

Caribbean Telecommunications Union

Handbook for the Implementation of Digital Identification Systems in the Caribbean

Abstract

This document identifies the rationale and activities to be undertaken by Caribbean Governments for implementing a foundational national Digital Identification System on the road to being a 21st Century Government.



CTU Secretariat

Issue: 1.1
Date: January 2021

Table of Contents

1.	DOCUMENT OVERVIEW.....	3
1.1	DISCLAIMER	3
1.2	PURPOSE.....	3
1.3	TARGET AUDIENCE.....	3
2	HISTORICAL OVERVIEW OF GOVERNMENT	3
3	DIGITAL TRANSFORMATION FOR 21ST CENTURY GOVERNMENT.....	4
4	DIGITAL IDENTITY FOR 21ST CENTURY GOVERNMENT	4
5	SCOPE OF THE NATIONAL DIGITAL IDENTIFICATION SYSTEM	6
5.1	PHASE 1 – CONTEXT ANALYSIS AND POLICY DEVELOPMENT	6
5.1.1	BENCHMARK OF DIGITAL IDENTITY STRATEGY	7
5.1.2	DEVELOP DIGITAL IDENTITY POLICY.....	7
5.1.3	IDENTIFY PRIMARY VISION AND OBJECTIVES	9
5.2	PHASE 2 – DEFINE STRATEGY	9
5.2.1	DEFINITION OF DIGITAL IDENTITY STRATEGY	9
5.2.2	IMPLEMENTATION OF DIGITAL IDENTITY STRATEGIC PROCESS.....	9
5.3	PHASE 3 – IMPLEMENT DIGITAL ID SYSTEM	10
5.3.1	IMPLEMENT GOVERNANCE MODEL	11
5.3.2	IMPLEMENT ARCHITECTURE MODEL.....	12
5.3.3	DESIGN AND IMPLEMENT TECHNOLOGY MODEL.....	14
5.3.4	INTEROPERABILITY AND MUTUAL RECOGNITION.....	24
5.3.5	IMPLEMENT ADOPTION MODEL	29
5.4	PHASE 4 - OPERATE AND CONTINUOUSLY IMPROVE.....	35
5.4.1	APPROACH TO CONTINUOUS REGISTRATION.....	35
5.4.2	BASELINE INTELLIGENCE	35
5.4.3	MONITORING AND EVALUATION.....	36
5.4.4	DIGITAL ID ROADMAP	37
6	CONCLUSION	37
7	WORK CITED:	41

Handbook for the Implementation of Digital Identification Systems in the Caribbean

1. Document Overview

1.1 Disclaimer

Some aspects of this document are adaptations of original work by the International Telecommunication Union (ITU) and The World Bank. Views and opinions expressed in such adaptations are the sole responsibility of the Caribbean Telecommunications Union and are not necessarily endorsed by the above-mentioned organisations.

1.2 Purpose

The purpose of this handbook is to guide national leaders, policy makers and implementing agencies in the Caribbean in developing a framework and implementation plan for their national digital Identity systems. A comprehensive roadmap and vision on the main elements and principles related to the notion of digital identity in a national context and approaches for its implementation are provided.

The intention is to provide the readers with the requisite knowledge to grasp the essential concepts of digital identity and how they may apply in a national context. Insight will be obtained for undertaking a wide range of initiatives in the field of digital identity in the pursuit of a national digital identity strategy and technology implementation in the Caribbean context.

1.3 Target Audience

The primary audience for this handbook comprises policy makers and technocrats responsible for developing national digital identity frameworks within the Caribbean. Secondary would be those public sector stakeholders that might be involved in the development and implementation of a digital identity system, including government staff and regulatory and legal authorities. These public sector actors would need to foster effective partnerships with Information and Communications Technology (ICT) providers, critical infrastructure operators, civil society and academia to support the implementation of a digital identification system.

2 Historical Overview of Government

A national Government has a unique relationship with its citizens. It is the only institution that consistently interfaces with all citizens through every phase of life, that is, from birth until death. As a citizen, one must be registered at birth, one must be educated, find employment or register a business, pay taxes, register one's marriage, purchase property, license a car, receive health treatments, and ultimately, have one's departure from this life registered. The Government, therefore, is uniquely and exclusively positioned to know and identify its citizens and has a responsibility to create and maintain systems that efficiently service their needs and enable them to participate effectively in the development of the country.

Historically, the knowledge systems governments employ have been based on government ministries and agencies operating independently, with systems rooted in processes that are centuries old. The citizen is required to provide their information to every ministry or agency with which they interact, notwithstanding that the information may already exist elsewhere in government records, often in the form of physical documents. This imposes unnecessary burdens of inefficient, time-consuming and costly processing, duplicated storage, repetitive processes, security risks, and lack of transparency in the delivery of government services to its citizens.

3 Digital Transformation for 21st Century Government

Given this history, there is a need for Caribbean governments to take a 21st Century Government approach to ICT investment that will ultimately maximise the returns and see governments becoming more citizen-centric and seamless. The benefits of investing in ICTs are not automatic but require commensurate reengineering of processes as well as appropriate policy, legislation and regulatory reform. These must be driven by a champion and leadership at the highest level of government, with the political will to change existing mind-sets, inspire citizens and to coordinate ministers and the activities of their ministries. There must be a focus on a citizen-centric, “whole of government” approach to interacting with various constituents, which include citizens and business. All of these must be implemented by people who are knowledgeable, trained and prepared with the skills to maximise the use of ICT in innovative ways.

The designated agency responsible for digital transformation must be able to articulate the challenges; define the objectives; design and plan appropriate programmes that would enable the objectives to be met; implement the programmes as well as monitor and measure the progress and impact. These processes will involve consultations with diverse stakeholders and must be supported by a comprehensive communication strategy that details the type and level of engagement of users, clients and beneficiaries. Periodic revisiting and appropriate adjustment of the processes will ensure the achievement of these objectives. It is also recommended that this agency reports to the Prime Minister or highest level of authority in the country so that the digital transformation initiative maintains a high priority on the national agenda.

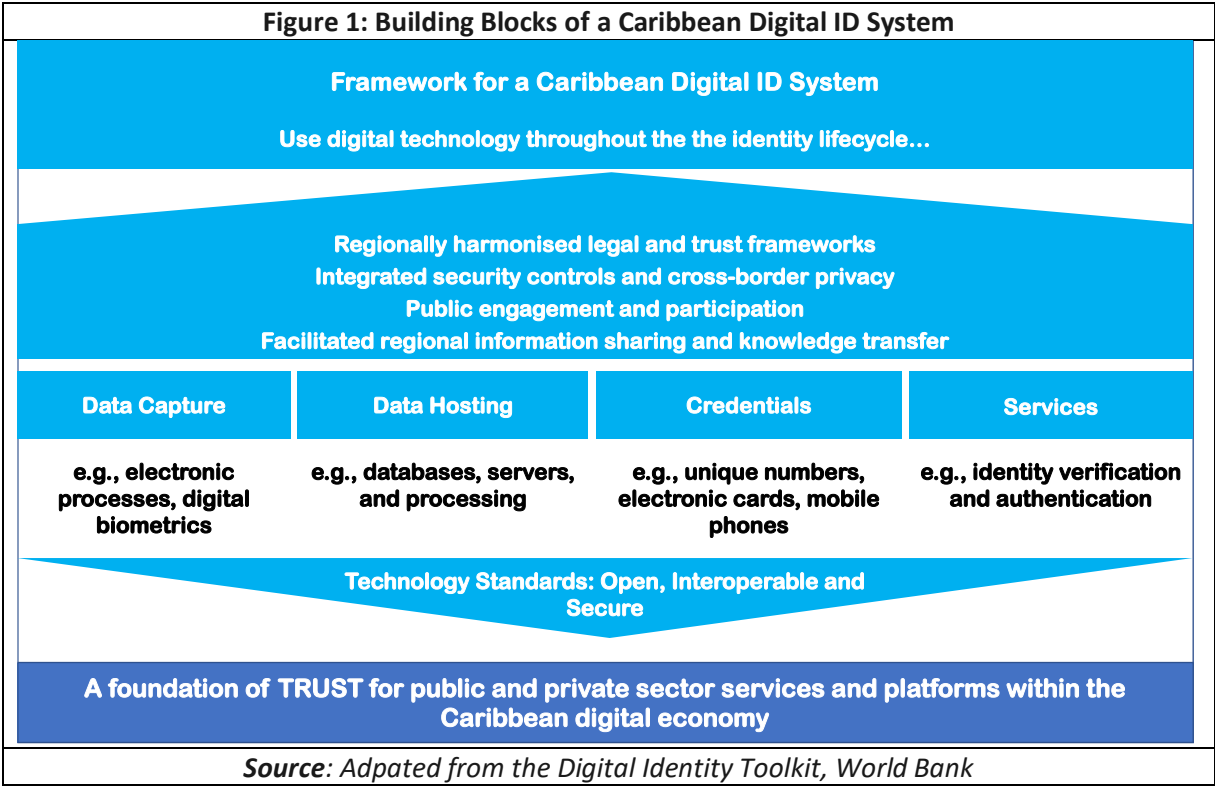
Caribbean nations seeking to put in place a 21st Century Government may have limited insight into the challenges and opportunities for effective ICT adoption. In such cases, benchmarking can be an important tool for enabling effective decision-making and planning; building metrics for monitoring and measuring progress; developing best practices; evaluating utility, costs, benefits and impact.

Finally, and very importantly, appropriate systems must be implemented to mitigate the potential negative societal impacts. Provisions must be made to value and protect citizens, their personal and professional endeavours, their intellectual, digital and physical possessions and their privacy. In this regard, data protection and privacy legislation are a critical enabling component of this ecosystem.

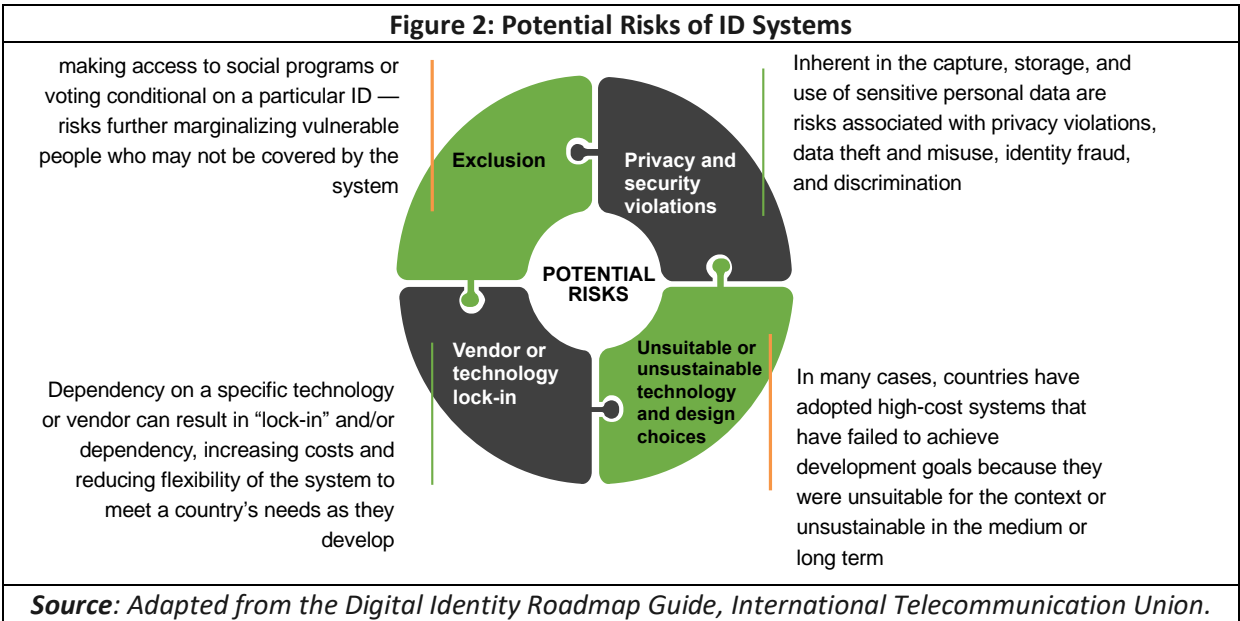
4 Digital Identity for 21st Century Government

At the core of 21st Century Government is the need to provide each citizen with a seamless and comprehensive digital profile that they will use in their interactions with the government and even the private sector. The concept of digital identity systems adopts fully an electronic identification framework that enables the implementation of the core characteristics of 21st Century Government. Such

characteristics include electronic databases and credentials, biometric recognition for automated replication of identity records and authentication, mobile devices and applications, and interoperability platforms (see Figure 1), all of which improve the accuracy of identity data and increase the efficiency of identity verification and authentication.

