployment

The implementation and deployment of the National Digital Identity Framework should follow a swift and schedule.

The speed in which a National Digital Identity Framework is deployed should be quick and steady 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, undermining the overall effectiveness of the services associated to it.

3.12 Identity as a platform

The 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. This approach opens the possibility to employ the digital identity environment as a platform to aggregate a variety of different and interrelated services, greatly improving the speed of adoption.

This can also lead to savings, when States are able to create a foundational identification system with enough coverage and interoperability or integration to rationalize duplicative functional systems. Cost savings takes place, for instance, using foundational registers and credentials to underpin voter lists, thereby reducing the costs of voter registration and/or eliminating the need for separate voter ID cards. Moreover, a foundational unique ID linked with the tax database can help improve taxpayer identification, potentially broadening the tax base and improving compliance.

3.13 Uniqueness of IDs

The National Digital Identity Framework should ensure that people are able to get only one ID.

A fundamental attribute of robust identification systems is not only the ability to establish the existence of individuals in a given jurisdiction, but also their uniqueness.

A unique identifier is an identity attribute that uniquely identifies a person or entity within a given population. In other words, 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 identifications employed, uniqueness of IDs should be pursued and ensured (i.e., ensuring users have not registered in the system multiple times or under multiple names), thus avoiding duplication and ghost users.

Furthermore, the creation of a unique identifier for each individual within the population can increase transaction efficiency and reduce opportunities for fraud.

3.14 Robustness and future-proofing technology

Technologies and systems described in the National Digital Identity Framework and used for the creation of Digital IDs should be robust and scalable, ensuring at the same time that they are future-proofed and do not get obsolete very soon.

A crucial condition for savings and revenue is the level of robustness in the identification system. 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, another key condition concerns the guarantee that developed systems and adopted technologies prove to be adequate over time and not get obsolete very soon, in order to assure a certain level of continuity to the whole process.

3.15 Data quality

The National Digital Identity Framework should be the base for other programs of national importance. Thus it is critical that steps are taken to ensure data quality at multiple levels.

Data quality and accuracy is first of all assured by establishing a unique identifier—e.g., 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 agencies that leverage 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 precede and 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 a set of elements that can ensure the appropriate level of comprehensiveness and effectiveness for the National Digital Identity Framework, while allowing a tailor-made design for its national context.

These good practice are grouped into four distinct focus areas representing the overarching themes for a National Digital Identity Framework. While both the focus areas and the elements have been put forward here as examples, it is particularly important that the latter are viewed in the national context, as some may not be relevant to a country's specific situation. Countries should identify the models that support their own objectives and priorities in line with their vision.

Lastly, it is important to stress that the order of the individual focus areas 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 for governing a National Digital Identity Framework:

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. The analysis of the currently 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 on the initiatives associated with the issuing of identity cards – combining the issuance of a Digital Identity. Others, instead, 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 experience and capabilities.

This section focus solely on the role of the Government, regardless of the number of other stakeholders involved (e.g. the number of service providers).

4.1.1 The Government is directly involved as Identity Provider

Governmental approach to digital identity can be either a "Buy" approach or a "Make" one. Both the approaches offer a secure and convenient digital identity to citizens. The 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 term of operation of the Digital Identity Lifecycle, from identity proofing to credential management, the authentication of identities, the integration with service providers, and the revocation of digital identities.

This option has both benefits and disadvantages. While it is certain that the Government might leverage on certain qualities, like its local presence on the territory, or other programs/initiatives already in place (like Identity Card program) or a more present control over the whole system, it also holds true

that this approach might not take advantage of the experience in managing digital identities gained over the years by third parties such as Telco Operators or Banks, or the ability to deploy a systems in a fast way leveraging experience, capabilities, and even user base.

Estonia is one of success cases of adoption of this model. The system introduced in 2002, currently has a coverage close to 98% on a total population of 1.3 million[1].

It is based on the use of electronic identity card, ID card, used as a comprehensive proof of identity in a digital and physical context. There are currently countless of uses, both in the public and private sectors. For instance, it can be employed as proof of identity when accessing bank accounts, to apply digital signatures, and to access public administration services (e.g. access to medical records, the tax situation, etc.).

Another prominent examples of this approach are India and Tanzania. For instance, in India, through its Asdhaar program, the Government acts as Identity Provider. In less than 5.5 years it has achieved 1.2 billion digital identities. In these cases, since the digital identity is provided directly by the Government, it can be seen as a more reliable and trusted digital identity for every-day use across multiple governmental services and other large scale programs such as banking and telecom.

It is important to point out that the option to act as Identity Provider in the National Digital Identity Framework does not completely prevent any kind of private involvement, thus letting to the governments taking advance of experience and capabilities of system integrators as identity management providers. A government in fact can develop and implement the system by itself , or more commonly engage a third parties for the deploying the technical solutions, maintaining de facto its Identity Provider role.

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

The section explores the scenario in which the Government acts as Regulator of the National Digital Identity Framework and buyers of the digital identity providing services. The model implies that other entities are engaged in managing the digital identities of the citizens. As anticipated, this model is commonly referred as the “Buy” model since it requires subsidies from the Government aimed at rewarding the third parties for the costs sustained and the service offered.

The Government has, on one hand, the role to regulate and control 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. This activities require specific attention as, in order to distribute its services, the Government requires a high level of Identity Proofing, usually the highest, that is “Proofing in person”. This requirement is due to the level of assurance that the Governments have to guarantee according to the international and national laws and regulations, ensuring it is at the same level of the issuance of physical identity documents (e.g. Passport).

On the other hand leveraging a service provided by third parties in particular when this is leveraged for accessing public digital services, requires subsidies from the Government aimed at rewarding the third parties involved for the service provided (e.g. 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 a clear expertise and capability in the field.

The Canadian government's initiative is one of the success cases of adoption of this model. Named SecureKey Concierge, it saw the creation of a system consisting of an Identity Broker and a set of Identity Providers. These has been selected among entities having a considerable number of identities already verified with a high level of assurance (e.g. banks) and already equipped with digital authentication solutions.

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

The goal has been to provide a method of identification and authentication – alternative to the one already offered by the Government – to access the services of the public administration, based on a "bring your own credentials" (BYOC) model where users are enabled the use of credentials that already have and use.

The Government signed a contract to an Identity Broker, SecureKey, which is a consortium bringing together some of the largest Canadian banks (at the inception of the system there were three of them; today they are five) that have already verified identities of the customers and provided them with already teste and secure means of authentication.

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

The 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. The model is very similar to the previous one but to this it adds an active role of the 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 of vice versa.

The English initiative, Gov.uk Verify, dates back to 2012, part of the government program Identity Assurance Program, is one of the success cases of adoption of this model. In that year, 5 Identity Providers were selected through a European tender. The selection was repeated in 2015, extending the maximum number of operators to 10, for a duration of three years with an option for a further year. Currently the Identity Providers are 8. The model requires that the Government makes use of and repay the Digital Identity providers, allowing citizens access to the digital services of the public administration. Access to public services is intermediated by the Government acting as identity Broker, with the goal of facilitating communication between Service Providers and Identity Providers by placing itself in the middle.

4.2 Focus Area 2 – Approach for adoption

The success of a National Digital Identity Framework is demonstrated by the level adoption among the involved stakeholders. The *level of adoption* refers more generically to multiple objectives that can be achieved: percentage of citizens who have a digital identity to population, number of public and private services able to offer services through the use of digital identity, number of accesses to digital services.

To achieve these challenging goals, it is crucial to address the needs and expectations of the two primary entities involved in a Digital Identity System: users (citizens) and Service Providers. The system is a *de facto* classic example of Two-sided Market where the needs and necessities 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, instead, require a large user base. Being able to successfully manage these different needs creates a virtuous circle, where more demand from one group stimulates the demand of the other.

The next sections describe the most important elements to be considered to foster/promote the participation of citizens and Service Providers.

4.2.1 Approach for fostering adoption on citizen-side

4.2.1.1 Value of digital identity usage for users

The first and one of the most critical drivers for citizen adoption is the real value in terms of public and private services that can be accessed with a digital identity. Even if a relevant percentage of users has an issued digital identity, the success of an initiative is demonstrated by the services that can be accessed by citizens and the number of accesses completed.

For this reason, Governments should consider promoting the participation in the system among public administrations so that real value can be provided to the citizens. The 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;
- Tax services;
- Pension services.

These can represent a key driver to foster citizen adoption. At the same time, extending the accessible services to private ones can further increase the interest in using digital identities among the citizenship. Estonia, for example, allows the usage of digital identities to a huge number of providers, belonging both to the public and private sectors.

