Joint 41st Executive Council and 23rd General Conference of Ministers

Considerations for a Caribbean Digital ID Implementation Playbook

“Digital Identity Roadmap”

Junior Mc Intyre
ICT Consultant, CTU

National Digital Identify Framework (NDIF)

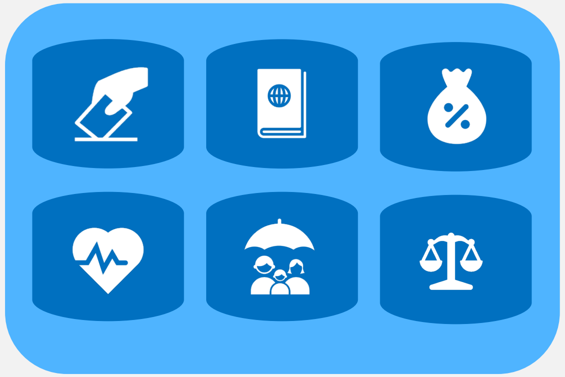
1. Categories of Digital Identifications
2. Governance Model
3. Approaches for Adoption
4. Architectural Model
5. Sustainability Model
6. Other Key Considerations
    - Risks – Challenges - Success Factors

Categories of Digital Identification

Foundational

Formal establishment of identity

- 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.



Functional

Specific sectors or use-cases

- 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).

Transactional

Digital Financial Services

- Intended to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors

1. Governance Model

Government as Identify Provider

- Government has a primary role in NDIF and acts as regulator and identity provider at the same time.

Government as Regulator & not Identity Provider

- Government acts as regulator of NDIF and procures digital identity services for citizens.
- Issue laws, regulations, criteria, procedures, controls and manage and accredits entities that acts as Identity Providers.

Government as Regulator, Identity Broker & Clearing House

- Active role in economic relationship between citizens, Identity Providers and Service Providers.
- Identity Broker as an intermediary between Service Providers and Identity Providers.

2. Approaches for Adoption

Citizen-Side

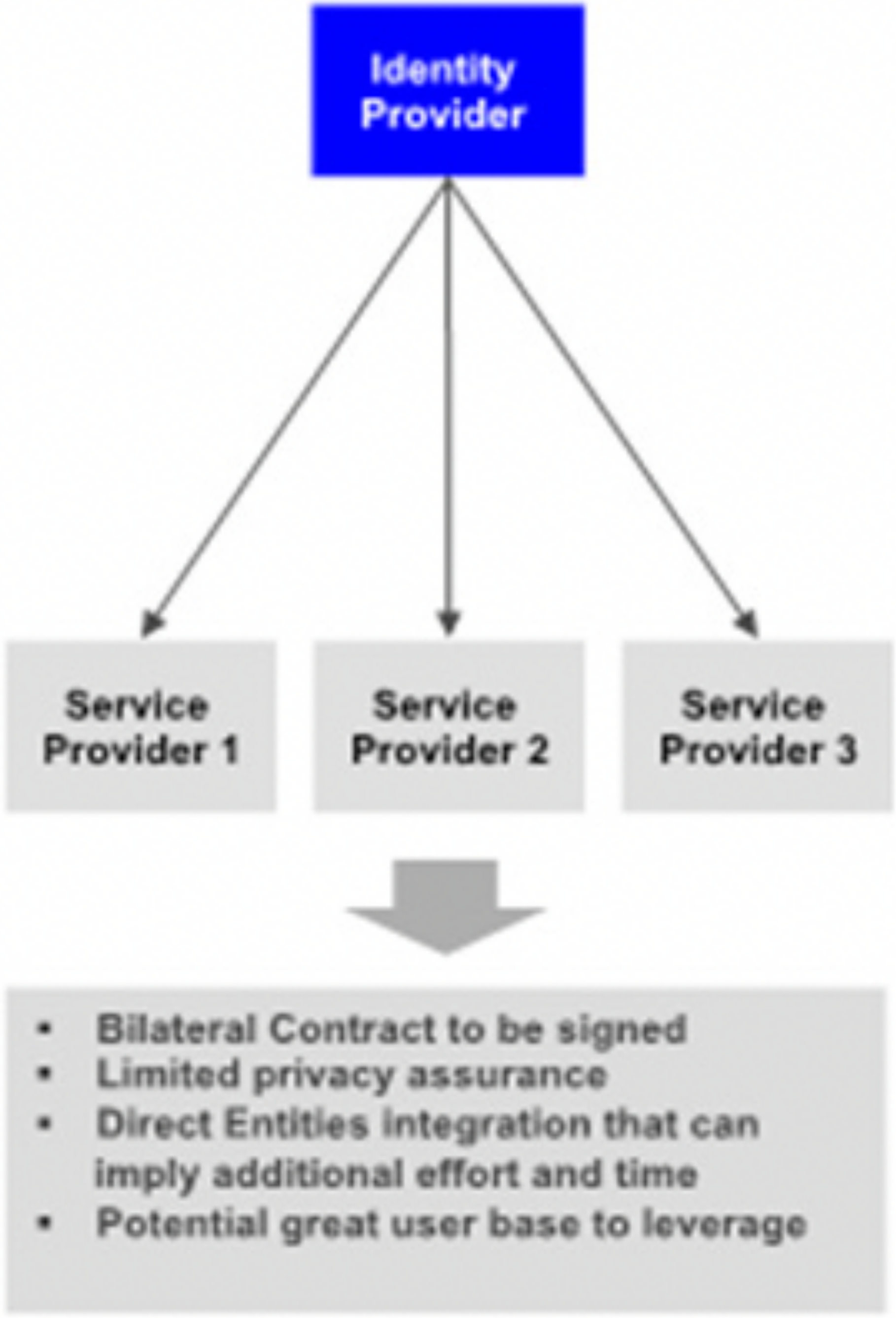
1. Value of digital identity usage for users
2. Issuing of digital identity: voluntary vs mandatory
3. Convenient enrolment process
4. Levering other digital identities systems
5. Usability
6. Security and privacy
7. Communication and awareness for the citizenship