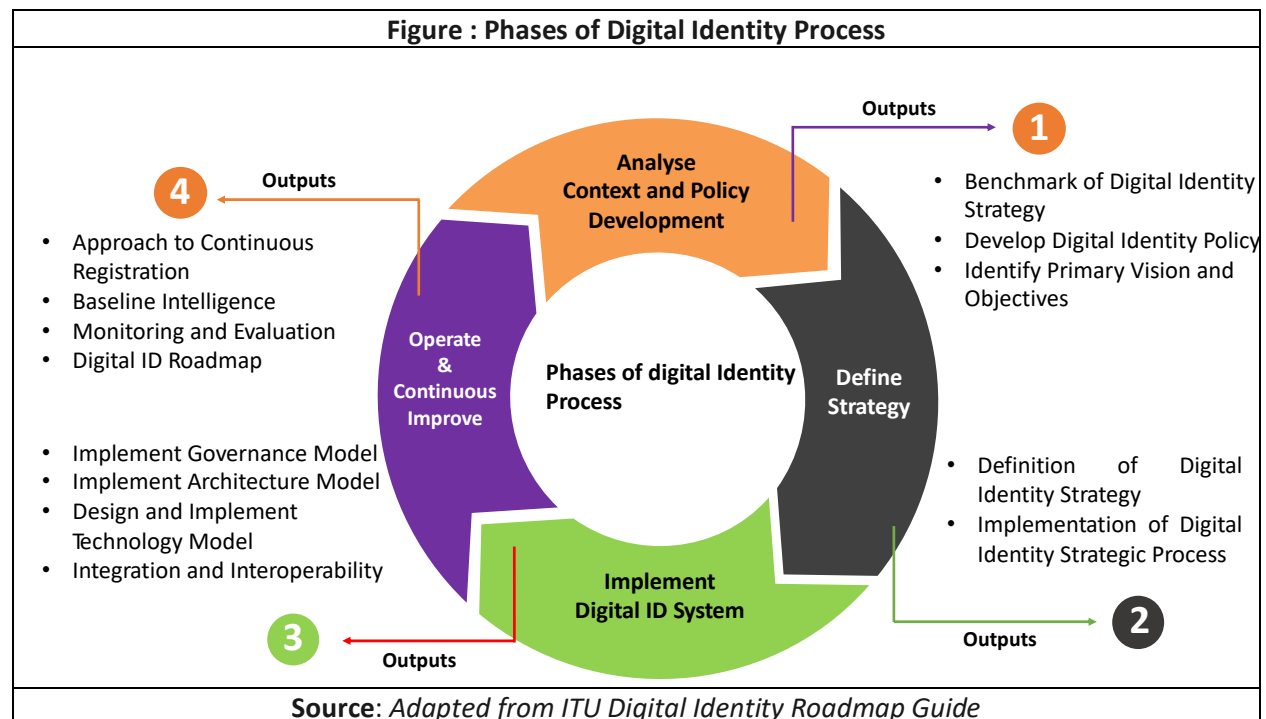


Importantly, however, while ID systems can create opportunities to further development national goals, they also present multiple important challenges and risks (see figure 2) that must be properly managed.



5 Scope of the National Digital Identification System

Prior to planning and implementing, the stakeholders involved in the development of the digital identity system should carefully assess the context and situation in which they will have to operate. This is necessary in order to establish the correct baselines that will subsequently ensure the greater precision during the implementation and operation process. This section provides an overview of the phases of the Digital Identity Process (see figure 3), defined as:



5.1 Phase 1 – Context Analysis and Policy Development

The objective of this phase is to develop and articulate a policy vision for digital identity that takes into account national objectives and circumstances in the context of regional and international trends, benchmarks and imperatives for technology and services. The policy vision must take into consideration the unique characteristics that shape the environment in which the digital identity system will be implemented and operated.

A comprehensive exploration of issues such as national culture, traditional public interfacing mechanisms, the accessibility of digital infrastructure and devices, trust in the government are influencing elements that may impact the implementation and operation of a digital identity system. These elements must be identified at the outset of the development process so that appropriate countermeasures can be investigated and determined in advance. For instance, a country with a large elderly demographic might decide to emphasize simplicity and accessibility, rather than efficiency driven through complexity. On the other hand, a nation with a relatively young population might opt for a digital identity system that integrates seamlessly into the digital fabric of citizens' already hyper-connected lives. The choices that govern each implementation must be tailored to each specific situation.

5.1.1 Benchmark of Digital Identity Strategy

Global experience in developing, specific systems for digital identity management, constitute an invaluable repository of information that can be used to gather relevant lessons-learned to build upon.

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




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

- **Case Selection:** cases to be analysed are selected from the public and private sectors based on a series of defined criteria; it is important to ensure a good balance in terms of geography, population size, layers of government, diversity of cultures and styles of government. A sample of different stages of advancement with respect to development and implementation of digital identity initiatives should be considered, from preliminary investigation or early development stage through to full deployment.
- **Case Analysis and Classification:** each selected case is analyzed and classified according to a well-defined set of criteria which facilitate understanding of the different approaches followed during the design and implementation phases, the primary objectives, the tools (laws, plans, actions, etc.) developed to implement the strategy, and the outcomes achieved.
- **Case Evaluation:** once the analysis is complete, good practice elements are derived to support objectives and priorities in line with the vision defined in the Digital Identity Strategy.

5.1.2 Develop Digital Identity Policy

The first phase of implementing a national digital identification system focuses on the planning and drafting of a comprehensive digital identity policy. All stakeholders involved in the development of the policy must carefully assess the context and situation in which the core digital ID is to be deployed. The digital identity policy draws from the work done in benchmarking the digital identity strategy. It establishes the correct baseline that would ensure proper implementation and sustainable operation of the **categories of digital identification** (see Figure 4) to build upon the core digital ID system.

Figure 4: Categories of Digital Identification

		
Foundational <i>Formal establishment of identity</i>	Functional <i>Specific sectors or use-cases</i>	Non-Governmental (Transactional) <i>Digital Financial & Mobile Network Operator Services</i>
<ul style="list-style-type: none">• Foundational ID systems and registries (e.g. national ID, population and Civil Registry)• Multi-purpose, serving as an authoritative source of the unique legal identity of people.	<ul style="list-style-type: none">• Created to address the specific needs of an individual sector (for instance, the healthcare or the transportation sectors, voting, taxation, social protection, travel, and more).	<ul style="list-style-type: none">• Intended to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors.
Source: Adapted from ID4D Practitioner's Guide, World Bank and the Digital Identity Roadmap Guide, International Telecommunication Union.		

Context analysis and identification of national specifics and peculiarities of the current identity landscape, that is, “understanding the status quo” is a valuable exercise for Caribbean countries planning new identification systems and those desiring to optimise existing systems.

Factors including cultural nuances, prevailing citizen identification models, citizens accessibility to digital means and trust in the government are critical. Elements of these factors must be identified at the outset of the development process, so that appropriate measures can be determined and mitigating plans setup beforehand. Implementation choices should be tailored to address each specific national situation.

Maximising the utility of identification in the medium- and long-term, requires a holistic view of existing ID systems and stakeholders within the **identity ecosystem** and assessment of their strengths and weaknesses, particularly regarding system coverage, quality and the enabling legal framework.

In addition, consultations with government stakeholders and diagnostics of the status quo should also include the perspectives of end-users as well as various government and private-sector institutions that would rely on these systems. It is recommended that governments consult with individual stakeholders to understand their particular experiences and challenges with the existing ID systems. A practical step towards understanding the current ID system landscape would be to take stock of the identity ecosystem and its stakeholders. See table 1 below:

Table 1: Identity ecosystem stock-taking			
System	Providers	Users	Supporters / Enablers
Foundational <ul style="list-style-type: none">- National ID- Civil register- Population register, etc.	Example <ul style="list-style-type: none">- Ministry of National Security- Ministry of Justice- Ministry of Health, Local governments, etc.	<ul style="list-style-type: none">- Other agencies- Private sector- Donors- Individuals	<ul style="list-style-type: none">- Regulator / oversight body- Ministry of finance- Ministry in charge of Digital Government- Ministry in charge of digital infrastructure, including broadband connectivity- Agency in charge of Cybersecurity technology- Civil society- Donors and other development partners, etc.
Functional <ul style="list-style-type: none">- Voter registry- Social assistance registries- Taxpayer registry- Passport- Driver’s license- Land registry- Property registry, etc.	Example <ul style="list-style-type: none">- Electoral commission- Ministry of Social Affairs- Revenue Department- Immigration Department- Transportation Department- Ministry of Interior, etc.		
Non-Governmental (Transactional) <ul style="list-style-type: none">- Financial sector IDs- SIM card registry- Credit registry- Donor program registries, etc.	Example <ul style="list-style-type: none">- Banks- Mobile operators- Credit agencies- Donors and International Organizations		
Source: ID4D Diagnostic Guidelines, World Bank			

5.1.3 Identify primary vision and objectives

Upon clearly identifying the environment and the context in which the digital ID system will operate and a review of comparable initiatives has been performed, it is important to articulate the primary vision and objectives the digital ID system has to satisfy.

At this point, the primary goals and objectives should already be apparent to the drafters of the digital identity framework. The goals and objectives ought to be finalized at this time, as the decisions and choices to implement the digital ID system will most likely rest on the ability to meet these specific needs. It is for this reason that a careful identification of objectives and principles are determined, to provide an appropriate guide for the subsequent 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 entities. Public consultations and working groups involving public sector, private sector, and civil society should be established as well, based on the complexity of the landscape and initiatives. This group of stakeholders will be responsible for validating the overall vision and scope of the strategy, setting implementation-level objectives, evaluating the current situation, prioritizing objectives in terms of impact on society and citizens, and ensuring the availability of necessary financial resources. Coordination of the initiative by a lead project authority or agency is desirable. The primary objectives and principles and the good practice elements arising from the context analysis during Phase 1 should be taken into account.

5.2.1 Definition of Digital Identity Strategy

At this stage, a lead government agency should be identified to undertake the drafting of the Digital Identity Strategy. The Digital Identity Strategy should provide the overall digital identity direction for the state. It includes expressing a clear vision and scope; setting objectives to be accomplished within a specific time frame; and prioritising these in terms of impact on society, the economy and infrastructure. Moreover, it should identify possible courses of action; incentivise implementation efforts; and drive the allocation of required resources to support all of these activities. The drafting of the Digital Identity Strategy could involve dedicated working groups either to focus on specific topics or to draft different sections of the Strategy.

The formal adoption of the Digital Identity Strategy development has to be ensured, and section 5.3.4 “Implement Adoption Model” provides approaches on adoption. The broad availability of the strategy will both ensure that the general public is aware of government’s priorities and objectives for digital identity and also support efforts to raise public awareness. This official adoption process will vary by country and will be based on how well the Strategy is defined in the legal and regulatory framework.