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

A different strategy sees the Government forcing the user to adopt a digital identity as a mandatory means to access digital public services. This approach has the potential of providing a major boost to adoption. In Oman, for example, the Omani Information Technology Authority has achieve an extensive adoption leveraging the mandate by the highest authority, Ministers' Cabinet that required the access to digital public services by the National Digital Identity Framework. The same approach has been adopted in Tanzania where the adoption has been encouraged thanks to the Government's action that made it mandatory to access a series of public services with digital identity such as:

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

4.2.1.2 Issuing of digital identity: voluntary vs mandatory

Another driver for adoption is related to the voluntary or mandatory nature of having a digital identity. As anticipated, this represents a determining element, perhaps not the most decisive among those that can decree the success of an initiative but certainly among those that can foster the adoption.

Essentially, two different approaches can be adopted for issuing of digital identities: Voluntary vs Mandatory based:

- **Voluntary-based**: the decision whether or not to have a digital identity is demanded to the citizens themselves. In this scenario, citizens must be encouraged to request a digital identity because it represents their key to access to a series of services. India, through its Aadhaar program, has adopted this approach. Citizens are not force to hold an Aadhaar-issued digital

identity. However, they must own one in order to participate to certain limited specific national or governmental welfare or social programs (i.e. social benefits);

- **Mandatory-based**: this approach does not allow the citizen to decide whether or not to request a digital identity. The approach is usually adopted in combination to initiatives where the enrolment of digital identity is contextual to that of ID documents. Forms of mandatory own of digital identity become decisive for promoting the adoption, but they do not guarantee a usage if it is not combined with an extensive service offering. Estonia has established a system which provides State-issued digital identities almost to the entirety (current figures stands around 98% of adoption) of its citizens. Citizen can access to a suite of services as e-governance, healthcare, security and safety, business and finance, education services.

  While this method has been extremely successful for Estonia, it can be challenging for those countries that don't manage national ID cards or see politically tough to manage the two identities – digital and physical – together.

4.2.1.3 Convenient enrolment process

Citizens have to complete the enrolment process in a convenient way, limiting the complexity and effort required. A decisive aspect is represented by the level of identity proofing required. Identity proofing is the method used to certify user authenticity prior to providing the credentials necessary to access the digital services. Identity proofing has 4 different Levels of Assurance (also, LoA), as commonly identified in international standard as ISO/IEC DIS 29115:

- 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 of what contemplated in the previous case.

Governments' initiatives require a high level of identity proofing, mostly the highest one, that is "Proofing in person". These can never rely on "Self asserted" digital identities. This requirement is due to the level of assurance that the Governments have to guarantee according to the international and national laws and regulations, ensuring it is at the same level of the issuance of physical identity documents. High levels of identity proofing, however, require more controls and, often, the need to visit a Government office or authorized one. 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 process and technicalities for proofing there are different approaches to the identification adopted as In person identitfication vs. Remote identification. In the first case, the government authorized entities (as public officials) verify the identity of the citizens *de-visu*. This approach offers a greater level of assurance, but entails certain complexities for the citizens and the Identity Providers alike. Citizens have to go to an office visit and the Identity Provider has to set-up multiple offices to complete the identity proofing. The second case – Remote identification – is commonly associated to the idea of provding 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 (e.g. face recognition, video anti-tampering), even though there is no consensus between experts on the comparison in terms of assurance between the two approaches. On the other hand the remote identification is considerably more efficient than the first one.

4.2.1.4 Levering other digital identities systems

In most cases, citizens already have digital identities that they use, for example, to access the services of banks, telecommunications, energy suppliers, etc. For that, they have already been verified and own authentication tools that are regularly used. Banks and telco operators in particular manage identities that required higher level of trust – as for Governments required – due to the type of service offering (mortgages, loans, etc.), which encompass transactions of higher value or due to the compliance to industry sector laws (Anti-Money Laundering or registration SIM). For this reason, Governments can look to the involvement of private entities to allow citizens to access into governmental services via their familiar online sign-in process, leveraging identity already verified.

Multiple benefits can achieve as for example:

- Governments leverage a significant number of already verified active users;
- Users' convenience is enhanced as the risk of forgetting credentials is minimized. Citizen typically don't access government services online, on a daily basis. For this reason users forget passwords for sites they don't visit regularly. Private operator's Identities are used instead on a regular basis reducing therefore this type of issues. This also lowers the number of credentials users will have to manage;
- Governments reduce efforts and costs related to credentials 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 one set of credentials for banking and Government access, the Canadian Government helps citizens maintaining fewer, higher quality passwords than before, simplifying customers' experience. The citizens don't have to remember multiple sets of credentials, and can use a single one instead. Governments are willing to involve other entities for authentication services that they can't provide simply because users visit their sites too rarely. Moreover these entities could provide new services based on its credential management.

This approach instead is not applicable or successful in those countries where there are many unbanked citizens. A critical mass of users can be achieved. More therefore the level of social inclusiveness is limited as citizens allows to access to digital services are limited to ones with a private identities if there are not deployed alternative solutions.

4.2.1.5 Usability

A National Digital Identity Framework should aim at achieving the highest level of usability possible. Indeed, a system that is complex to operate for the users will have far lesser chances to experience a full participation of the citizenship and users in general.

To make a National Digital Identity Framework effective, the design of its processes, components, and systems should be done taking into account the principles of simplicity and immediacy for access. No advanced skills should be required for 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 digital aspects, such as the elderly and people with a general lower level of computer literacy.

Extending the concept to interoperability, users can see a value in the possibility of recognizing your identity on multiple platforms and / or domains without the burden of having to enter more credentials or use multiple authentication tools.

4.2.1.6 Security and privacy

Citizens demand for a simple, convenient, and secure use of digital identities. Protection of identity from abuse, compromise and fraud through certified solutions and services with a proven reliability is

a crucial driver for adoption. At the same time guaranteeing transparency in terms of data processing must be is a goal to be achieved.

Security is a complex multi-faceted aspect that touches upon many different elements. Defining specific security-related and privacy-based objectives from the beginning of the digital identity program, enables to consider security and privacy across the entire digital ecosystem.

Governments should adopt specific actions aimed at ensuring that citizens and service providers can benefit of the maximum achievable level of security. Indeed, there are multiple security risks related to different phases of a Digital Identity Lifecycle that needs to analyse through an accurate threat profile starting from core processes as:

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

At the same time, multiple stakeholders are involved: citizens, identity providers, service providers, brokers, etc. therefore, national leaders and policy makers should adopt a security by-design approach, which ensures that the digital identity system is adequately secured against external attackers and internal abuses. Consequences of an incident might have destructive impact on the level of trust associated to the system.

The other crucial element that has direct impact on the trust level given to the system is the safeguard for the privacy of the users. The recent introduction of norms such as the European Union General Data Protection Regulation[2] reveals a strong attention that legislators and the society in general have on the topic.

Since the use of services that rely on digital identity entails the sharing of certain amount of personal data, sometime being of a very sensitive nature (such as biometric data), national leaders and policy makers should make an effort to reassure users that privacy is respected at every step of the process, through a privacy-by-default approach.

One of the way to ensure that data privacy is more easily managed and maintained is to introduce in the system a broker/manager for the digital identities. Canada, for instance, adopted this approach. In its 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 users' privacy. Users can be confident that banks cannot see what they are doing online; the government cannot see the user's banking details; and the Concierge service is not aware of the user's identity.

Promoting an open and transparent approach about how data are processed, stored, deleted, shared and about the rights users have in relation to the management of their personal data is therefore very important for 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 are managed transparently, with clear communication about how it is used and shared;
- The Identity Provider does not have access or knowledge about the services the user is adopting;

[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)"

- The Government does not have access or knowledge about the identity provider the user decided to adopt (applicable only when multiple identity providers are present);
- All the identity providers and service providers have to meet government and international standards for security and data protection.

4.2.1.7 Communication and awareness for the citizenship

All of the elements previously described need to be presented to the citizens.

Governments need to constantly promote the digital identity initiative and its benefits to the citizens, taking into account the different target audience. They have to assess the context and decide on a communication strategy. Suffice here to say that this is an often overlooked element that, when is not correctly managed, can gravely impair the success of the initiative.

4.2.2 Approach for fostering adoption on service providers-side

4.2.2.1 Promoting or forcing the public administration participation

As anticipated, the success of a National Digital Identity Framework is demonstrated by the number and extension of services that the citizens can access, both public and private. Governments' action should aim at involving public and private digital service providers, according to their Digital Identity Strategy and related objectives.

As presented in the previous sections, Governments' actions with the public administrations can be facilitated by the role as regulator that the Government has for specific sectors. The approaches can include forcing the participation or promoting it.

Governments might request an exclusive access to digital public services with digital identities. This requires the service providers' to replace their identity management systems with those adopted at the Nationa levelintegration. What might appear to be a simple operation at first glance, requires instead a careful design of the digital Identity systems employed, a focus on the integration and interoperability taking into account standards that can facilitate it, the planning in terms of deployment in the light of the central role that the identity system plays. Examples of success cases are Oman or Tanzania. In these initiatives the State provides public services that can be accessed only to users that have a digital identity.