Service Providers-side

1. Promoting or enforcing the public administration participation
2. Engaging with the private sector operators
3. Introducing Identity Broker
4. Fostering Federation of Identity Providers

3. Architectural Model

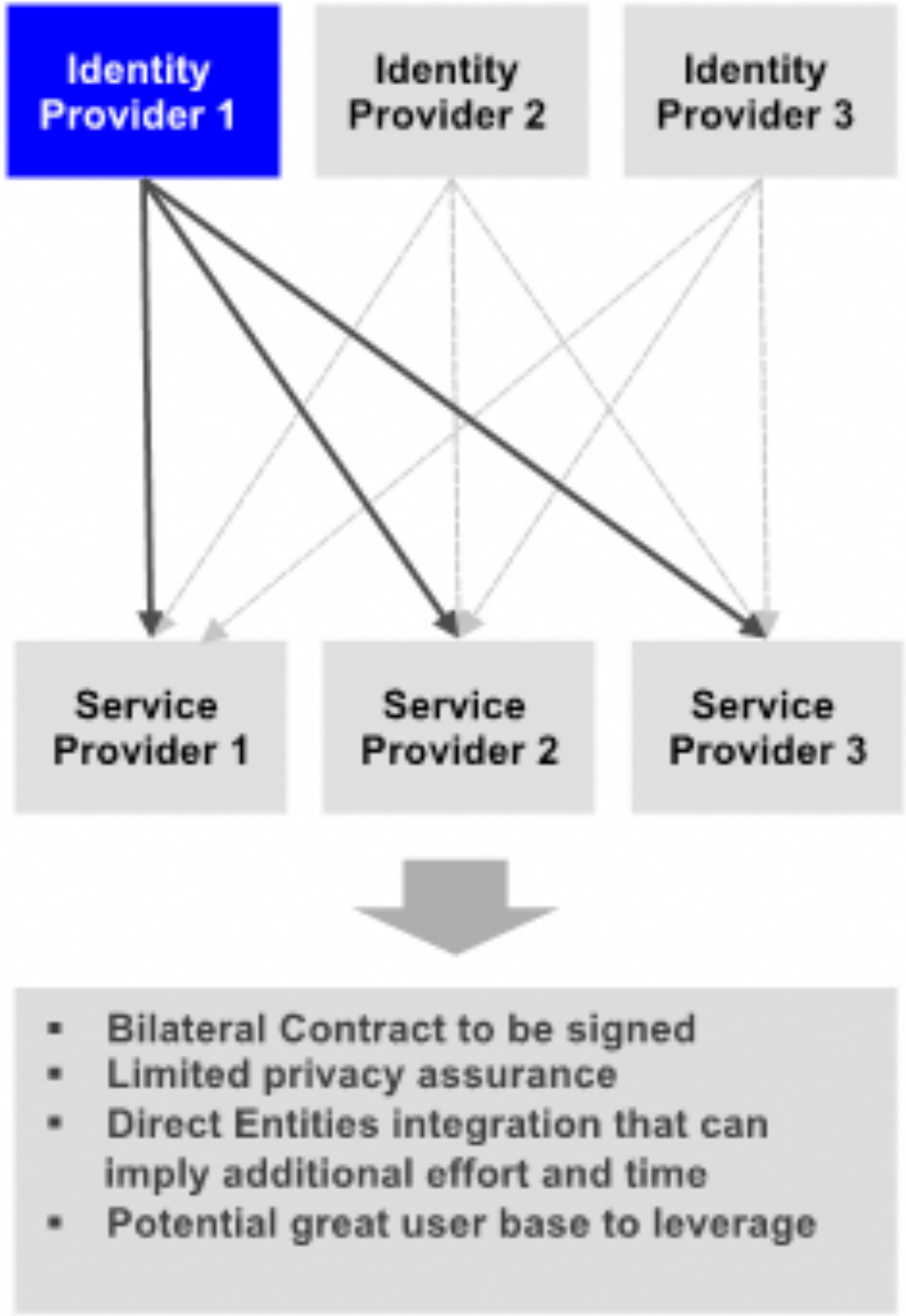
- **One unique Identity Provider**
- In centralised identity systems, a single entity acts as an Identity Provider that authenticates users to Service Providers and transfers their attributes. These systems are often designed to stream-line service delivery, enable data aggregation and provide a single view of users across multiple Service Providers.