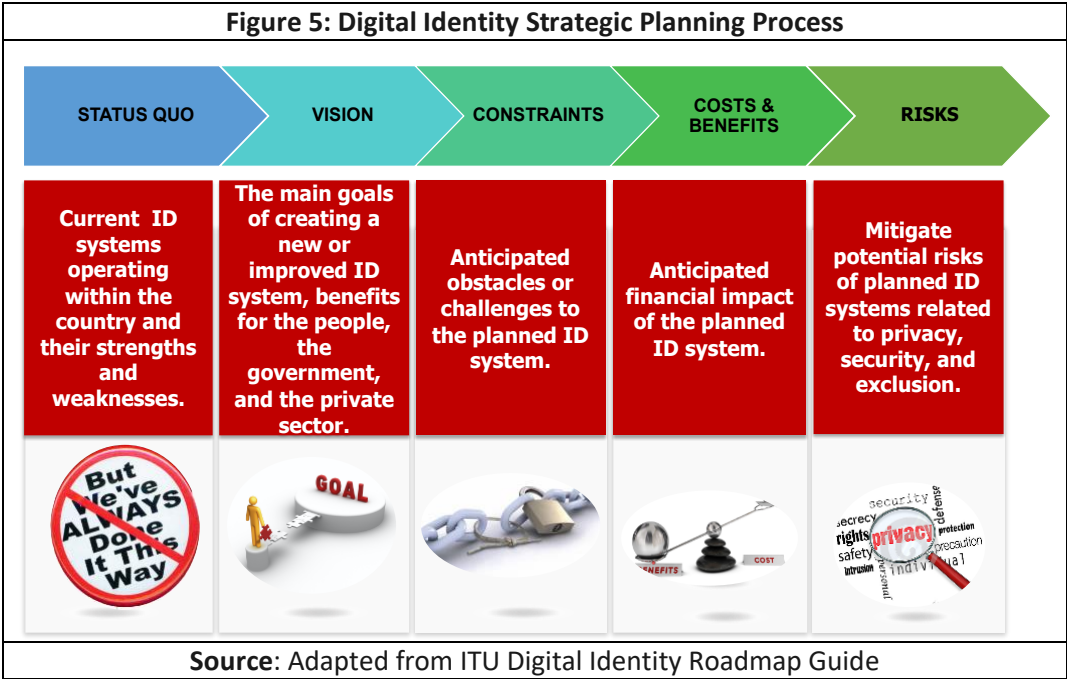
5.2.2 Implementation of Digital Identity Strategic Process

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 an important part of its development. The implementation phase should be centered on a clearly defined Action Plan, which

can support the effective implementation of the strategy to guide the various activities that are envisioned.

In the Action Plan, the specific initiatives are identified and detailed within each focus area that will support the objectives and achieve the desired outcomes, as well as coordinate efforts and pool resources. The timeline and dependencies between tasks and efforts needed for the implementation of these initiatives should be ranked in accordance with national priorities to ensure that resources are appropriately leveraged. Initial thought should be given to approaches for consideration of the governance, architectural and adoption models at this stage.

As part of the definition of the implementation process, specific metrics and key performance indicators, tied to the objectives, should be identified to establish baselines and facilitate monitoring and evaluation of the efficiency and effectiveness of the initiatives during and beyond implementation. See figure 5 for digital identity strategic planning process.



5.3 Phase 3 – Implement Digital ID System

The Digital Strategy in Phase II would have put forward a clear governance model and mandate that defines the roles and responsibilities of key stakeholders. This phase will include the identification of the digital ID governance, architectural, technology design and adoption models to be supported and the entities assigned with responsibility for the overall management, implementation and ongoing oversight of the digital ID operations.




Focus will be placed on assessing the technologies related to the digital identification lifecycle, setting the context to address the technology challenges that practitioners and stakeholders may have to address

while evaluating or implementing digital ID systems. The importance of open and interoperable standards for a secure and efficient digital identify platform will be explored.

5.3.1 Implement governance model

This will focus on the identification of the digital ID governance model to be adopted and the entity assigned with responsibility for the overall management, implementation and ongoing oversight of the digital ID operations, through a central regulatory or government authority.

Figure 6: Typical digital ID Governance Models

		
Government as Identify Provider	Government as Regulator & not Identity Provider	Government as Regulator, Identity Broker & Clearing House
<ul style="list-style-type: none"> Government has a primary role in digital ID and acts as regulator and Identity Provider at the same time. 	<ul style="list-style-type: none"> Government acts as regulator of digital ID and procures digital identity services for citizens. Issue laws, regulations, criteria, procedures, controls and manage and accredits entities that acts as Identity Providers. 	<ul style="list-style-type: none"> Active role in economic relationship between citizens, Identity Providers and service providers. Identity Broker as an intermediary between Service Providers and Identity Providers.
<i>Source: ID4D Practitioner's Guide, World Bank</i>		

Regardless of the Governance Model adopted, checks and balances must be maintained over organisations charged with this oversight responsibility. Ultimately, a robust multi-layered institutional governance structure is needed.

Table 2 below provides examples of ID authorities. Those that are agencies or directorates within an existing ministry, which reports to that ministry. There are however several different potential governance models for autonomous agencies, including reporting directly to the executive branch (e.g., a Cabinet) or to a board of directors.

Table 2: Examples of ID Authorities

Organisational Type	Examples
Autonomous, with direct Cabinet- or Executive-level reporting	<p>India: Initially, the Unique Identification Authority of India (UIDAI) was set up as an organisation attached to the Planning Commission of India, reporting to a Chairman who had the status of a cabinet minister. Following the passage of the Aadhaar Act in 2016, UIDAI became a statutory authority responsible for implementation of the Act, under the Ministry of Electronics and Information Technology.</p> <p>Ghana: The National Identification Authority of Ghana was set up as an organisation within the Office of the President.</p>
Autonomous, governed by a board representing stakeholders	<p>Nigeria: The National Identity Management Commission (NIMC) is governed by a board of 18 individuals representing different government agencies and stakeholders.</p>

	<p>Philippines: The Philippine Statistics Authority (PSA) is governed by a board of representatives of 28 Government departments and commissions and one representative of the private sector, chaired by the Secretary of Socioeconomic Planning. The Philippine Identification System (PhilSys) Policy and Coordination Council, comprising a subset of these departments but also chaired by the Secretary of Socio-Economic Planning, will oversee the implementation of the PhilSys.</p>
Agency or directorate within an existing Ministry	<p>Thailand: The Bureau of Registration Administration (BORA) under the Department of Provincial Administration (DOPA) of the Ministry of Interior.</p> <p>Argentina: The Registro Nacional de las Personas (RENAPER) is a directorate under the Ministry of Interior and Transportation.</p>
<p><i>Source: Adapted from the Digital Identity Toolkit, World Bank</i></p>	

5.3.1.1 Define and review regulations or laws

For most countries in the Caribbean region, existing legislation that would impact digital identity is dispersed 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 effective measures for amendments instituted.

During the review of laws and regulations, the broader ICT policies and regulatory environment should also receive attention. Digital identity is an integral element of ICT and would benefit from policies that aim 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 development.

5.3.2 Implement architecture model

The architectural model can follow different approaches: a centralised system with a single identity provider that collects and manages all the information and data; a distributed system with multiple identity providers; or a 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 and options.

Defining a pilot scope initiative that validates specific use cases (for example, a particular government sector that delivers social services, utilising one (1) unique identity provider) could help in identifying required functional and infrastructure adjustments in terms of architecture scalability to be addressed in the future. Three typical architectural models:

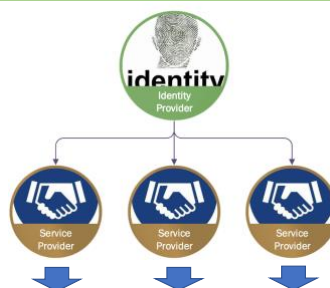
Figure 6: Architectural Model Option 1

Architecture Model: Option 1

A centralised identity system where a single identity acts as an Identity Provider that authenticates users to Service Providers and transfers their attributes. **This option may be a logical starting point for most Caribbean countries.**

Such systems are often designed to streamline service delivery, enable data aggregation and provide a single view of users across multiple Service Providers.

One Unique Identity Provider



- Bilateral contract to be signed
- Limited privacy assurance
- Direct integration of entities that may result in additional effort and time
- Potential for large user base to leverage

Source: Adapted from ITU Digital Identity Roadmap Guide

Figure 7: Architectural Model Option 2

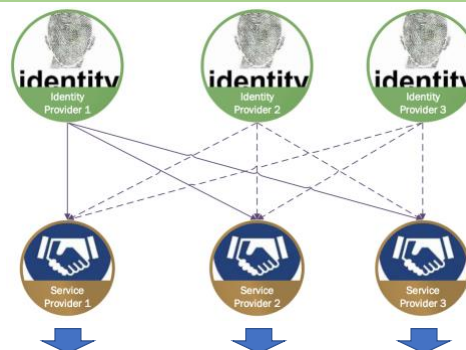
Architecture Model: Option 2

In distributed identity systems multiple Identity Providers collect, store and manage user credentials and attributes interacting with multiple Service Providers. **This option may be the next evolution of Identity Providers in the Caribbean.**

These systems leverage the capabilities of multiple Identity Providers and differentiators for completion of identity processes. In particular for identity proofing.

Extensive experience in managing identities and identify solutions already placed in branches that facilitate the interaction with citizens are key elements for selecting the scenario. Moreover, users are allowed to choose between different Identity Providers.

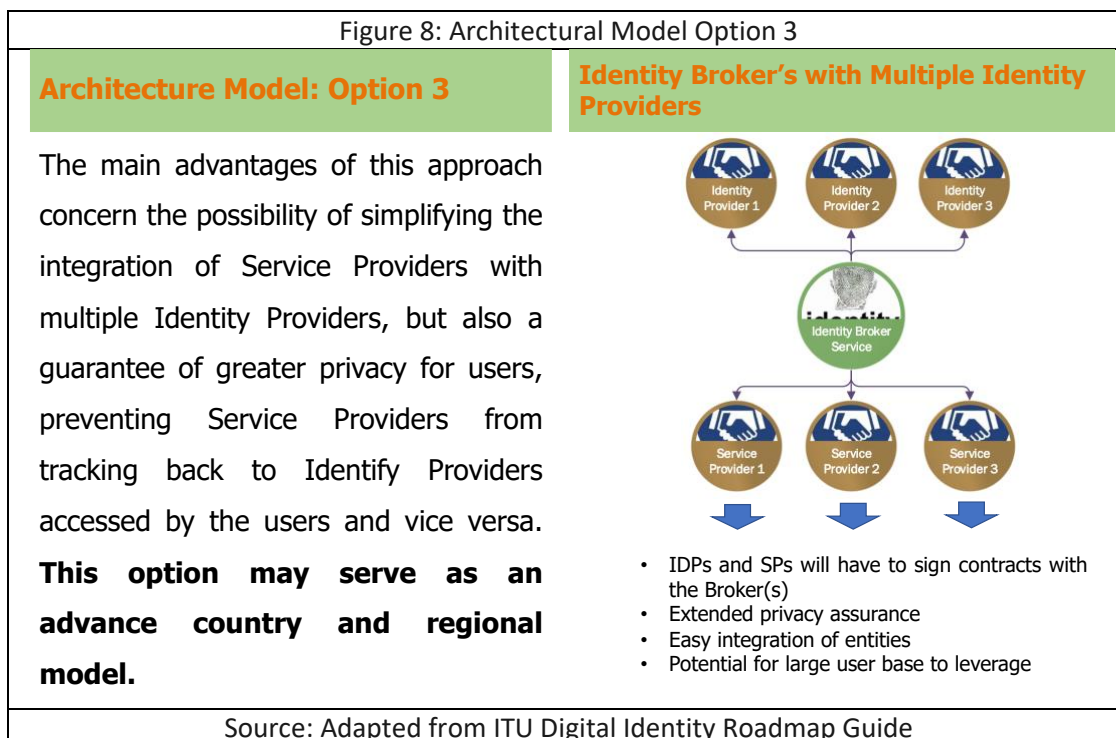
Multiple Identity Providers



- Bilateral contract to be signed
- Limited privacy assurance
- Direct integration of entities that may result in additional effort and time
- Potential for large user base to leverage

Source: Adapted from ITU Digital Identity Roadmap Guide

Figure 8: Architectural Model Option 3



5.3.3 Design and implement technology model

Technology plays a crucial role in the development of a digital identity in a country, dimensions that come into play includes technology impact on data privacy and security, digital identity lifecycle and intra- and inter-country interoperability.

An important part of the technology approach is an assessment of a country's underlying, enabling technology infrastructure. Deployment of high-speed broadband Internet is often a necessary requirement for an online identity solution. Although the region has made significant progress in this area, many Caribbean countries are still working to develop and deploy adequate broadband infrastructure. 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, point-of-sale devices, automatic teller machines, agent networks, and payment networks to benefit from digital identity.

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

The guideline, standards and approaches included in this section are intended to inform technology choices and the development of the technical specifications for the digital ID systems. Countries may choose to customise and adapt the models and recommendations in this section to meet specific country needs, resources, implementation and institutional capacity.