Other countries have adopted a different approaches where there are no services that can only be accessed via digital identity. This option implies that physical or traditional identity systems are offered as alternatives, working in parallel. Even if Service Provider's participation to the identity system is mandated by the Government, this approach limits the action of accelerator towards citizens' adoption.

4.2.2.2 Engaging with the private sector operators

Service providers play a crucial role for the success of a National Digital Identity Framework. Extending the service offering to private sector can be seen as a compelling driver for accelerating the adhesion of citizens. It is therefore crucial for facilitating this participation of private Service Providers to the National Digital Identity Framework to provide real advantages or cost reduction. These private providers decide upon their participation in the system based on a cost-benefit analyses.

As said a National Digital Identity Framework encompasses high levels of identity proofing (i.e. verification in person) to the benefit of the public Service Providers. 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 compared to the one from the Government. E-commerce operators do not have the same needs (e.g. self-declared identity for payments for which a credit card is appropriate) of

banks and financial operators, which have more critical transactions (e.g. opening accounts, request mortgages) and compliance obligations (anti-money laundering or SIM registration).

	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 can be considered to support the cost-benefits analysis:

- Contribution to value:
  - Leverage faster a larger user base;
  - 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 (e.g. 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;
  - Being able to customize the experience through qualifying attributes;
  - Let them focus on their core offering, due to reduction of involvement in non-core services;
- Cost reduction:
  - Reduce costs associated with identification proofing processes;
  - Reduce costs associated with credentials management;
  - Reduce costs for starting and managing new services.

4.2.2.3 Introducing 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 the participants.

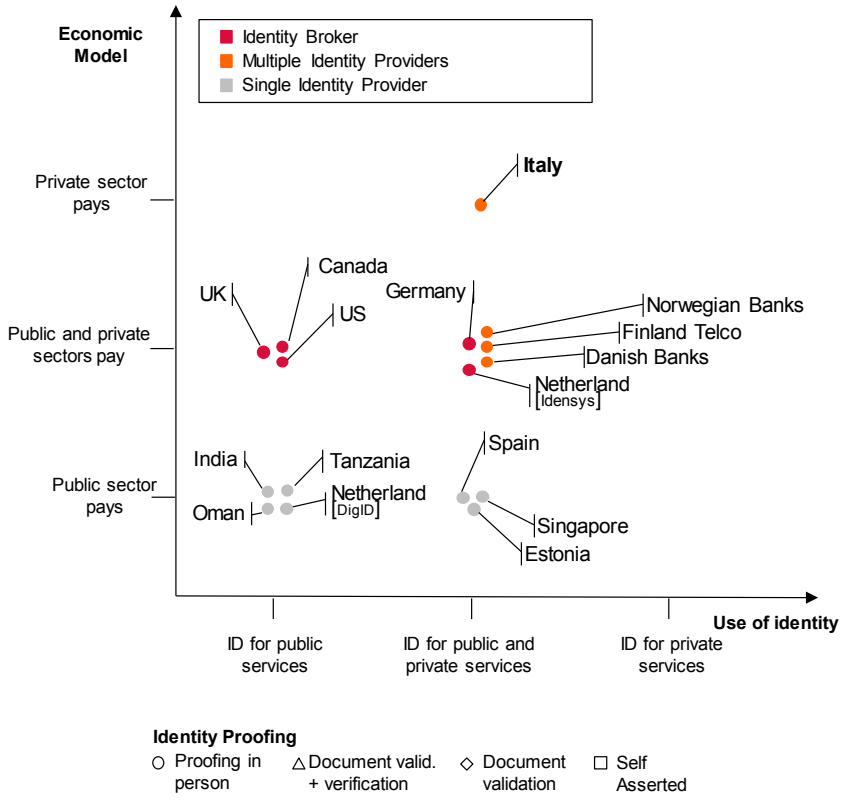
This element is a key facilitator in particular when there are multiple Identity Providers that need to be integrated with multiple Service Providers. This is even more crucial when small and medium public or private providers are willing to be engaged.

The primary benefits of introducing an Identity Broker are related to:

- Identity Providers and Service Providers have to sign, define single agreement with the Broker/s despite bilateral agreements with all the entities involved. Moreover the broker provider can act as clearing house can log the transactions or usage of identity and proceeds with the invoices to Service Providers and the payment of Identity Providers;
- Easy technical integration with just one entity – the Identity Broker – reducing efforts and time;

- Extended privacy assurance.

Success case of adoption of Identity Brokers are conducted, for example, in UK, Germany, Canada and US where one Identity Broker is implemented. In The Netherlands, the revisited National Digital Identity Framework, Idensys, contemplates even multiple Identity Brokers at the national level.



4.2.2.4 Fostering Federation of Identity Providers

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

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

4.3 Focus Area 3 – Architectural model

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

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

Three different architectural models are adopted for Digital Identity System:

- One unique Identity Provider
- Multiple Identity Providers

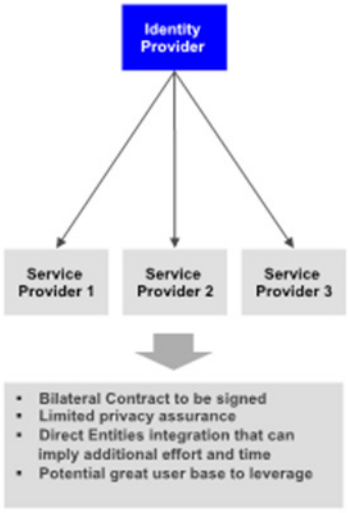
- Identity Broker/s with Multiple Identity Providers

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

4.3.1 One unique Identity Provider

The section explores the scenario in which only one entity is authorised to provide for digital identities.

In centralised identity systems, a single entity acts as an Identity Provider that authenticates users to Service Providers and transfers 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 is accountable for the identity proofing of the citizens. It holds users' credentials and attributes;
- The Identity Provider is accountable for the authentication of the users that are allowed to access digital services of multiple Service Providers, public and private. A set of defined attributes is transferred to Service Providers to enhance the personalisation of services and efficiency of processes;
- When this architecture is adopted the Government is directly involved as Identity Provider;
- Private service providers participation is allowed subject to criteria compliance and fee payment;
- Privacy is limited compared to other system as the Identity Provider is aware of the services that the user is accessing.

India is a well known example of this approach. The Aadhaar is world's largest digital identity program, and has adopted a centralized digital identity system.

Another example is Finland. The Finnish "Population Registry" well describe the single Identity Provider scenario. The Population Registry is a national database that is owned and maintained by the Finnish government. The government acts as the 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, etc. Private Service Providers may also access this data, subject to criteria compliance and fee payment.

In the same fashion, the so-called DigID is a digital authentication system for Dutch residents who are accessing 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. Their national identifier number is transferred from the national citizen registry to the Service Providers.

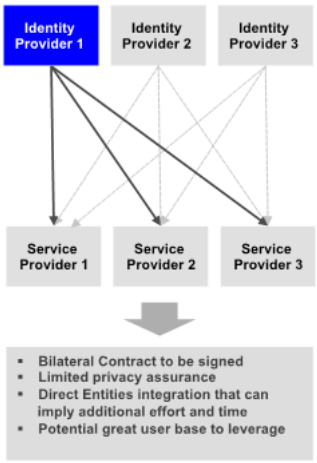
Estonia as well represents a successful case in which the Government operates as unique Identity Provider. The Estonian model is based on an electronic identity card, ID card, used as a definitive proof of identity in a digital and physical context. There are countless uses in both public and private sector: bank accounts identification access, digital signatures, public administration services access (such as medical records and tax situation). Subsequently, also a Mobile-ID mobile solution has been introduced, allowing citizens to use mobile phone as a secure form of digital identity. Both the ID-card and MobileID are government regulated: the ID-card is issued by Police and Border Guard and

they are also responsible for establishing the identity of users through MobileID, though MobileID compliant SIM cards are issued by mobile network operators.

4.3.2 Multiple Identity Providers

The section explores the scenario in which multiple entities are authorised to provide for digital identities.

In distributed identity systems, multiple Identity Providers collect, store and manage user credentials and attributes interacting with multiple Service Providers. These systems are notable as they leverage multiple identity providers' capabilities and differentiators for completion of identity processes in particular for identity proofing. Extensive experience in managing identities, identity solutions already in place branches where facilitate the interaction with citizens, are key elements for selecting this scenario. Moreover users are allowed to choose between different Identity Providers.