- Bilateral Contract to be signed
- Limited privacy assurance
- Direct Entities integration that can imply additional effort and time
- Potential great user base to leverage

3. Architectural Model

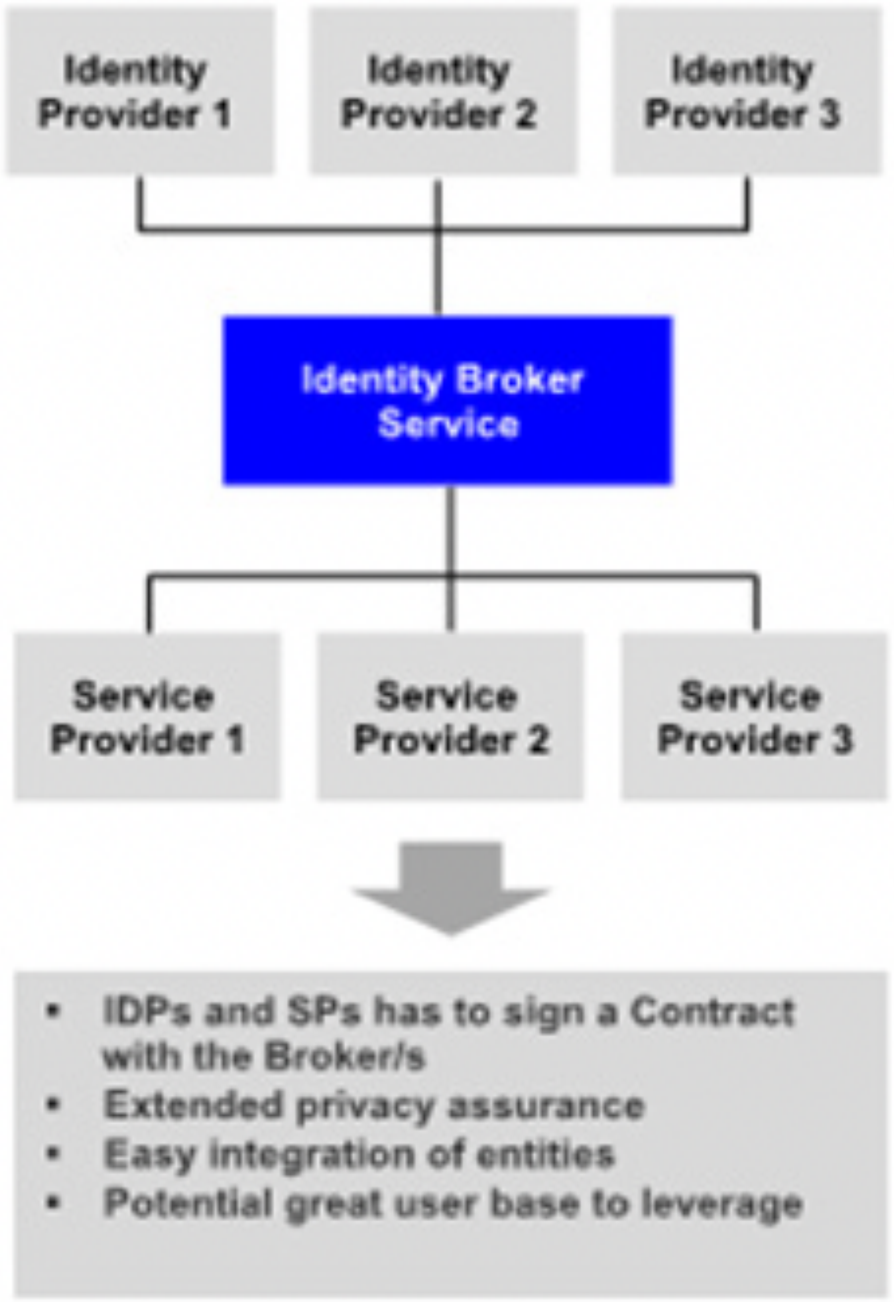
- **Multiple Identity Providers**
- In distributed identity systems, multiple Identity Providers collect, store and manage user credentials and attributes interacting with multiple Service Providers.
- These systems are notable as they leverage multiple identity providers' capabilities and differentiators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