5.3.3.1 Privacy and security

Implementing a privacy-and-security-by-design approach is important for maintaining user privacy and the security of systems that process, collect, store, use, and disseminate personal data is a fundamental concern for ID systems. This approach requires complementary controls working together throughout the digital ID system lifecycle. This includes:

1. **Legal controls** for privacy and data protection, as well as information and cyber security;
2. **Management controls** for monitoring, oversight and risk management;
3. **Operational controls** that promote security awareness, training and detection; and
4. **Technology controls** that limit and protect the processing of personal data and ensure the physical and virtual security of systems that process this data (adapted from ISO/IEC 29100).

Table 3: Privacy and data protection enhancing technologies and operational controls		
Strategy		Recommended technology controls (not exhaustive)
Data-oriented	Minimise the collection and processing of personal data to limit the impact to privacy of the system.	<ul style="list-style-type: none"> - Collecting and sharing minimal data - Anonymisation and use of pseudonyms when data is processed.
	Hide personal data and their interrelationships from plain view to achieve “unlinkability” and unobservability, minimising potential abuse.	<ul style="list-style-type: none"> - Encrypt data when stored or in transit - End-to-end encryption - Key management/key obfuscation - Anonymisation and use of pseudonyms or tokenisation for data processing - “Zero semantics” or randomly generated ID numbers - Attribute-based credentials (ABCs).
	Separate, compartmentalise, or distribute the processing of personal data whenever possible to achieve purpose limitation and avoid the ability to make complete profiles of individuals.	<ul style="list-style-type: none"> - Tokenisation or pseudonymisation by sector - Logical and physical data separation (e.g., of biographic vs. biometrics) - Federated or decentralised verification.
	Aggregate personal data to the highest level possible when processing to restrict the amount of personal data that remains.	<ul style="list-style-type: none"> - Anonymise data using k-anonymity, differential privacy and other techniques (e.g., aggregate data over time, reduce the granularity of location data, etc.).
Process-oriented	Inform individuals whenever their data is processed, for what purpose, and by which means.	<ul style="list-style-type: none"> - Transaction notifications - Data breach notifications.

Give individuals tools to control the processing of their data and to implement data protection rights and improve the quality and accuracy of data.	<ul style="list-style-type: none"> - User-centric identity services - Attribute-based credentials
Enforce a privacy policy that complies with legal requirements.	<ul style="list-style-type: none"> - Role-based access control with two-factor authentication - Remote access.
Demonstrate compliance with the privacy policy and applicable legal requirements.	<ul style="list-style-type: none"> - Tamper-proof logs - Audits.
Source: ID4D Practitioner's Guide, World Bank	

Table 3 above, provides a snapshot of some common practices in implementing privacy and data protection enhancing technologies and operational controls. The specific privacy and security enhancing operational and technical controls adopted by the digital ID system will depend on context and other technical design choices, in country.

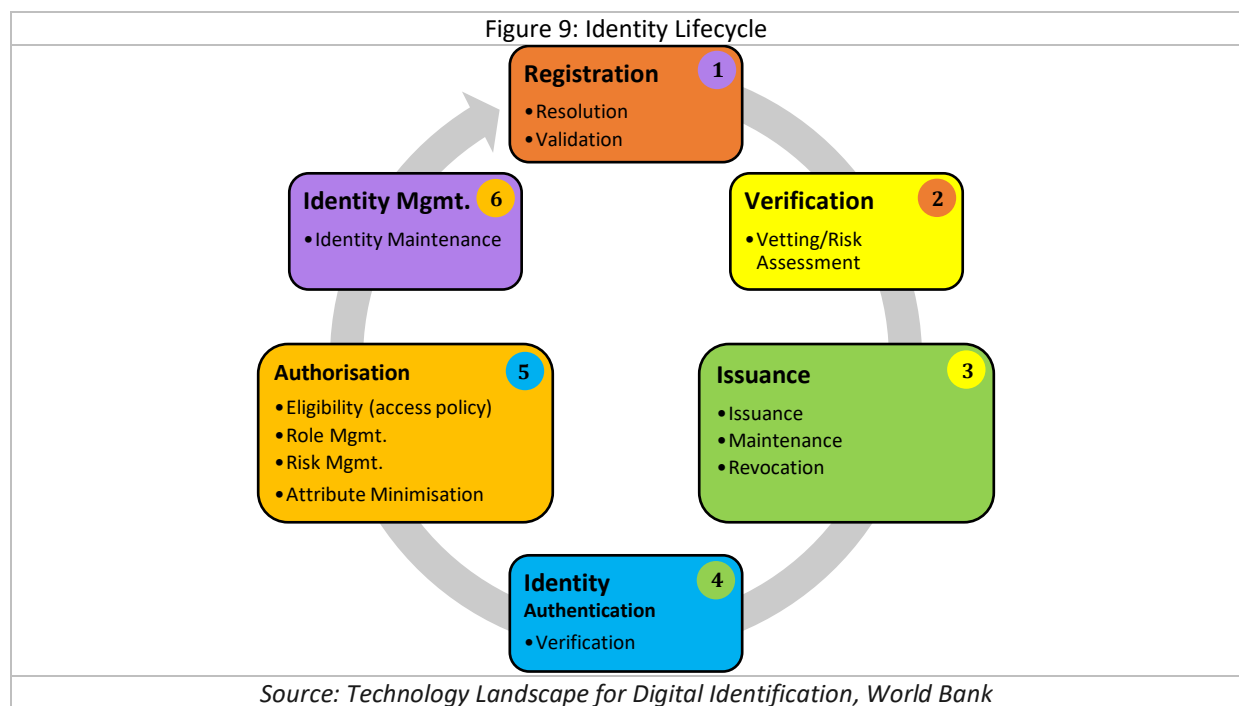
The important categories of technologies and strategies include:

- Encryption
- Digital certificates and PKI
- Tokenisation
- Platforms for personal access and control
- Tamper-proof logs
- Data center security
- Implementing a cybersecurity program

5.3.3.2 *Technology Impact on the Digital Identity Lifecycle*

Understanding the Identity Lifecycle

The identity lifecycle groups the identity process into its key steps and provides the framing for the different enabling technologies that support the various stages of the identification lifecycle. The identity lifecycle starts when a person applies for a digital ID and ends when the record is removed, and the ID is invalidated owing to death, request for removal by the individual, or some other event.



Registration (Identity Proofing)

The foundational aspect of one's identity is established during the registration process, when an applicant provides evidence of his or her identity to the credential-issuing authority. If the person reliably identifies himself or herself, the authority can assert that identity with a certain level of identity assurance. Once verification is completed, biometric registration and de-duplication will bind the applicant to his or her identity claim, which will then be used during subsequent identity interactions.

Registration may start with Resolution, the process of uniquely distinguishing an individual in a given population or context. The next step is Validation, where the authority determines the authenticity, validity, and accuracy of the identity information the applicant has provided, and relates it to a living person. This is followed by Verification, the establishing of a link between a claimed identity and the real-life subject presenting the evidence. The final step is Vetting/Risk Assessment, assessing the user's profile against a watch list or a risk-based model.

Issuance (Credential Management)

Credential Management starts with Issuance, which is the process of creating and distributing virtual or physical credentials like decentralized identity proofs, e-passports, digital ID cards, and driver's licenses; and a unique identifier (with central biometric authentication), such as the Aadhaar system in India. The other steps are Maintenance (the retrieval, update, and deletion of credentials) and Revocation (the removal of the privileges assigned to credentials). Interoperability of these credentials for authentication is becoming increasingly important for intra-country and inter-country service delivery, as can be seen in the European Union (EU), East African Community (EAC), and West Africa regions.

Identity Authentication

Authentication is the process of verifying an identity claim against the registered identity information. Such information could be a personal identification number (PIN), a password, biometric data such as a fingerprint, a photo—or a combination of these. Challenges in this phase include how to reduce processing time, improve accuracy of matching for authentication, ensure a seamless experience for applicants, mitigate challenges with network connectivity, counter fraudulent behaviour, and find affordable hardware and software solutions.

Authorization











Authorization typically takes place after an individual's claim of identity is authenticated and defines access rights (or grants) that a Relying Party has associated with the identity aligned to the relationship between the individual and the Relying Party (e.g., a financial institution)—independent of the Identity Provider (e.g., the National Identification Authority). In more advanced authorization schemes the grants are contextual and dynamic. Because this report is focused on Identity Providers and the provisioning of identities, not Relying Parties and the authorizations that they may associate with an identity, it will not explore the various authorization processes and technologies emerging in the market today.





















Identity Management (Identity Maintenance)

Identity management or maintenance is the ongoing process of retrieving, updating, and deleting identity attributes or data fields and policies governing users' access to information and services. Identity retrieval involves fetching a user's identity attributes. Security policies should be used to enforce access privileges to ensure that only authorized individuals can access, alter, or delete identity information, and to ensure that the actions are audited and cannot be repudiated. This approach ensures that resources are made available only to authorized users according to rules of access that are defined by attributes and policies. Credentials may be deactivated, revoked, or made dormant as a result of certain events, and identity information may be updated or deleted.

Mapping Technologies to the Identity Lifecycle

Embarking on a detailed assessment of the technologies, requires an in-depth understanding on how they enable or affect a certain step in the Identity Lifecycle. For example, fingerprint and vascular capture and matching technologies are applicable in Registration, Authentication and Identity Management, but not in Issuance. Likewise, blockchain is applicable only after Identity Proofing. Figure 10 indicates which technologies can enable or affect a certain step in the Identity Lifecycle.

Figure 10						
Technologies		Registration (Identity Proofing)	Issuance (Credential Lifecycle Management)	Identity Authentication	Identity Management	
Credential Technologies	Biometrics	 Fingerprint Recognition	✓		✓	✓
		 Iris Recognition	✓		✓	✓
		 Face Recognition	✓		✓	✓
		 Voice Recognition	✓		✓	✓
		 Behaviour Recognition	✓		✓	✓
		 Vascular Recognition	✓		✓	✓
		 Rapid DNA Profiling DNA Matching	✓		✓	✓
	Cards	 Nonelectronic Cards	✓	✓	✓	✓
		 RFID Non-Smart Cards	✓	✓	✓	✓
		 Contact Smart Cards	✓	✓	✓	✓
		Contactless Smart Cards or Documents	✓	✓	✓	✓
		Biometric System on Card	✓	✓	✓	✓

	Supporting Technologies for Cards	 Bar Codes	✓	✓	✓	✓
		 Magnetic Strips	✓	✓	✓	✓
		 Machine-Readable Text	✓	✓	✓	✓
	Mobile	 One-Time Passwords	✓	✓	✓	✓
		 Smart ID	✓	✓	✓	✓
		 Cryptographic SIM	✓	✓	✓	✓
		 Registration Using Mobile Devices	✓	✓	✓	✓
		 Mobile Connect	✓	✓	✓	✓
		 Authenticator Mobile App		✓	✓	✓
		 Trusted Platform Mobile (TPM)		✓	✓	✓
Authentication and Trust Frameworks: Technologies and Protocols	 Blockchain			✓	✓	
	 FIDO Universal Authentication Framework			✓	✓	
	 FIDO Universal Second Factor (USC)			✓	✓	
	 OAuth 2.0			✓	✓	
	 OpenID Connect			✓	✓	
	 SAML			✓	✓	
Analytics	 Risk Analytics	✓		✓	✓	
	 Predictive Analytics	✓				
	 Business Activity and Operational Analytics					
	 Biographic Matching (Fuzzy Search)	✓		✓	✓	
Source: Technologv Landscape for Digital Identification. World Bank						

Source: Technology Landscape for Digital Identification, World Bank

Technology Assessment Framework

The following assessment framework can be used as a reference to enable implementers to determine the optimal approach to manage the deployment of technologies at each stage in the Identity Lifecycle. The six (6) assessment parameters are presented below:

Maturity: How long has the technology been in use? How well is it understood?

- *Longevity:* How long has the technology been available and in use (regardless of adoption)
- *Interoperability:* Is the technology based on Standards (preferably open)? How interoperable is the technology with the other technologies in the identity ecosystem?

Performance: How well suited is the technology for performing the required task?

- *Throughput:* How many identity service requests can the technology process per unit of time?
- *Response time:* How quickly can the system respond to an individual request?
- *Accuracy:* How frequently does the technology generate false matches or false rejections during matching or how often does the technology fail to enroll a specific percentage of the population?
- *Stability:* To what degree will the technology be resistant to change in the face of external forces such as age, environmental conditions, pace of development, and others?

Scalability: Can use of the technology be scaled as needed?