The main characteristics of this approach are:

- Multiple Identity Providers are accountable for the identity proofing of the citizens, and respectively holds users' credentials and attributes. The options for the user to own different identities can be contemplated;
- Service providers have to enable the option for the users to select between the different identity providers;
- Identity Provider is accountable for the authentication of their own users that are allowed to access digital services of multiple Service Providers, public and even private. A set of defined attributes might be transferred to service providers to enhance the personalization of services and efficiency of processes;
- 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;
- Private service providers participation is allowed subject to criteria compliance and fee payment;
- Privacy is limited compared to other system as the Identity Provider is aware of the services that the user is accessing.

An example of a Multiple Identity Providers system is offered by the Italian SPID. The system has been launched in March 2016 with the aim of providing digital identities to Italian citizens to allow access to public administration and 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).

4.3.3 Identity Broker/s with Multiple Identity Providers

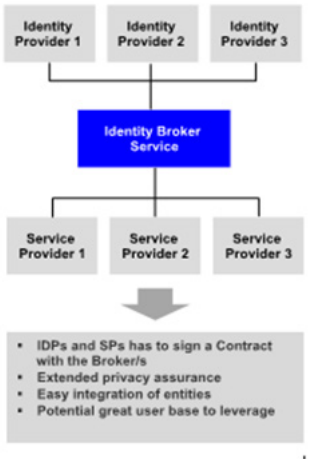
The section explores the scenario in which multiple entities manage digital identities, while interacting with one or more identity broker.

The majority of initiatives with multiple Identity Providers envisage the implementation of a Broker as an intermediary that connects Identity Provider and Service Provider.

Through the adoption of an Identity Broker, the objective is to intermediate the communication between Service Provider and Identity Provider, placing the Broker itself between these two entities.

The main advantages of this approach concern the possibility of simplifying the integration of Service Providers with multiple Identity Providers, but also a guarantee of 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 the citizens, and respectively holds users' credentials and attributes. The options for the user to own different identities can be contemplated.
- Service providers have to integrate just with the broker that is responsible to present to the users the option between the different identity providers
- Identity Provider is accountable for the authentication of their own users that are allowed to access digital services of multiple Service Providers, public and even private. A set of defined attributes might be transferred to service providers to enhance the personalization of services and efficiency of processes.
- 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 Government might deploy and operate the Identity Broker or demand this role to an external entity.
- Private service providers participation is allowed subject to criteria compliance and fee payment.
- Privacy is higher compared to other system 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.

As anticipated in other section, the introduction of an Identity Broker can simplify Service Providers adhesion, facilitating those who have reduced capacity both in economic and technical terms. This will also make it possible to reduce integration times and activities, especially in case of integration 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. In fact, it is currently impossible for a Service Provider to invoice each of the accredited Identity Providers.

A clear example of the role of an Identity Broker is given 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 ten Identity Providers. Once the users are authenticated through one of these providers, they are granted access to the government service they are trying to access. The programme uses a 'hub' (Broker) that allows identity providers to authenticate identities to relying parties without:

- government centrally storing an individual's data;
- privacy being breached by exchanging unnecessary data;
- either transacting party openly sharing user details.

4.3.4 Other architectural models

Distributed ledgers might represent a future alternative architecture for identity management that is certainly worth to be evaluated by Governments. This architecture contemplates that multiple Identity Providers can interact with multiple Services Provider as in other architecture models. The difference

is related in what is called process of "identity attestation". This implies that identity credentials are attested by users and third-parties on a decentralised database.

The role of the Government is very susceptible. When this model is not properly addressed, it can relinquish control to the benefit of third parties (such as corporations) or completely shift the control to users.

4.4 Focus Area 4 – Sustainability model

The sustainability of a National Digital Identity Framework is effectively one of the main concerns that national leaders and policy makers should have in mind when designing a framework. Indeed, even the most efficient, effective, and innovative solution does not have chances of success if it is not economically sustainable for the State.

Managing the identity of users entails certain costs. These are mainly related to the two processes of verification of the identity of the users, and the authentication of users. 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, the European regulation 910/2014 (eIDAS) defines three levels of guarantee for the electronic identification means (i.e. authentication) which must however be used taking into account the verification of the completed identity.

To summarise, high authentication tools are to be expected following high identity checks. An analogous approach has been adopted by the standard ISO29115.

The process that is likely to have the highest impact on the sustainability of the framework is the verification of users' 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 digital identity framework is given by the combination of two different aspects:

- How identities are employed
- Who pays in the system

4.4.1 Use of identity

In the context of a digital identity framework, it is possible to identify three different approaches related to how an identity can be employed by the users.

4.4.1.1 Identity for public services

In this case, the identity can be employed exclusively to access services offered by the Government or the Public Administration. Some examples of this approach are 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 belong only to private initiatives. No States have adopted such an approach to date.

---

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

[4] Ibid.

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 characterised 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 characterised 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 characterised 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.[1]

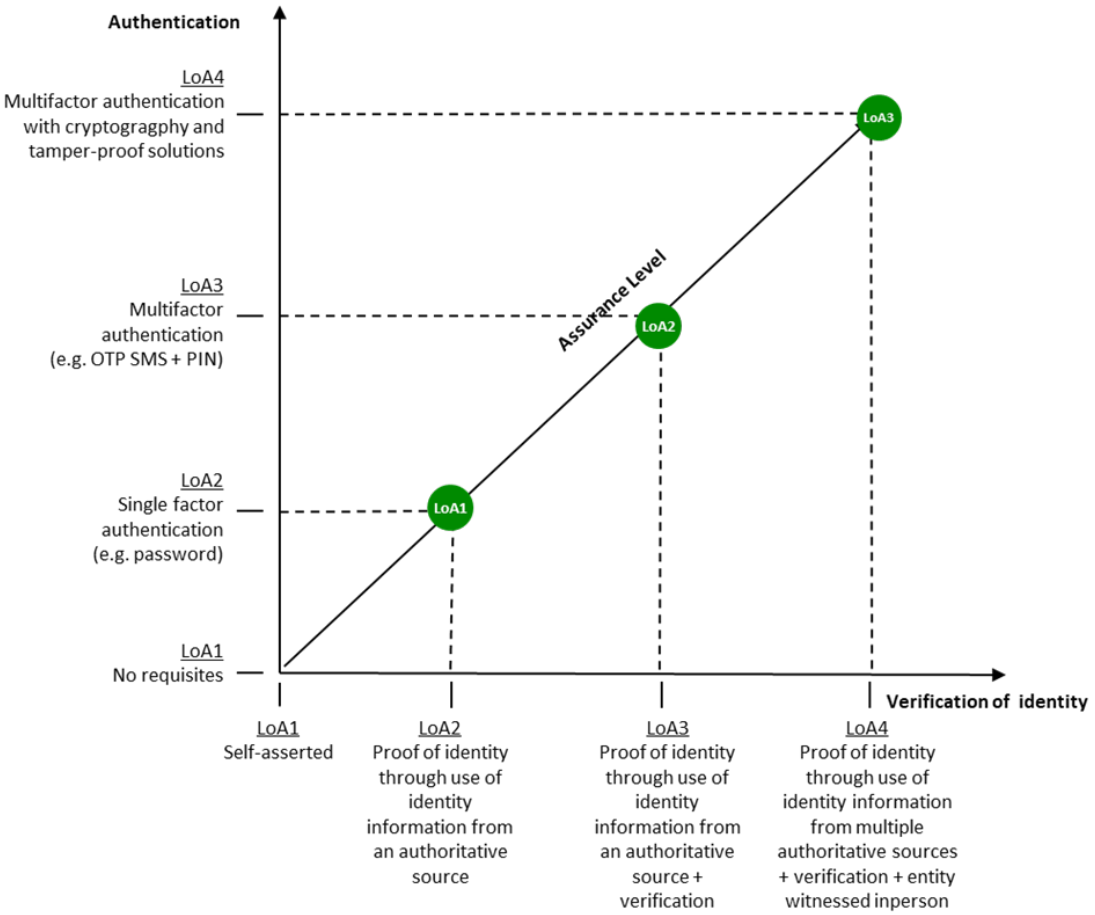
[1] See https://www.eid.as/home/

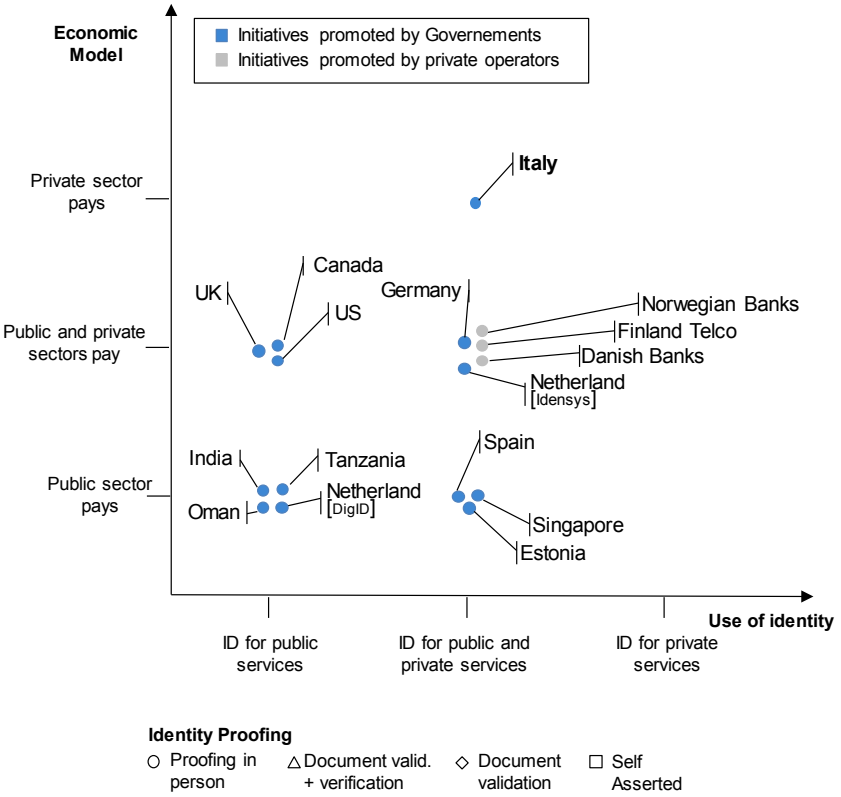
- Identity for public and private services: in this case, the identity can be employed to access services offered by both private entities and public administration. This is by far the most common model, counting the majority of the systems currently existing.

4.4.2 Economic models

In the context of a digital identity framework, it is possible to identify three different approaches related to how the system is financed.

- 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 specific approach.
- Public and private sectors pay: in this case, both the public sector and the private one sustain the costs of the digital identity system. It is a well-established models and many examples can be found.
- The private sector pays: in this case, the private sector fully sustains the costs of the digital identity system. It is a very uncommon way to sustain a National Digital Identity System and there are 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 (requiring therefore, requiring the approach with highest level of assurance, in-person verification) it is still private entities (playing the role of Identity Providers) that pays 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 a full opening of the system to private services.





Identity Proofing

○ Proofing in person △ Document valid. + verification ◇ Document validation ☐ Self Asserted

5 Digital Identity Framework Development

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

5.1 Phase 1 – Analyse

Prior to the beginning of the planning and drafting of a 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 a correct implementation and operation of the Digital Identity Framework.

5.1.1 Context analysis

5.1.1.1 Identification of national specifics and peculiarities

Among the first aspects to be taken into consideration, one should certainly look into the unique characteristics that shape the environment in which the Digital Identity Framework will be placed. Different countries, indeed, carry different features.

Cultural level, traditional models, accessibility to digital means, trust in the government, etc. These are just a few of the prominent elements that might impact the implementation and operation of a Digital Identity Framework. Therefore, given the potential consequences on the effectiveness of the framework, said elements must be identified at the outset of the development process, so that appropriate countermeasures can be investigated beforehand. For instance, a country mainly comprised of elderly people might decide to emphasise simplicity and accessibility, rather than efficiency. On the other hand, a relatively young population from another country might better respond to a Digital Identity System that seamlessly integrate into the digital fabric of their already hyper-connected lives.

These choices should necessarily be tailored to each specific situation. There is no one-size-fits-all approach for this. That is why it is so crucial to correctly assess national characteristics and peculiarities.

5.1.1.2 Benchmark of Digital Identity Strategy

Many governments and organisations worldwide are now equipped or are developing specific systems for digital identities management. This background provides an invaluable source of information that can be used to gather the most relevant lesson-learned to build upon.

In particular, the review of Digital Identity strategies should be focused, on one hand, on the overarching objective of the government for developing their strategy and the intended future state that it wants to reach through the strategy; on the other hand, the review should concern the main elements of the plan to realize the vision.

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 public and private sector based on a series of defined criteria; a good balance in terms of geography, population size, layers of government, diversity of cultures and styles of government should be ensured. A sample of different stages of advancement with respect to development and implementation of Digital Identity initiatives should be considered, from preliminary reflection or early development stage to full deployment.
- Case Analysis and Classification: each selected case is analyzed and classified accordingly to a well-defined set of dimensions, which help to understand the different approaches followed during the design and the implementation phases, the objectives that have been addressed

primarily, the tools (laws, plans, actions, etc.) developed to implement the strategy and the outcomes achieved.

- Case Evaluation: once the analysis is completed, good practice elements are derived to support own objectives and priorities in line with the vision defined in the national Digital Identity Strategy.

5.1.1.3 Identification of primary objectives

Once the entity developing the 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 Digital Identity System has to satisfy.

At this point, a set of goals and objectives should already be present, as the decision to implement a Digital Identity System most likely rests on specific needs. It is for this reasons that a careful identification on objectives and principles is crucial for provide an appropriate guide for the further phases.

5.2 Phase 2 – Define strategy

The purpose of this phase is to develop the Digital Identity Strategy by engaging key stakeholders from the involved entity. Public consultations and working groups involving public sector, private sector, and civil society could be established as well, based 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. As part of this phase, the primary objectives and principles and the good practice elements raising from the Benchmark activities conducted during Phase 1 should be taken into account.

5.2.1 Definition of Digital Identity Strategy

The Digital Identity Strategy should provide the overall Digital Identity direction for the country; express a clear vision and scope; set objectives to be accomplished within a specific time frame; and prioritise these in terms of impact on society, economy, and infrastructure. Moreover, it should identify possible courses of actions; 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 to focus on specific topics, or to draft 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 that sense, 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 the Strategy development, its formal adoption has to be ensured. Its broad availability will both ensure that the general public is aware of the government's priorities and objectives for Digital Identity, and also support any effort to raise awareness. This official adoption process will vary by country and be based on how the Strategy is defined in the legislative framework. Furthermore, it is pivotal that the Strategy is not only developed with approval from the highest levels of government, but that this commitment continues in its implementation phase.

5.2.2 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 as part of its development. The implementation phase should be centred on an Action Plan, which can support the effective implementation of the Strategy and guides the various activities envisioned.

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

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

5.3 Phase 3 – Implement system

5.3.1 Implement governance model

Governments have to carefully implement the governance models and supporting tools. Once it has selected which role it will play in the National Digital Identity Framework (just regulator, as Identity Provider, etc.) it is important to define the entire set of processes, roles and responsibilities that need to be implemented in order for the Government to efficiently play the role it has decided to adopt. These have to be formalised and distributed among the right stakeholder.

5.3.2 Define of review regulations or 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 regulations and laws should be investigated in advance and a set of proper measures instituted.

During the review of laws and regulations, attention should be reserved also to the broader ICT policies and regulatory environment. Digital Identity is an integral element of ICT and could benefit from policies that aim, in the long term, to promote modern and effective ICT infrastructure in a country. For example, policies that aim to provide more connectivity and online access to everyone, improved digital education and training, and incentives for the private sector to participate in the development of ICT infrastructure in the country could also positively affect the Digital Identity Framework development.

5.3.3 Design/Implement architecture

The architectural model can follow different approach: a centralized system with a single identity provider that collect and manage all the information and data; distributed system with multiple identity providers; or system with intermediaries between identity provider(s) and the other elements that act with 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.

Technology strategy thus plays a crucial role in the development of a Digital Identity in a country; dimensions that come into play include cost, capacity, interoperability, usage, security, privacy, and long-term viability. Many of the technical components revolve indeed 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 the technology strategy is an assessment of a country's underlying, enabling technology infrastructure. High-speed Internet is often a necessary requirement for an online identity solution, but many developing countries are still working to develop and deploy it. 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 payment system, POS devices, ATMs, agent networks, and payment networks- to benefit from Digital Identity.

For these reasons, the architectural choices- that include the identification of functional and non-functional requirements, the selection of platform components, the definition of the 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 to be addressed in the future.

5.3.4 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 includes 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 the citizens can update their data in a secure yet convenient manner. Without a procer data update mechanism, the data related to the digita 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.
- Deprovisioning: removal of accounts, credentials and/or privileges based on specific request, events or rules.

5.3.5 Implement sustainability model

Sufficient, consistent, and continuous funding provide the foundations for an effective Digital Identity initiative. Based on the Governance model established for the 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 (i.e., dedicated budget), people, material, as well as the relationships and partnerships and continued political commitment and leadership required for 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 costs. The kind of pricing and cost-distribution models that are selected are vital to ensure a sustainable Digital Identity

System. Governments can consider potential revenue flows by offering identity services to offset the costs of Digital Identity development and for inducing sustainability in the operations.