- *Data scalability:* How well can the technology adapt to an increase or decrease in the volumes of data being processed or the number of people in the system?
- *Simplicity of computational resources:* How easily can system architects procure and install the necessary hardware and software?

- *Simplicity of network infrastructure:* How easily can system architects establish data transfer channels especially in bandwidth constrained domains?

Adoption: To what degree do system operators and users accept the technology?

- *Integration:* Can we integrate the technology with legacy and future systems?
- *Ease of learning:* How easily can system operators learn to use the technology?
- *User interface (UI) simplicity:* How complex are the technology's software and hardware interfaces?
- *Simplicity of training:* How easy is it to train someone to use the technology?
- *Cultural acceptance:* What are users' feelings and thoughts about the technology?

Security: How secure is the technology against unauthorized access and usage?

- *Circumvention resistance:* How well protected is the technology from hackers and other attacks?
- *Resilience:* How quickly and effectively can the technology recover from an attack or breach?
- *Transmission security:* How secure is the information-exchange channel?

Affordability: How economical is the technology?

- *Hardware affordability:* How cost-effective is the dedicated hardware?
- *Software affordability:* How cost-effective is the dedicated software?
- *Revenue opportunities:* To what degree could we recoup our investment in the technology through interoperability arrangements such as fees from private-sector service providers for conducting e-KYC (Know Your Customer) using the government unique ID database?
- *Time cost savings:* How cost-effective is the technology based on time required to be fully functional?

Three-Point Rating Scale

The Technology Assessment Framework uses a three-point scale of "high," "medium," and "low" to represent responses to each of the above questions. "High" is the maximum score or best outcome for a particular parameter, while "low" is the worst outcome or lowest score for a parameter.

Credential Technologies

Figure 11 below are the results of the categorises for the three (3) credential sub-technologies evaluated using the technology assessment framework: biometrics, cards and card supporting. A biometric identifier can be used as a credential once it has been registered with the issuing authority. Cards and smart cards can be used to store identity information and can be used as evidence to support an identity claim.

Figure 11											
Technology Parameters	Biometrics			Smart Cards					Card Supporting Technologies		
	Finger	Facial	Iris	Nonelectronic Card	RFID Non-Smart Card	Contact	Contactless	Biometric System on Card	Barcode	Magnetic Stripe	Machine-Readable Text
Maturity	High	High	High	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Longevity	High	High	High	High	Medium	Medium	Medium	Medium	High	High	High
Interoperability	High	High	High	High	High	High	High	High	Medium	Low	Medium
Performance	High	High	High	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Throughput	High	High	High	N/A	N/A	Medium	Medium	Medium	High	Medium	High
Response Time	High	High	High	N/A	Medium	Medium	Medium	Medium	High	Medium	High
Accuracy	High	High	High	N/A	N/A	N/A	N/A	Medium	Medium	Medium	Medium
Stability	High	High	High	High	Medium	High	Medium	Medium	Low	Medium	N/A
Scalability	High	High	High	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium
Data Scalability	High	High	High	Low	Low	Medium	Medium	Medium	Medium	High	High
Simplicity of Computational Resources	High	High	High	High	High	High	High	High	High	High	Medium
Simplicity of Network Infrastructure	High	High	High	N/A	High	Medium	Medium	High	High	High	High
Adoption	Medium	Medium	Medium	High	Medium	Medium	Medium	Medium	High	Medium	High
Integration	High	High	High	High	High	High	High	Medium	High	High	High
Ease of Learning	Medium	Medium	Medium	High	High	High	High	High	High	High	High
UI (User Interface) Simplicity	High	High	High	N/A	High	High	High	High	High	High	High
Simplicity of Training	Medium	Medium	Medium	High	High	High	High	Medium	High	High	High
Cultural Acceptance	High	High	Medium	High	Medium	High	Medium	Medium	High	Medium	High
Security	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium	Medium	Medium
Circumvention Resistance	Medium	Medium	Medium	Medium	High	Low	Low	High	High	Low	High
Resilience	Medium	Medium	Medium	N/A	N/A	N/A	N/A	N/A	Medium	Low	N/A
Transmission Security	Medium	Medium	Medium	N/A	Medium	High	High	High	Medium	Medium	Medium
Affordability	Medium	Medium	High	High	Medium	Medium	Medium	Medium	High	Medium	High
Hardware Affordability	Medium	Medium	Medium	High	High	High	High	Low	High	High	High
Software Affordability	Medium	Medium	Medium	N/A	High	High	High	Medium	High	High	High
Revenue Opportunities	High	High	High	High	High	High	High	High	High	Medium	High
Time Cost Savings	High	High	High	High	High	High	High	High	High	High	High

Source: Technology Landscape for Digital Identification, World Bank

Credential Technologies

Figure 12 below are the results of the for the four (4) Mobile Technologies evaluated using the technology assessment framework. Mobile devices can be used to store identity information and can be used as evidence to support an identity claim.

Figure 12							
Technology Parameters	Mobile Technologies						
	OTP	Smart ID	Cryptographic SIM	Registration Using Mobile Device	Mobile Connect	Authenticator Mobile App	TPM
Maturity	High	Medium	High	Medium	Medium	High	Medium
Longevity	High	Medium	High	Medium	Medium	High	High
Interoperability	N/A	High	High	Low	High	N/A	Medium
Performance	Medium	High	High	Medium	High	Medium	High
Throughput	N/A	High	High	High	High	N/A	High
Response Time	High	High	High	High	High	High	High
Accuracy	High	High	High	High	High	High	High
Stability	Medium	High	High	Medium	High	Medium	High
Scalability	Medium	High	High	Medium	High	Medium	Medium
Data Scalability	Low	High	High	High	High	Low	High
Simplicity of Computational Resources	High	High	High	Medium	High	High	Medium
Simplicity of Network Infrastructure	High	High	High	High	High	High	High
Adoption	High	Medium	Medium	High	High	High	Medium
Integration	High	High	High	High	High	High	High
Ease of Learning	High	High	Medium	High	High	High	Medium
UI (User Interface) Simplicity	High	High	Medium	High	High	High	High
Simplicity of Training	High	High	Medium	High	High	High	High
Cultural Acceptance	High	Medium	High	High	High	High	High
Security	Medium	Medium	Medium	Medium	Medium	Medium	High
Circumvention Resistance	Medium	High	Medium	Medium	High	Medium	High
Resilience	Medium	Medium	Medium	N/A	Medium	High	High
Transmission Security	Medium	High	High	Medium	High	Medium	High
Affordability	Medium	High	High	High	High	Medium	Medium
Hardware Affordability	Medium	High	High	High	High	Medium	Medium
Software Affordability	Medium	High	High	High	High	Medium	Medium
Revenue Opportunities	N/A	High	High	High	High	N/A	High
Time Cost Savings	High	High	High	High	High	High	High

Source: Technology Landscape for Digital Identification, World Bank

Authentication and Trust Frameworks: Technologies and Protocols

Figure 13 below are the results of the six (6) technologies and protocols for authentication and trust frameworks evaluated using the technology assessment framework. Federated authentication provides a standards-based solution to the issue of trusting identities across diverse organizations which may even be across countries. This requires the establishment of a trust framework between the identity provider and the relying party (service providers). A trust framework is a set of business, legal, and technical rules that members of a community agree to follow to achieve trust online.

Analytics Technologies

Figure 13 below are the results of the four (4) analytics technologies evaluated using the technology assessment framework. Analytics technologies use mathematical, statistical, and predictive modelling techniques that leverage a variety of data sources to find meaningful insights and patterns in data. In digital ID systems, analytics can be used to build a comprehensive identity for an individual by combining data from multiple sources. Use of such analytics adds a layer of intelligence to an individual's identity profile. In this report, the following are examined: risk analytics, predictive analytics, business activity and operational analytics, and biographic matching (fuzzy search).

Figure 12

Technology Parameters	Authentication and Trust Frameworks: Technologies and Protocols						Analytics Technologies			
	Blockchain	FIDO (UAF)	FIDO (U2F)	OpenID Connect	OAuth 2.0	SAML	Risk	Predictive	Business Activity and Operational	Biographic Matching (Fuzzy Search)
Maturity	Medium	Medium	Medium	Medium	Medium	High	Medium	Medium	Medium	Low
Longevity	Medium	Medium	Medium	High	Medium	High	Medium	Medium	Medium	Low
Interoperability	Medium	High	High	Medium	Medium	High	Medium	Medium	Medium	Low
Performance	Medium	High	High	High	Medium	High	Medium	Medium	Medium	Medium
Throughput	Medium	High	High	High	Medium	N/A	High	High	High	Low
Response Time	Medium	High	High	High	Medium	High	Medium	Medium	Medium	Medium
Accuracy	High	N/A	N/A	High	High	N/A	Medium	Medium	Medium	Medium
Stability	High	N/A	N/A	N/A	N/A	High	High	High	High	Medium
Scalability	Medium	High	High	High	Medium	High	Medium	Medium	Medium	Medium
Data Scalability	Medium	High	High	High	Medium	N/A	High	High	High	Medium
Simplicity of Computational Resources	Medium	High	High	High	N/A	High	Low	Low	Low	Low
Simplicity of Network Infrastructure	Medium	High	High	N/A	N/A	High	Medium	Medium	Medium	Medium
Adoption	Medium	High	High	High	High	High	Medium	Medium	Medium	Medium
Integration	Low	High	High	High	High	High	High	High	High	Low
Ease of Learning	Medium	High	High	High	High	High	Low	Low	Low	Low
UI (User Interface) Simplicity	Medium	High	High	High	High	High	High	High	High	Medium
Simplicity of Training	Medium	High	High	High	High	High	Low	Low	Low	Low
Cultural Acceptance	Medium	High	High	High	High	High	Medium	Medium	Medium	Medium
Security	Medium	High	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Circumvention Resistance	Medium	High	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Resilience	High	High	High	Medium	Medium	N/A	Medium	Medium	Medium	Medium
Transmission Security	Medium	High	High	N/A	Medium	Medium	Medium	Medium	Medium	N/A
Affordability	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Hardware Affordability	Medium	Medium	Medium	Medium	Medium	N/A	Medium	Medium	Medium	Medium
Software Affordability	Medium	Medium	Medium	Medium	Medium	High	Low	Low	Low	Medium
Revenue Opportunities	Medium	High	High	High	High	Medium	High	High	High	Low
Time Cost Savings	Medium	High	High	Medium	Medium	High	Medium	Medium	Medium	Low

Source: Technology Landscape for Digital Identification, World Bank

5.3.3.3 *Hosting Infrastructure*

Digital ID systems are built on strong IT infrastructure, including computing resources, hardware, applications, network and server architecture, and more. The IT architecture that interlocks all these technologies together is a critical determining factor of the reliability, security, and flexibility, with major implications for program cost, sustainability, suitability for different use cases, the ability to protect personal data, and the adaptability of the system over time.

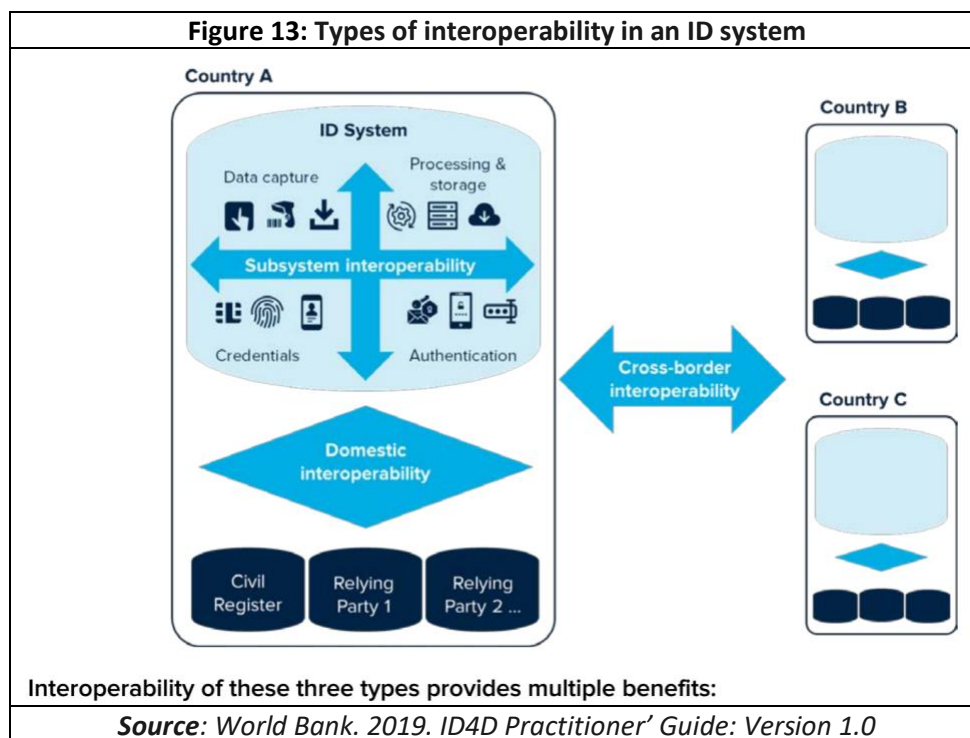
Devising an IT architecture that balances all these factors effectively is a major undertaking. A detailed assessment of key decisions should be completed to take into account various Hosting options for data, services, and related applications.