Public-private partnerships can provide an avenue to relieve the fiduciary burden and has been demonstrated to be successful in many countries around the world. A financial and economic model, with detailed expected costs, and potential revenue streams, needs to be developed upfront and implemented accordingly.

5.4 Phase 4 – Operate and continuosly improve

During this phase, all the tasks related to the operations 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 is still reflecting the government's objectives and what adjustments are necessary.

Continuous assessment of the implementation plan (i.e., 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 of potential improvement. This approach will ensure that the relevant stakeholders are held accountable to the commitments set, as well as that any challenges to implementation are identified early on. In turn, this would allow the government to either rectify the situation or adapt its plans accordingly based on the lessons learnt in the implementation process.

In addition to assessing the 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 realised or whether different actions should be considered.

Once a digital identity platform is operations, monitoring for fraud management also becomes critical. One set of frauds can be managed by inherent technology design of the ID system. Another set of frauds need to be monitored during ongoing operations such as data updates & authentication.

6 Critical success factors and conflicting principles

Designing and implementing a successful Digital Identity Framework involves a huge number of factors, considerations, and complex decisions. Among all the factors that influence this process, some can be seen as critical enablers that, when correctly implemented, can greatly increase the chance of success of the Digital Identity Framework and of its underlying system.

Also, another set of elements with a considerable impact on the advancement of the project comprises certain key-principles that, by their nature, stand as opposite to one another. These set of paired-principles will force Governments and National entities to carefully decide how to characterise their Digital Identity Frameworks.

6.1 Critical success factors

Certain factors might enhance the chance of success of a National Digital Identity Framework. There is no exhaustive list of them, as their effectiveness may vary in different context. However, some of them retain their importance across different situations.

6.1.1 Organization structure and capacity building

When a certain environment is built around a solid organization and can provide for appropriate and diverse skill sets, the design and implementation of the National Digital Identity Framework will greatly benefit of this pool of structured expertise.

The areas of competence that most likely can have an impact are:

- Government processes;
- Technology;
- Program management;
- Legal & regulatory;
- Media, communication & civil society outreach.

6.1.2 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 ensuring a speedy deployment.

6.1.3 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).

6.1.4 Regulatory & framework

How the identity program would fit in the regulatory framework of the country needs to be defined. This would also dictate stakeholders' engagement.

6.2 Conflicting principles

While certain factors can be seen as useful aid to the development of a Digital Identity Framework, other present certain set of constrains. These constrains are hardly avoidable, as they originates from the inherent conflicts that arise when certain principles have to be put into the design of the Digital Identity system.

6.2.1 Homeland 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 homeland/national security rationale. Digital identities can be a powerful tool in combating crime, patrolling border, ensure security, etc. For this reason, Governments might be willing to primarily employ their Digital Identity System for security reasons. On the other hand, Governments might decide to implement a Digital Identity System to enhance the service offering to their citizens (e.g. increasing the efficiency of welfare and social system), rather than strengthening its control capabilities.

The two approaches mentioned above can hardly be equally implemented in a Digital Identity Framework, as the first one (national security) will require a wider approach to the monitoring of individuals and their information, while the second one will be best implemented in a "data minimization" regime (meaning that only the data necessary to a specific purpose will be collected and processed). Since the scenarios have distinctively different characteristics, it is extremely complicated to strike the right balance between them. Therefore, Digital Identity Systems tend to be closer to one or another, rather than embracing both of them.

6.2.2 Data security vs citizen convenience

When managing data of users, and especially when those data are sensitive (as in the case of data regarding identity), security should certainly be one of the top priority of the system. However, it holds true that tight security measures can greatly affect the success of the system. Indeed, users might not see the benefits of operating in a secure environment. Instead, they will likely perceive the inconveniences (e.g. time spent to authenticate multiple times, physical authentication devices that have to be carried around, etc.) they have to suffer in order to use the services offered by the system.

This is a challenge that Nations implementing a Digital Identity System will have to face. Each one will have to find the correct balance, by performing careful analysis of the risks and the benefits.

6.2.3 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. On one hand, a Digital Identity System can be fully populated with newly created digital identities. This might ensure a good level of consistency of the entries, since a standardised approach is adopted from the inception of the implementation. On the other hand, since in the framework of services offered by national entities and government it is likely that some sort of identification means already exist, it might be possible to leverage on this already existing capabilities to build an identity database. This second approach might provide for certain advantages, such as a potential lower cost of implementation. However, it carries a number of problems, mainly related to the fact that these kind of identification means are not designed to manage digital identities. For instance, some of them might not provide a universal coverage (e.g. voters ID database covers only people that reached voting age, or driving license database cover only people who have a license). Also, it is worth pointing out that, since in this second case the entries do not have a shared standard, the efforts required to normalise the database (i.e. complete partial identities with the correct attributes, and reach out for identities that are not already digitalised) might be higher than those required by the creation of a *de novo* database.

6.2.4 Minimal citizen data vs full citizen data register

The degree of data collected and associated to each identity can greatly influence the design decisions related to the 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 resources necessary to maintain up-to-date the database. Obviously enough, deciding on a minimal data collection approach rather than a full one can impact the range of services that the Government will be able to provide.

On one side, digital identity system could be used as an opportunity to capture ID number associated with all social and government services that a citizen is part of (e.g. voter ID card, Income Tax ID, passport number, census data, etc.). The positive of this approach would be that the Government would have 360 degrees view of the citizen, which could 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 of this approach would be that the Government could do profiling and could use this knowledge against certain communities basis political affiliations or other reasons. This approach might be seen as giving Governments too much control. Also, it would increase the complications and time in enrolling the citizens as different local areas or regions might run different welfare programs with little standardisation of data formats (this holds true in particular for larger States).

6.2.5 Tokenless identity vs token based identity

In the realm of digital authentication, such a process is carried out by verifying the identity of users by mean of “something they own” (for instance, a smart card), “something they know” (for instance, a password), “something they are” (for instance, through biometric parameters) or a combination of these elements.

Digital identities are intangible assets. However, this does not necessarily mean that no tangible asset can be employed to define how digital identities are utilized. Two opposite views exist in this regard. In the first case, a Digital Identity System embraces the tokenless nature of digital identity, releasing user from the necessity to carry additional devices. In this particular scenario, the identity of users can be verified only through “something they know” or “something they are”. Said approach is flexible and highly convenient for the user, who is more likely to slowly grow accustomed to the ease-of-use of this kind of digital identity systems. However, it is also poses a number of security threats, especially when the system employs either the “something you know” approach (a mere username and password can more easily hacked) or the “something you are” one (biometrics are highly sensitive data that require special protection).

In the second case, one or more physical tokens are associated to each user. This approach grants a higher level of security, as the “something you own” approach effectively places and extra layer of protection over the digital identity. However, the necessity to always carry around a physical token might be seen as a burden (especially by younger people, often more focused on convenience than risk prevention) that can impair the rate of adoption and chances of success of the system on the long term. Also, in this case, the cost of replacing the token / ID in case someone loses their token, could be higher.

While making a decision on this regard, one should consider the cost, processes involved, uniqueness attribute and citizen convenience in the complete lifecycle of identity management.

7 Reference Materials

In the process of developing this Guide a stocktaking of existing guides and best practices was conducted. This allowed to identify materials already available to support countries in developing their Digital Identity Framework, such as standards or other tools, but also a series of case studies that can be investigate to see how other States approach a National Digital Identity Framework. The list below provides a comprehensive, but not exhaustive catalogue of the abovementioned materials, including web links.

7.1 Digital Identity System Cases

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

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

7.1.1 Sultanate of Oman

The Information Technology Authority (hereinafter,ITA) in Oman aims to consolidate the government policies to transform the Sultanate into a knowledge-based economy and to achieve social and economic benefits to the Omani society by using technology within the policies of economic diversification and sustainable development. In order to support the 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. To increase citizens and businesses trust in electronic transactions, ITA has started the formulation of an e-Legislation for Oman, with the goal to establish the required infrastructure to implement the applications needed to support delivery of electronic and internet-based services.

ITA launched the National Public Key Infrastructure (hereinafter, Oman National PKI) in order to support the use of e-Services and to lead 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 authentications 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 to uniquely identify the claimed owner. Citizens and Residents who use electronic services should require a digital identity certificate (authentication certificate), a credential that contains the public key for an individual along with other identity information. The certificate is created and signed by a trusted third party as certificate authority (CA), the Oman National PKI. 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 legal binding.

Once signed and activated, the authentication certificate and related credential are embedded in a National ID Card or in a Mobile ID (PKI enabled SIM Cards):

- 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/residents, 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/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. The citizens/residents get the Digital ID the moment thy obtain an ID Card in all Civil Status Centers in all governorates.

The activation is done immediately after receiving the ID card by entering a 6-digits PIN in 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 illegal uses.

- PKI enabled SIM Cards are provided by Mobile Network Operators (hereafter, MNOs) who are also accredited as RAs in Oman National PKI. The Digital Identity certificates are registered by the MNOs and issued by the National PKI. The digital Identity will be embedded inside the SIM card in a PKI certificate. The enrollment process is optional. The citizens/residents may ask the MNO for a PKI enabled SIM card the moment they obtain a SIM card. The activation is provided via our portal www.oman.om/tam after receiving the registered SIM card and by entering a 6-digits PIN in the phone. It is necessary to activate the identity before it is ready to be used in order to secure it and prevent illegal uses.

What was the goal in developing a Digital Identity System?

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

Who is the Identity Provider?

Oman National PKI provides the digital identity certificates, which are embedded in the eID, the Mobile ID SIM card, or a Smart Card Token for official use.

How are users identified?

For the digital identity in the National/resident Card, citizens and residents are identified and confirmed physically by ROP (an accredited RA).

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

What is the role of the Government?

The government (Oman National PKI) issues digital identity certificates to citizens and residents. The certificate registration is then implemented by ROP and MNOs.

Which are the uses of the digital identity?

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

What are adoption enablers (e.g. Support to citizens or service providers)?

1. The National eOman Strategy acts as an umbrella for the government electronic transformation initiative where unlimited support is provided to transfer the traditional services to electronic service.
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; Oman e-Transaction Law.
4. Integration of the National ID card registration system with the National Digital Identity System.

5. Integration of the telecommunication registration systems with the National Mobile PKI Identity System.
6. Enforcement to provide government services via PKI services. In Oman, the enforcement is achieved using a mandate by the highest authority, ministers' cabinet. Online services are only provided by PKI services. There is no other way.
7. Good awareness strategies and campaigns for the entities and the public.

How is identity proofing completed?

By integrating the entities websites, applications and mobile apps to the National Digital Identity System and National Mobile PKI Identity System. When citizens/residents attempt to utilize an online service, they will be redirected to the national identity gateway to provide the digital identity for secure authentication.

Which are the methods of authentication?

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 are issued in the Eid cards and Mobile ID for 4.5 million population in Oman

- **Number of Transactions**

  From July 2013 – July 2018: **14.1 million** electronic transaction have been by the citizens and residents using the digital identity.

- **Integrated Entities**

Oman provide hundreds of services that are delivered only to users that have a digital identity. As 24 government/private entity are integrated to the national digital identity, the services are commercial service, manpower service, health care services, financial service, customs services, social insurance services, SMEs services, elections services, and municipalities services.

7.1.2 India

The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar Act of 2016. Prior to its establishment as a statutory authority, UIDAI was functioning since February 2010 as an attached office of the then Planning Commission (now NITI Aayog). Later, on 12 September 2015, the Government revised the Allocation of Business Rules to attach the UIDAI to the Department of Electronics & Information Technology (DeitY) of the then Ministry of Communications and Information Technology.

UIDAI was created with the objective to issue Unique Identification numbers (UID), named as "Aadhaar", to all residents of India in order to

1. Eliminate duplicate and fake identities.
2. 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. Person willing 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; the uniqueness is achieved through the process of biometric de-duplication.

UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedures, and system for issuing Aadhaar numbers to individuals and perform authentication. It also requires to ensure the security of identity information and 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 of the country to deliver various subsidies, benefits and services by using the resident's Aadhaar number only. Two of the most critical goals of India's digital identity system are uniqueness of identities & 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 the residents in various programs of the government. It has been estimated that there are substantial leakages due to existence of duplicates and ghosts in the set of beneficiaries of every program. Another reason for ensuring uniqueness is to create a citizen-centric view of benefits and services which various programs cover.
- **Inclusion:** The 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 till 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 and avail 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 & biometric data from residents through Enrolment Agencies and send to UIDAI. UIDAI carries out required backend quality check and deduplication process to generate Aadhaar & communicate the same to residents.

How are users identified?

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

What is the role of the Government?

Government owns and manages the identity the platform. Besides, government is also one of the biggest users of the digital identity platform to render social services to citizens.

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

Which are the uses of the digital identity?

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

- **Aadhaar as Cleansing Agent:** 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 the residents in various programs of the government. This objective is achieved by adding Aadhaar number of beneficiary to the respective records in the program databases. For example, in a scholarship program, all the 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 etc get eliminated from the database. Aadhaar seeding is the necessary first step in Government of India's Direct Benefit Transfer (DBT) program which now covers over 430 schemes across 55+ ministries[2].
- **Aadhaar as Financial Address:** For all such programs in which 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 Aadhaar number to the bank/ bank account). Such programs range across student scholarships, pension schemes, livelihood support, food distribution system, cooking gas subsidies, health care schemes etc. This program is referred to as Direct Benefit Transfer details of which are available on 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:
    - Confirming Beneficiary before delivery of the services such as food grain delivery to Public Distribution System beneficiaries, health service delivery to beneficiaries of different health programs.
    - Attendance tracking for programs 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 banking system to open new accounts and to issue credit products, by Telcos for issuing SIM cards to customers and by various government programs to add beneficiaries. Over 250 agencies are using eKYC service. On an average, about 9 million eKYC transactions are carried out every day[5].

What are 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 program to reengineer their services. Leveraging Aadhaar (both adding Aadhaar to service delivery databases & online authentication) benefits both residents (convenience & portability) and service providers (cheaper, faster, ensures targeted service delivery).

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

- Self-incentivized ecosystem that enables 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:

---

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

  - 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
- Open, standards-based inter-operable platform to allow easy plug-and-play for various service delivery/support systems; this was supported by well-defined (& 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 & definition of quality, technology and processes to ensure robust backbone and adequate quality of data in the system
- Focused project management based approach, well designed proof of concept studies (PoCs) & pilots followed by large scale rollout

How is identity proofing completed?

Biometrics are at the heart of Aadhaar which ensures 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 the enrolment form, getting demographic and biometric data captured, submitting proof of Identity and address documents, before collecting acknowledgement slip containing Enrolment ID. The data is then sent to UIDAI data centre wherein Aadhaar generation process begins.
- **Aadhaar Generation**: A backend process that involves activities such as quality check, packet validation, demographic and biometric de-duplication etc. Aadhaar is generated successfully only if:
  - 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.

Which are the methods of authentication?

Aadhaar authentication[6] is the process wherein 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 the residents are 'who they say they are' in order to supply services and give access to benefits.

Aadhaar provides online authentication[7] through following means:

- Demographic data
- Fingerprint

[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

- Iris
- OTP

What is the level of adoption?

Transaction volume on Aadhaar adoption can be found on Aadhaar Dashboards portal & DBT portal. Some statistics (as on Aug 2018) are follows:

- Number of Aadhaar 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 FY 2017-2018: 1.24 billion
- Amount transferred under DBT scheme: >USD 61 billion

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 to online identity. Some of the social benefits of Aadhaar include:

- Aadhaar has resulted in the largest service delivery reengineering program in the world. Since Aadhaar in an online identity, any service that needs to use Aadhaar needs to be in online format. Aadhaar adoption by various service delivery programs has expedited the long pending process transformation and digitization of most government programs.
- 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 under privileged that requires zero minimum balance.
- Aadhaar has also transformed the delivery of social welfare programs by bringing in population that were earlier cut off from such benefits due to their 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].
- Aadhaar has enabled the government to shift from indirect to direct benefits transfer. In financial year 2017-2018, Government of India transferred subsidies worth over USD 26.2 billion directly to beneficiaries' bank account[9].

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

7.1.3 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 maintaining National ID Database for the purposes of enhancing security and socio-economic development of the country. NIDA is a government Institution which is under the Ministry of Home Affairs of Tanzania.

---

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/

NIDA was established with the following core objectives:

1. Registering people living in Tanzania of 18 years and above (Citizen, Legal resident, and refugees).
2. Building a Database of registered persons and share data with all stakeholders and beneficiaries.
3. Producing and issuing ID Cards to all registered people with their status to be as an Identification document for various transactions wherever Identifications is requested.
4. Foster Good Governance.

In a view of digitalisation of this activity NIDA has launched the 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:

1. Biographical Data (e.g . National ID number, name of the card holder, gender, birth date, birth place (District), place of Issue, place where card is printed (i.e. Dar Es Salaam), birth certificate Number);
2. Photo;
3. Fingerprint (fingerprint right and left fingerprint templates of the card holder);
4. Residential address;
5. Personal reference information.

Each Individual who registers with the National Identity Authority (NIDA) is associated to a number called National Identification Number (NIN). The NIN is assigned to an individual at the time of the initial registration with NIDA. NIN is associated with a single set of biometric attributes of the individual holding the NIN and 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 national ID database registry. All new applicants' records must go through AFIS check so that they can be checked if their records are existing in the National ID Database or they have been blacklisted.