5.3.4 *Interoperability and Mutual Recognition*

Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems. Specifically, interoperability allows different functional units (e.g., systems, databases, devices, or applications) to communicate, execute programs, or transfer data in a manner than requires the user to have little or no knowledge of those functional units.

For digital ID systems, this occurs at three levels, see Figure 13 below:

1. Between ID subsystems (components/devices). Within the ID system itself, standards-based technical interoperability allows different components and devices to communicate with each other and work together. This includes, for example, interoperability between fingerprints captured with a scanner device and the deduplication engine, interoperability between smartcards and readers, interoperability of biometric formats captured during registration with those captured during authentication, interoperability between images captured by devices from different vendors, etc.).
2. With other domestic systems. ID systems must be interoperable with other systems—such as the civil registry and service providers that are relying parties of the system—in order to exchange data or facilitate queries. Communication with other systems may be provided through various interoperability layers, web services and APIs, or direct connections.
3. With ID systems in other jurisdictions. Cross-border frameworks for interoperability and mutual recognition allow credentials from one country to be accepted in other countries. This includes, for example, the acceptance of standards-compliant passports across the globe (covered by the ICAO DOC 9303 standard), as well as regional frameworks for the mutual recognition of ID credentials e.g., the European Union’s electronic identification.



5.3.4.1 Mutual recognition of IDs across borders

When digital IDs issued by one country are recognized by other countries, whether for face-to-face or online transactions, they become a powerful driver of economic and regional integration, including to promote safe and orderly migration. Importantly, digital ID systems can be mutually recognized without the need for harmonisation into a common system through the use of minimum standards to facilitate interoperability and legal and trust frameworks (e.g., for levels of assurance) to set rules and build confidence in respective systems.

The following are two typical regional use cases:

- migration, through which a physical or digital identity credential can be recognized as a travel document in lieu of a traditional passport, and;
- cross-border electronic transactions as part of the digital economy, which can be facilitated when a digital identity issued by one country is recognized for transactions online in another country.

5.3.4.2 Understanding the levels of assurance

A level of (identity) assurance (LOA) is the certainty with which a claim to a particular identity during authentication can be trusted. Higher levels of assurance reduce the risk of a fraudulent identity and increase the security of transactions, but also can increase the cost and inconvenience to ID holders and relying parties, which could lead to potential exclusion. Therefore varying requirements of different use cases with respect to LOA should be considered. For example, biometric-based authentication is likely to be inappropriate for use across all use cases because some transactions (e.g., scheduling a medical appointment through a website) carry less risk.

Assurance levels depend on the strength of the Identity proofing process and the types of credentials and authentication mechanisms used during a transaction. For identity proofing, the level of assurance depends on the method of identification (e.g., in-person vs. remote), the attributes collected, and the degree of certainty with which those attributes are verified (e.g., through cross-checks and deduplication). For authentication, the level of assurance depends on the type of credential(s), the number of authentication factors used (i.e., one vs. multiple), and the cryptographic strength of the transaction.

The LOAs selected depend on the use case; some sectors and types of transactions will require higher levels of assurance than others. For example, changing an address may rely on a lower level of assurance than changing a password. Financial and health services often require a higher level of assurance than others due to the sensitivity of the data that is collected and maintained in those systems. **Ideally, the ID system's authentication architecture will be able to provide multiple levels of assurance appropriate to different use cases** (see Table 4 for examples).

Table 4: Levels of Assurance			
	Low (level1)	Substantial (level2)	High (level3)
Identity assurance level (IAL)	Self-asserted identity (e.g., email account creation on web), no collection, validation or verification of evidence.	Remote or in-person identity proofing (e.g., provide credential document for physical or backend verification with authoritative source), address verification required, biometric collection optional	In-person (or supervised remote) identity proofing, collection of biometrics and address verification mandatory.
Authentication assurance level (AAL)	At least 1 authentication factor—something you have, know, or are (e.g., password or PIN)	At least 2 authentication factors (e.g., a token with a password or PIN)	At least two different <i>categories</i> of authentication factors and protection against duplication and tampering by attackers with high attack potential (e.g., embed cryptographic key material in tamper-resistant hardware token + PIN, biometrics with liveness detection + PIN/smart card)
Federation Assurance Level (FAL)	Permits the relying party to receive a bearer assertion from an identity provider. The identity provider must sign the assertion using approved cryptography	FAL1 + encryption of assertion using approved cryptography	FAL2 + user to present proof of possession of a cryptographic key reference in the assertion
Level of risk taken by relying party	mitigated	low	minimal
Source: World Bank. 2019. ID4D Practitioner' Guide: Version 1.0			

Key Assumptions:

It is assumed that Caribbean countries that desire to benefit from mutually recognised digital identities will seek to adopt the following key principles:

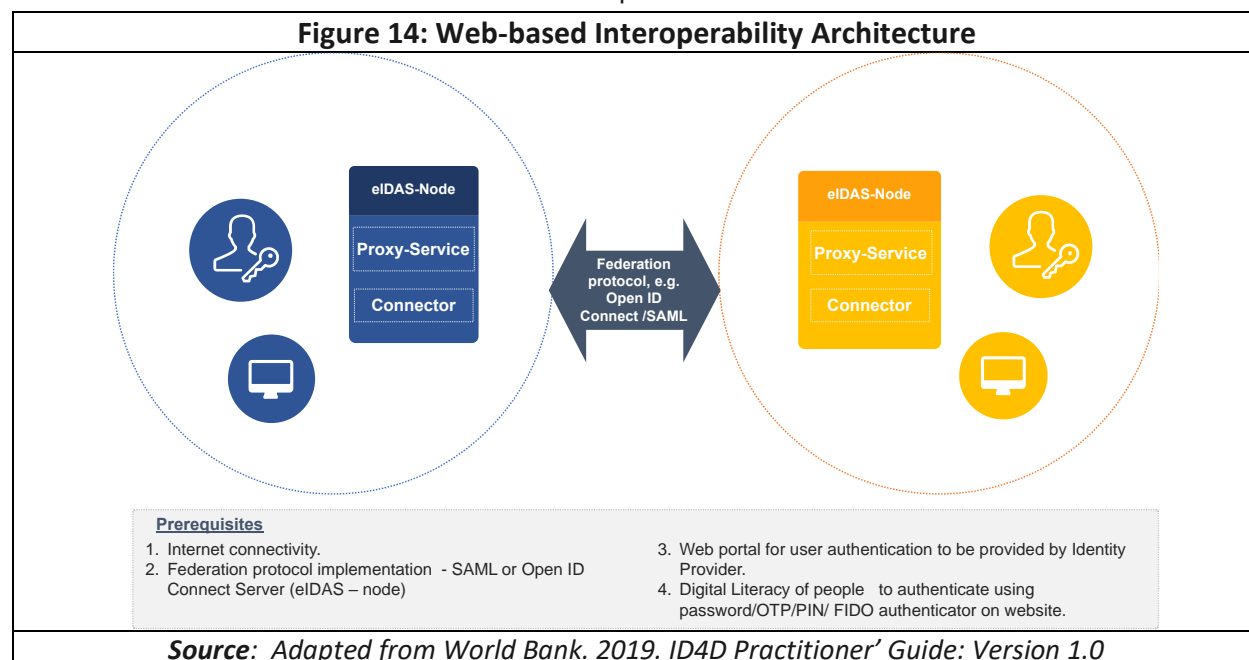
1. **Harmonization:** The legal, process, data and technical standards are defined and agreed upon by the respective countries of the region for cross-border mutual recognition.
2. **Levels of Assurance:** The level of assurance required for access to a service and the assurance level of the credentials/authentication mechanisms is defined and agreed upon by the respective countries.

3. **Flexibility:** Countries may have one of more different forms of credentials/authentication mechanisms which may be same or different when compared to other states (e.g. Password, PIN, OTP, smart card, FIDO authenticator, mobile ID, biometrics).

5.3.4.3 Options for Regional Digital ID Interoperability

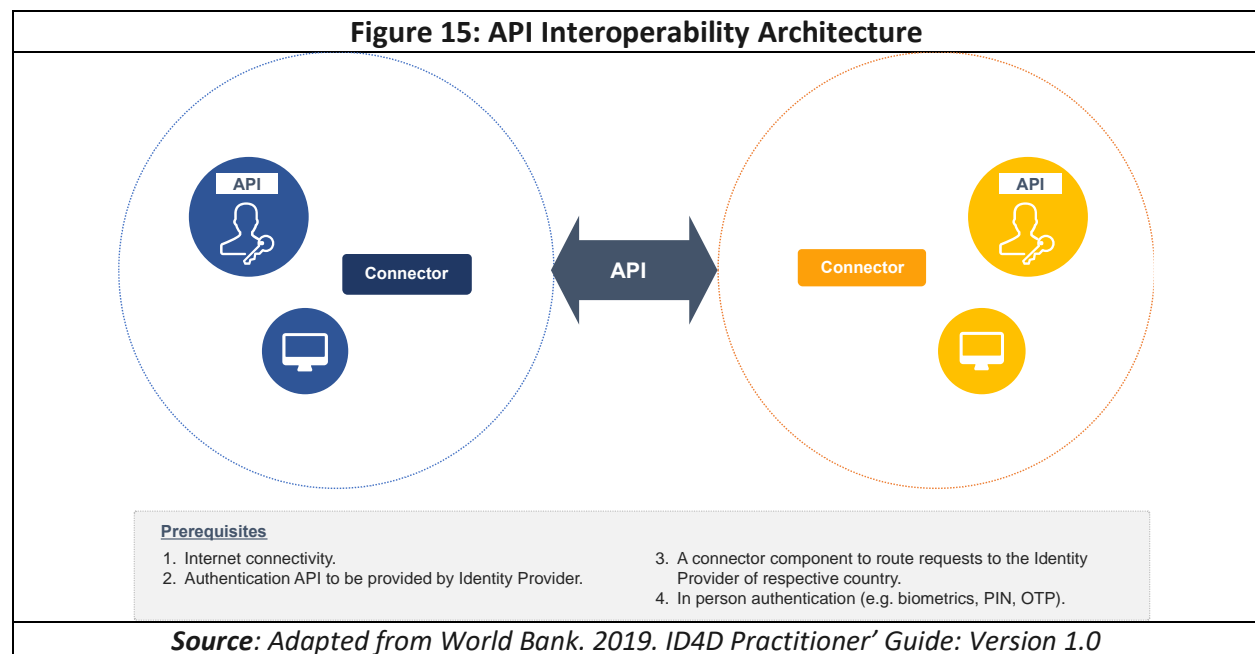
Option #1. WEB-BASED

- Online web-based authentication using federation protocol (e.g. SAML or Open ID connect)
- Architecture used for eIDAS framework in European Union territories



Option #2. API

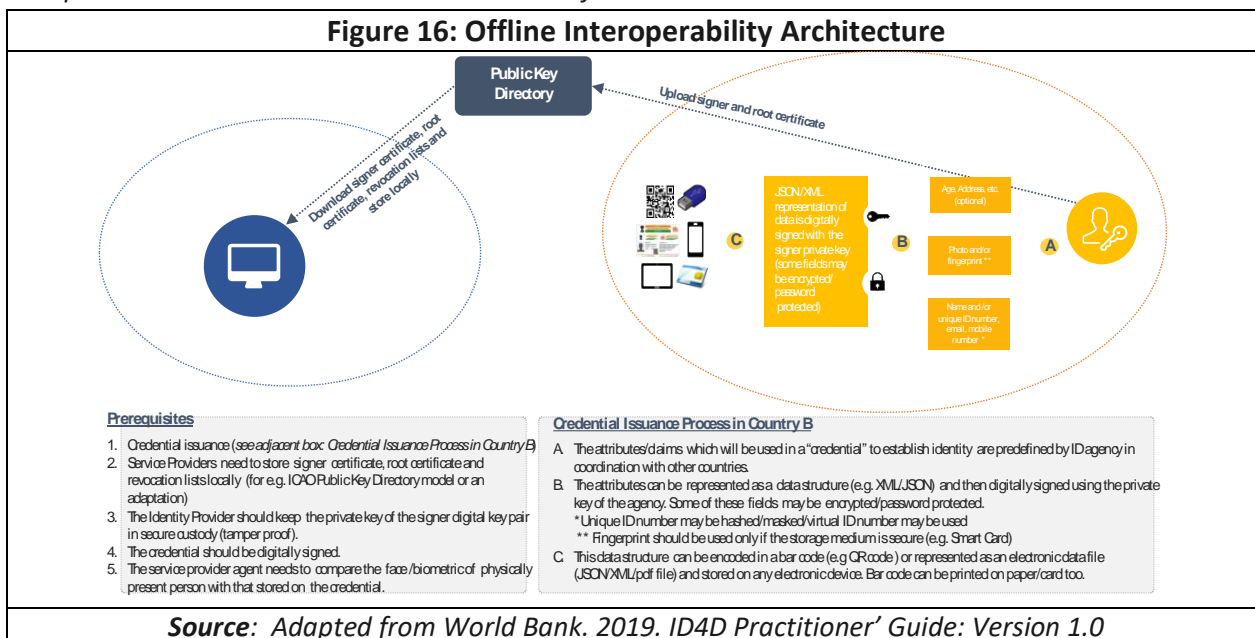
- Online authentication using an API approach
- Architecture used Latin America and Caribbean Islands



Option #3. OFFLINE

- Offline authentication
- Architecture inspired by the ICAO biometric passport used for cross-border identification and India's offline authentication architecture with Aadhaar

Note: The offline architecture can be used when there are connectivity challenges and/or to handle exception scenarios when online authentication fails.



5.3.5 Implement adoption model

Table 5: Approaches for Adoption	
Citizen-Side	Service Providers-Side
<ol style="list-style-type: none">1. Value of digital identity usage for users2. Issuing of digital identity: voluntary vs mandatory3. Convenient enrolment process4. Levering other digital identities systems5. Usability6. Security and privacy7. Communication and awareness for the citizenship	<ol style="list-style-type: none">1. Promoting or enforcing the public administration participation2. Engaging with the private sector operators3. Introducing Identity Broker4. Fostering Federation of Identity Providers
<i>Source: Adapted from ITU Digital Identity Roadmap Guide</i>	

5.3.5.1 Citizen-Side

Value of digital identity usage for users

The most critical drivers for citizen adoption are the real value in terms of public and private services that can be accessed with a digital identity. Regardless of the percentage of users that are issued digital identity, its success is demonstrated by the services that can be accessed by citizens and the number of accesses completed.

Consequently, governments should promote the participation in the system among public institutions so that real value can be provided to the citizens. The public institution 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 and;
- Other key services.

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

Governments therefore should define a comprehensive strategy and roadmap for the involvement of service providers that is aligned to the vision behind the national digital identity framework. Outcomes measured and represented by a service catalogue of needs must be defined in advance and constantly updated.

Issuing of digital identity: voluntary vs mandatory

Voluntary-based: A decision must be made whether or not a digital identity is mandatory for citizens. In a voluntary 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 forced to hold an Aadhaar-issued digital identity. They must however own one in order to participate in certain limited specific national or governmental welfare or social programs that provide basic social benefits.

Mandatory-based: This approach does not allow the citizen to decide whether or not to request a digital identity. It is usually adopted in combination with initiatives where the enrolment of a digital identity is created in parallel with another ID document, such as a physical ID card. Forms of mandatory possession of digital identity can be critical for promoting adoption, but may not guarantee use of that identity if it is not combined with an extensive service offering. Estonia, for example, has established a system that provides state-issued digital identities to almost the entirety of its citizenry (current figures stand at around 98% adoption). Citizens can access a broad suite of services, such as e-government, healthcare, security and safety, business and finance and educational services.

This method has been extremely successful for Estonia, but it can be challenging for countries which do not already have a national ID card or finds it challenging (politically and logistically) to simultaneously manage digital and physical identities.

Special attention should be paid to policies, laws, and regulations related to mandatory possession of a digital identity that have the potential to exclude significant portions of the population. A strict conditioning of essential government services on the presentation of a specific identification can be problematic, if access is not universal or is applied in discriminatory ways. This problem can be particularly acute when a digital identity is required for services (for example, financial services that utilise know-your-customer as a condition for access) but are provided only to nationals, unless alternative means are made for residents and other groups ordinarily living in a country, for example, migrants, refugees, and stateless persons, to access public and private sector services. A number of jurisdictions have seen legal challenges to the constitutionality of mandatory ID systems, including India, Jamaica, and Kenya.

Levering other digital identities systems

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

Such an approach can yield multiple benefits:

- Governments leverage a significant number of already verified active users;
- User convenience is enhanced as the risk of forgetting credentials is minimized.

Citizens typically do not access government services online on a daily basis and users typically forget passwords for sites they do not visit regularly. Conversely, banking, telecommunications or other private services are often accessed very regularly. Leveraging the same digital identity reduces the overhead of re-verifying lost credentials and simplifies the number of personal credentials users have to manage.

- Governments reduce the effort and costs related to credential management.

Usability

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

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

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

Security and privacy

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

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

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

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

Since multiple stakeholders are involved, citizens, identity providers, service providers, identity brokers, etc., national leaders and policy makers would be advised to adopt a security-by-design approach, which ensures the digital identity system is adequately secured against both external attacks and internal abuses. The consequences of a security breach can have a very destructive impact on the level of stakeholders' trust in the digital identity system.

Another critical element having a direct impact on the level of trust accorded to any digital identity system is the safeguards protecting user privacy. The recent introduction of norms such as the European Union General Data Protection Regulation (GDPR) reveals the high degree of attention this issue is attracting from legislators and society, globally.

Since the use of services that rely on digital identity entails the sharing of a certain amount of personal data that may be very sensitive in nature (such as biometric data), national leaders and policy makers should make every effort to reassure users that privacy is respected and protected at each step of the process. This can be achieved through a sound legal and regulatory framework and, more generally, by

complying with the privacy-and-security-by-design approach, referred to in section (5.3.3.1 Privacy and Security).

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

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

The following are a number of safeguards that can be adopted to ensure a higher level of both data protection and data privacy, refer to (Table 3: Privacy and data protection enhancing technologies and operational controls) for more technical example:

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

Communication and citizen awareness

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

5.3.5.2 Service Providers-Side

Promoting or mandating public administration participation

The success of a digital identity system is measured by the number and extent of services that citizens can access, both public and private. Government action should aim to involve public and private digital service providers, according to the alignment of their digital identity strategy and related objectives to government.

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

Governments might decide to request that certain digital public services be exclusively accessed through digital identities. This requires service providers to employ the identity management system used by the

government at the national level. What might appear to be a simple operation at first glance, however, requires careful designing of the digital identity systems employed. The design will need to focus on integration and interoperability, taking into account technical and other standards that can facilitate this. It will also require meticulous planning in terms of deployment, in the light of the central role played by the identity system. Examples of success stories include Oman and Tanzania, where the state provides public services that can be accessed only by users who have a digital identity.

Engaging with private sector operators

Service providers play a critical role in the success of a national digital identity system. Extending the service offering to the private sector can be a compelling driver for accelerating citizen adoption. Since private providers will decide on their participation in the system based on a cost-benefit analysis, a critical part of facilitating the participation of private service providers in the enhancement and proliferation of the digital identity system will be to provide **real advantages** and **cost reductions** in service offerings.

National digital identity systems incorporate high levels of identity proofing (in-person verification) to the benefit of public service providers. As highlighted in Figure 17, private service providers have different requirements in terms of levels of identity proofing. Consequently, the price they are willing to pay for identity services is different from that of government departments. Simple e-commerce operators do not have the same needs, for example, self-declared identity for payments for which a credit card is appropriate, as banks and financial or telecoms operators, which have more critical transactions and compliance obligations.

While this certainly holds true for entities with highly polarized needs, such as, online commerce vs banks, it is also true that each private entity will prefer a specific identity proofing approach according to its specific business model (see Figure 17).

Figure 17: Comparison of two options for identity proofing		
	Option 1 - Private Operators Leveraging Highly Trusted Identity	Option 2 - Private Operators Leveraging "Self Asserted" Identity
Identity Proofing Level	High	Low
Authentication recom.	Strong and Weak Authentication	Weak Authentication
Identification of the Target Market Segments	Banking, Insurance, Telecommunications, Public services and Health care	Media and Web 2.0 Communication
	Traditional production (Automot.), Retail, E-commerce, Online info / entertaimt., Utilities, Transport.	
Private sector operators that requires identities with high level of proofing as enabling factor for their business value proposition.		Private sector operators that leverages a "Self Asserted" identity as enabling factor for a better customer insight or completing micro payments
Source: ITU Digital Identity Roadmap Guide		

Several drivers should be considered when considering cost-benefit analysis:

- Contribution to value:
 - Leverage a larger user base faster
 - Improve the user experience: users can access new services more quickly and with less effort because they can share trusted information that has already been vetted, for example, single sign-on, one click to purchase

- Take advantage of additional services such as payments, logistics and shipping services that can be offered by identity providers
 - Customize user experience through qualifying attributes
 - Enhanced focus on core offering, eliminating the need for involvement in non-core services.
- Cost reduction:
 - Reduce costs associated with identification proofing processes
 - Reduce costs associated with credential management
 - Reduce costs for starting and managing new services.

Introducing an Identity Broker

The Identity Broker is an intermediary that connects Identity Providers and Service Providers, providing further protection for privacy and acts as a clearing house for participants. Identity Brokers are essential, when there are multiple Identity Providers that need to be integrated with multiple Service Providers. This is even more imperative when small and medium public or private providers are willing to participate in the ecosystem.

The primary benefits of introducing an Identity Broker are:

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

Success stories related to the adoption of Identity Brokers can be found in the UK, Germany, Canada and the US, where in each case one Identity Broker is implemented. In the case of the Netherlands and the use of Idensys, multiple Identity Brokers are conceived at the national level.

Fostering Federation of Identity Providers

It is anticipated that one of the key drivers of the involvement of Service Providers is the opportunity to access a large user base. Governments can leverage this goal in many ways. A typical option would involve private operators as Identity Providers using a transparent selection process determined on criteria defined by the government.

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

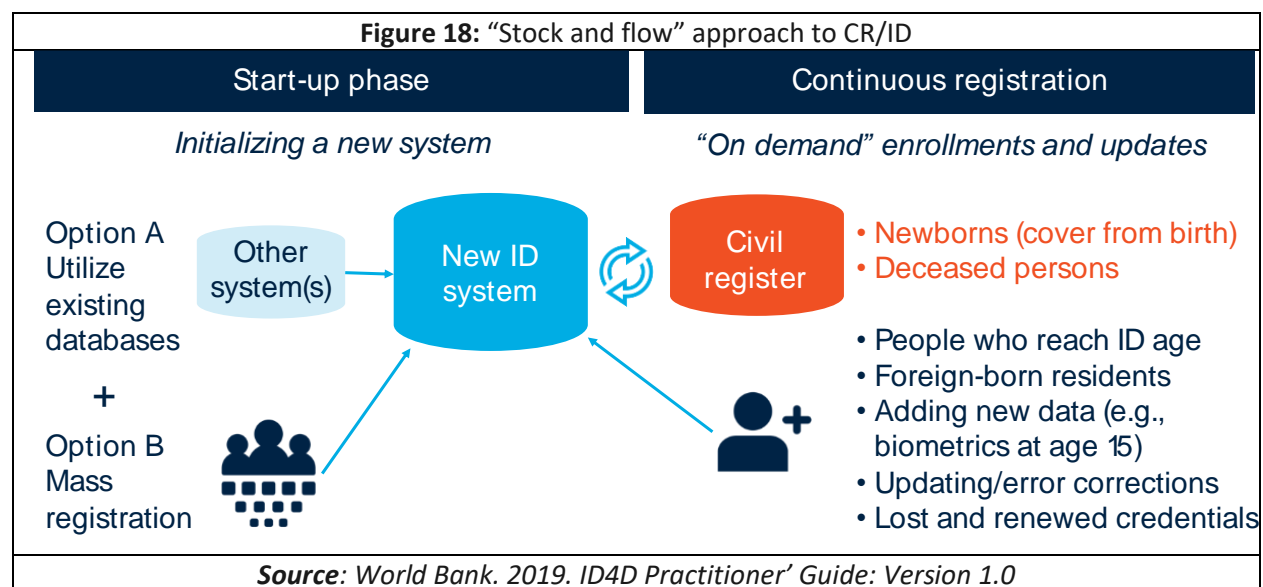
5.4 Phase 4 - Operate and continuously improve

This phase will place focus on the importance of developing baseline metrics to enable better monitoring of actions, identify opportunities for potential improvement and sustainability and the Digital Identification Roadmap.