All Processed Information are Central stored in the State of the art Data Centre. The Data Centre meets all the International Standard (ISO 27001 and ISO 9001). The Data Centre is equipped with a Disaster Recovery Site which is a Mirror site. In case of disaster on the Main Data Centre the Disaster Recovery Site can be used to operate the National ID System. NIDA requires nationwide ICT access services to connect all Districts Registration Offices with the Data Center.

To register and obtain the ID card, citizens must send information to the central processing center for verification purposes. The information are subjected to the AFIS system to remove the duplicates. Once that information are verified, the IDs are printed. All printed IDs are subjected to 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 of 18 years and above (Citizen, Legal resident, and refugees);
2. Building a Database of registered persons and share data with all stakeholders and beneficiaries;
3. Producing and issuing ID Cards to all registered people with their status to be as an Identification document for various transactions wherever Identifications is requested;
4. Foster Good Governance.

Who is the Identity Provider?

NIDA is a governmental institution which is under the Ministry of Home Affairs of Tanzania. The National Identification Authority (NIDA) is the only reliable Institution vested with mandate of preparing and Issuing Identification Cards and useful information from its Database to various Stakeholders.

How are users identified?

In Tanzania a person gets a digital identity at the moment he/she obtains an Identity Card. The issuance of both physical and digital identities, therefore, happens at the same moment.

What is the role of the Government?

Government is directly involved in the digital identity system as managemer and as Identity Provider through NIDA.

Which are the uses of the digital identity?

National ID system has led to several benefits for Tanzania government, from the elimination of ghost workers in Government Payroll System to the assistance in the identifications for the National Social Security schemes. The ID system is used by financial institutions in terms of giving loan to individual, or to solve problems in identifying the potential beneficiaries of the student loan. The National Identification system is expected to reduce significantly financial resources that are used in Government major systems through the harmonization of identification of persons, to increase the security of border control and to fight crime.

What are adoption enablers (e.g. Support to citizens or service providers)?

In Tanzania the adoption has been encouraged thanks to the Government's action that made it mandatory to access a series of public services with digital identity such as:

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

How is identity proofing completed?

To register and obtain the ID card, citizens must send information to the central processing center for verifications purposes. All information's after objection are passing via different approval process. The information are subjected to the AFIS system to remove the duplicates. Once that information are verified the IDs are printed. All printed IDs are subjected to the Quality check for physical and electronic checking and then IDs are bundles for the issuance purposes.

Which are the methods of authentication?

In Tanzania the following authentication methods are adopted

- Fingerprint or PIN matching against central database through Common Interface Gateway and APIs
- Fingerprint matching against smartcard
- 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, approx. 56% of theentire adult population;

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

- 5.2 million national ID cards issued;
- 53 institutions have agreed to access Common Interface Gateway for authentication services through API;
- Registration Office established in all 150 Districts.

7.1.4 UK

Gov.uk Verify is the name of UK Digital Identity project started in 2012 as part of the government initiative Identity Assurance Program.

Access to private services is considered crucial as demonstrated by the dialogue opened by the Government with banks, insurance companies and retailers to ensure that Verify becomes the national authentication scheme not only for public administration services.

The commitment of the British Government has been substantial. The budget made available was £ 150M for the three years of service, above the £ 25M value for the first initiative.

Other feature of Verify is the capacity of interact between Identity Provider and Service Provider. This has been simplified through the creation of an Identity Broker with the aim of mediate communication between Service Provider and Identity Provider.

The benefits are:

- simplify the integration of Service Providers with multiple Identity Providers
- Guarantee privacy for users. Service Provider is not able to trace the Identity Provider to which the users access and vice versa.

What was the goal in developing a Digital Identity System?

The goal is to spread the use of Digital Identity System for the access to public services as already done with:

- 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)

Who is the Identity Provider?

In UK, the Identity Providers have been chosen with a tender. As of today, 8 different Identity Providers exist, up to a maximum of 10, for a duration of three years with an option for a further year.

How are users identified?

Identity verification is completed online by validating multiple identification documents (e.g. passport, driving license).

What is the role of the Government?

Government chooses Digital Identity Providers. Digital Identity Providers have been chosen with a tender. Access to private services is considered crucial as demonstrated by the dialogue opened by the government with banks, insurance companies and retailers to ensure that Verify becomes the national authentication scheme not only for public administration services.

Which are the uses of the digital identity?

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)
- Request a basic Disclosure and Barring Service (DBS) check (DBS)
- Update your rural payments details, with the Department for Environment, Food and Rural Affairs (Defra)

What are adoption enablers (e.g. Support to citizens or service providers)?

In both cases, supporting citizens in the access to public services and allowing to service providers to offer the services. The Digital Identity providers have been chosen with a tender, the maximum number of providers is 10, for a duration of three years with an option for a further year.

How is identity proofing completed?

Identity verification is completed online by validating multiple identification documents (e.g. passport, driving license).

Which are the methods of authentication?

Several methods of authentication: usr/password, PIN, ofb Pin, Biometric, HW/SW token

What is the level of adoption?

In April 2016, when the system became fully operational, there were about thirty services available. The Government plans to integrate additional others in the future. The challenging objective given by the Government was to reach 90% of the demographic coverage by April 2016.

7.1.5 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. Digital Identity system of Estonia, called e-Estonia, introduced in 2002, currently has a coverage close to 94% on a total population of 1.3 million. It is based on the use of electronic identity card, ID card, used as a definitive proof of identity in a digital and physical context.

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 having a card reader.

What was the goal in developing a Digital Identity System?

Create an advanced digital society building an efficient, secure and transparent ecosystem that saves time and money. Electronic identity card, ID card, is used as a definitive proof of identity in a digital and physical context.

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 having a card reader.

What is the role of the Government?

The government is the Identity Provider.

Which are the uses of the digital identity?

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

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

What are adoption enablers (e.g. Support to citizens or service providers)?

All Estonian citizens and who has a residence permit are required to hold a Digital Identity. This greatly promoted the quick and steady adoption of the system, which as of today has an almost complete coverage of Estonian population.

How is identity proofing completed?

Identity verification is completed by validating the identification documents (e.g. passport, driving license).

Which are the methods of authentication?

Id card and Mobile-ID mobile solution.

What is the level of adoption?

All Estonian citizens and who has a residence permit are required to hold a Digital Identity. Digital Identity system of Estonia, called e-Estonia, introduced in 2002, currently has a coverage close to 98% on a total population of 1.3 million.

7.1.6 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 Canadian Government has chosen SecureKey as Identity Broker, and five of the major banks of the country as the Identity Providers, these have provided a large number of customers and secure means of authentication. The contract amount is $ 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- alternative to the one already offered by the Government- to access the services of the public administration, based on a "bring your own credentials" (BYOC) model where users are enabled the use of credentials that already exist and use

Who is the Identity Provider?

The Canadian Government has chosen SecureKey as Identity Broker, and five of the major banks of the country as the Identity Providers, these have provided a large number of 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 role of the Government?

The Canadian Government has chosen SecureKey as Identity Broker though a tender.

Which are the uses of the digital identity?

SecureKey Concierge is a next generation authentication network for conveniently connecting people to critical online services using a banking credential they already have and trust.

What are adoption enablers (e.g. Support to citizens or service providers)?

By adopting already existing credentials, leveraging on the convenience of users, the Canadian Government has been able to push for the adoption of the framework.

How is identity proofing completed?

The users are already registered in the Identity Providers database (banks) as clients. New users can be identified with an identity document at the banks that offer the service of providers.

Which are the methods of authentication?

Through instruments already defined by the Identity Providers (Banks) based on the 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 used was 1 million and transactions amounted to 1 million a month.

7.2 Standards and best practices

As of today, the topic of National Digital Identity Framework is a widely debated one. 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.

The list is quickly expanding, and it is surely not possible to provide for an exhaustive one. Following, some of the currently most relevant ones are briefly described.

7.2.1 International Telecommunication Union

7.2.2 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;

- 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; and
- Provides guidance concerning controls that should be used to mitigate authentication threats.

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 (i.e., the entity) is in fact the entity to which that identity was assigned.

The actors involved in the EAAF include entities, Credential Service Provider (CSPs), Registration Authority (RAs), relying party (RPs), verifiers, and trusted third party (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.

Entity Authentication Assurance Framework (EAAF) provides a model with specific phases and processes; organizations adopting this Framework shall establish policies and procedures that provide the necessary supporting processes and fulfil requirements set forth in the Framework.

7.2.3 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.

7.2.4 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 provide 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 it also provides the required proper security procedures when two IdM systems are interoperated.

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

7.3 Referenced documents and web links

The list below provides a comprehensive, but not exhaustive catalogue of the abovementioned materials, including web links.

7.3.1 Documents

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.

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

7.3.2 Web links

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

https://dbtbharat.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