5.4.1 Approach to Continuous Registration

To ensure sustainability, maximum coverage, inclusion and quality and reduce cost when introducing a foundational identity system, countries should assess the readiness of the Civil Registry (CR) system to support such an effort. For example, the CR system should be sustainable, sufficiently digitalised and the data it holds should be reliable enough to play a role in the Identity proofing process. However, CR systems in many countries, particularly low and middle-income economies, have historically been of poor quality and low coverage because of underinvestment, legacy legal frameworks and processes, and limited incentives for citizens to register their vital events and for governments to strengthen CR systems.

As a result, many people alive today were not registered at birth or their birth registration records have been lost or destroyed. Many people only register a birth when they have to (e.g., to apply for their first passport, which requires someone to prove where they were born). Likewise, a country's CR system only covers births and other vital events that have occurred in that country's territory and jurisdiction (that may also include vital events of nationals residing overseas), which means that migrants and refugees who were born overseas are most likely to be excluded. See figure 18 below.



5.4.2 Baseline Intelligence

The establishment of baseline metrics will enable better monitoring of actions and highlight areas of potential improvement. Adopting this approach in the initial phase, 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.

5.4.3 Monitoring and Evaluation

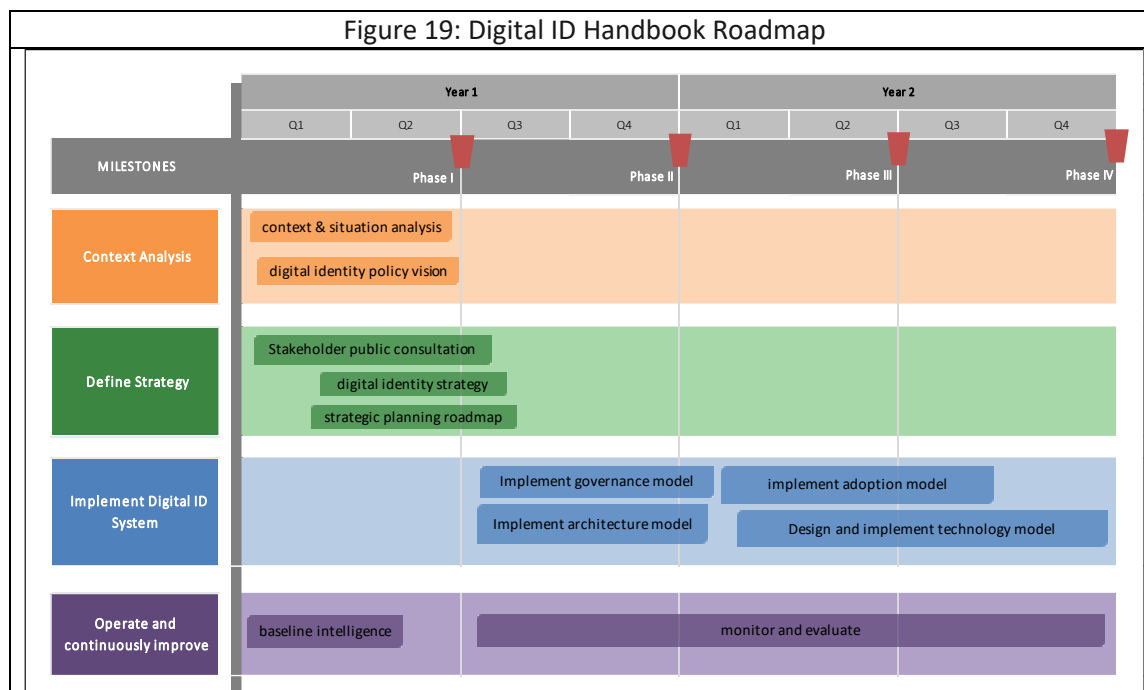
During this phase, all the tasks related to the operations of the Digital Identity lifecycle are to be performed and a formal process to monitor and evaluate the implementation progress and efficiency of the strategy should be defined and applied. In the monitoring phase, the government should ensure 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.

Once a digital identity platform is operation, 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 and authentication.

5.4.4 Digital ID Roadmap

The Digital ID Roadmap envisages a two (2) year rollout plan to fully implement all four (4) phases of the digital identity framework. See Figure 19 below.



6 Conclusion

The CTU has been promoting the principles of 21st Century Government throughout the region, which clearly demonstrates the value, in particular, of countries adopting a national digital identity system and its beneficial effects on national development. This is especially true for Caribbean countries, where the digitalisation of services can advance the proliferation of ICT-enabled economies and societies across the region and greatly increase competitiveness and efficiency, functional cooperation, entrepreneurial development, innovation and citizens welfare.

The notion of digital identity is gaining significant traction in international fora and entities such as the United Nations and the World Bank are now promoting the use of digital identity systems, globally. Several Caribbean countries have commenced, or are currently in the process of initiating projects to implement digital identity systems, for example, the OECS Digital Transformation project and other countries such as Jamaica, Barbados and Trinidad and Tobago have all initiated some form of digital identity initiative. Caribbean countries have for the most part, expressed an interest in digital identity for citizens and are moving towards readiness for the implementation of digital identity systems.

There is indeed a heightened thrust among Caribbean countries to move towards the implementation of national digital identity systems. To some extent, institutional arrangements are present within the current establishments to support the existing identity systems and related registries. However significant

strengthening of institutional capacity, robust governance structures and system integration will be required to support the provisioning of planned national digital identity systems and mutual recognition of digital identity among the Member States.

The fundamental step towards adopting an effective national digital identity system, as outlined in the Digital Identity Roadmap, is the development of a clear, implementable framework that is relevant to the local context. This is of the utmost importance, as it provides the structure around which the entire digital identity system is planned, designed, implemented, operated and improved. The Caribbean has suffered in the past, from approaches to the adoption of technology that neglected to pay sufficient attention to the analysis of its local context and the relevant frameworks that would effectively guide its implementation.

Assessment of the local context should be conducted on the basis of specific elements existing in the environment in which the digital identity system will operate. Elements that may influence this assessment, include, among others, the supporting legal and regulatory frameworks and the main demography to be served. Caribbean countries should conduct prior investigations and reviews of issues that may arise from gaps in existing regulations and laws that can potentially impact the adoption of a digital identity system. The gaps in regulations and laws must be addressed through the drafting of the relevant legislation that must be assented to by an act of Parliament.

Effective measures for amendments to the applicable regulations and laws must be instituted prior to officially pursuing and implementing adoption models. Appropriate legal controls for security, data protection and privacy, as well as cyber security must also be in place. Robust legal and trust frameworks are important factors in providing the adequate levels of assurance to facilitate interoperability and harmonisation of common cross-border systems. A number of jurisdictions have seen legal challenges to the constitutionality of mandatory ID systems, including India, Jamaica, and Kenya.

The approach taken by governments to address the demographics, will need to consider a number of factors, including the number of citizens expected to use the digital identity system, how often they might do so, and the total number of services comprised within the digital identity system. Success will depend very much on the correct assessment of these factors.

Equally important, are the consultations with government stakeholders and assessment on the status quo that will impact the perspectives of end-users as well as various government and private-sector institutions that would rely on the digital identity systems. It is recommended that governments consult with individual stakeholders to understand their particular experiences and challenges with the existing identity systems. A practical step towards understanding the current identity system landscape would be to take stock of the identity ecosystem and its stakeholders, similar to the example exhibited in Table 1.

Once a government has thoroughly assessed the local context and decided on its role, it should take measures to ensure that the digital identity system will be adequately adopted. Several options have been recommended for governments to apply that can increase adoption, each having its specific peculiarities from both the citizens and service provider perspectives. The important factor for Caribbean governments, is to clearly and precisely define the role they will play in all aspects of adoption. Government must establish itself as the lead and most involved stakeholder from the inception, in order to successfully drive the digital identity programme.

It is also important for governments to assess its own capacity and experience in the field of digital identity nationally and be willing to source specific expertise that can be leveraged regionally. This can provide significant insight into digital identity strategic goals national leaders and policy makers intend to satisfy, and what approaches they prefer to pursue (i.e., transactional, functional or foundational IDs).

Caribbean countries need to ensure that a well deployed high-speed broadband Internet is in place to support an online identity solution. This will also facilitate cross-border electronic transactions as part of the digital economy. Digital ID systems can be mutually recognized without the need for harmonisation into a common system through adopting minimum interoperability standards and legal and trust frameworks, providing for levels of assurance, to set rules and build confidence and acceptance in respective digital ID systems.

The operational models that national leaders and policy makers in the Caribbean decide to adopt is therefore of great importance, and directly influences the stakeholders and actors involved in the system. For this reason, governments need to carefully evaluate their options and pursue governance, architectural, technical and adoption models that suit the country specific approaches or needs. A governance model that allows government to either act in the dual role of the regulator and identity provider or simply the regulator of the identity provider will allow a country start with a less complex governance model that is robust enough to manage to complexities of the digital identity system. Regardless of the governance model adopted, checks and balances must be maintained over organisations charged with this oversight responsibility. Ultimately, a robust multi-layered institutional governance structure is needed.

The architectural model may follow different approaches: a centralised system with a single identity provider that collects and manages all the information and data (recommended as the logical starting point for most Caribbean countries); a distributed system with multiple identity providers (may serve as the next evolution of identity providers in the Caribbean); or a system with intermediaries between identity provider(s) and the other elements that act with specific verification or control functions (may serve as an advanced country and regional model). The selected architectural model will determine how the digital identity system will be built and evolved and the options to be considered for the technology solutions.

Finally, the economic aspects need to be considered. For any national digital identity system to be successful, realistic and sustainable goals need to be established and pursued. Governments therefore need to plan in advance how the system will be sustained, for instance, internally by generated revenues, or externally by government subsidies. Caribbean countries can leverage recent experience gained with the implementation of complex Public Private-Partnership (PPP) agreements that involved large communications infrastructure projects such as, CARCIP, to explore digital identity PPP arrangements with the private sector.

There is no one single model for a national digital identity approach that is better than another and no one-size-fits-all solution, as each country has its own distinctive characteristics, needs and goals. The CTU's Handbook on the Implementation of a Digital Identity System for the Caribbean (HIDISC) describes the elements that directly shape how a member state approaches the implementation of its national digital identity system.

Member states are therefore strongly advised to reference the HIDISC to obtain the necessary tools to assist in evaluating the myriad aspects and elements necessary to design their own roadmap towards the

implementation. This Handbook provides a summary of the main elements of some sufficiently mature national digital identity systems which represent an invaluable source of information that can be consulted to draw lessons-learned about different approaches adopted globally, but adapted for the Caribbean context.

In conclusion, the HIDISC is intended to be a support tool giving a general understanding about national digital identity systems, in one instance efficiently informing policy making decisions, and on the other providing operational support to plan, design, implement, operate, and subsequent improve the national digital identity system. The CTU remains at the disposal of our member states to provide support to advance in the planning and implementation of national digital identity initiatives.

7 Work Cited:

- *World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank. License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.*
- *International Telecommunication Union, Digital Identity Roadmap Guide. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). This is an adaptation of an original work by the International Telecommunication Union (ITU). Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by above mentioned organizations.*
- *World Bank. 2018. Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.*
- *Caribbean Telecommunications union. Towards 21st Century Government: Issue 1.5 (January 2018).*