- Bilateral Contract to be signed
- Limited privacy assurance
- Direct Entities integration that can imply additional effort and time
- Potential great user base to leverage

3. Architectural Model

- **Identity Broker/s with Multiple Identity Providers**
- The main advantages of this approach concern the possibility of simplifying the integration of Service Providers with multiple Identity Providers, but also a guarantee of greater privacy for users, preventing Service Providers from tracing back to Identity Providers accessed by users and vice versa.

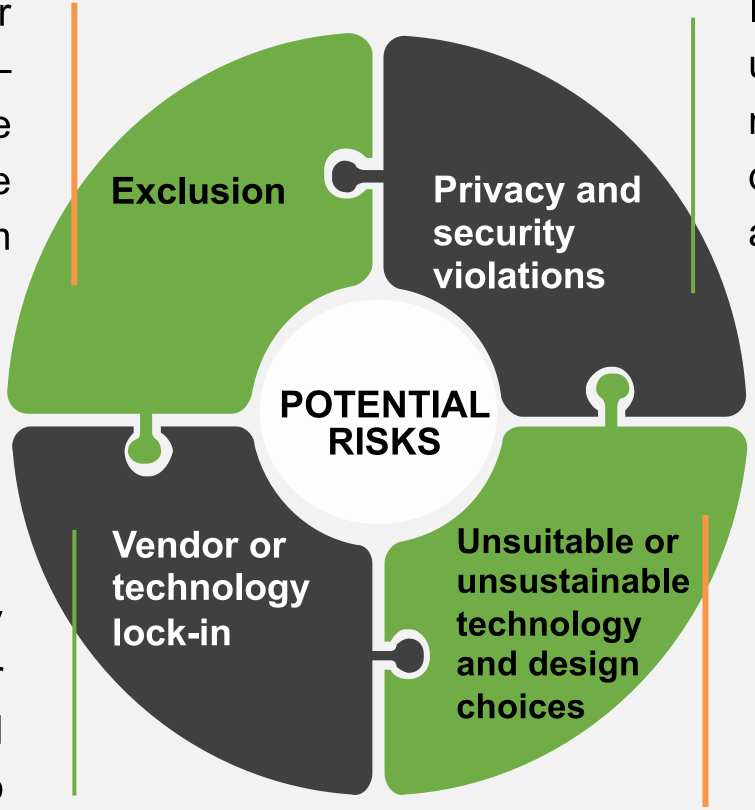


- IDPs and SPs has to sign a Contract with the Broker/s
- Extended privacy assurance
- Easy integration of entities
- Potential great user base to leverage

Risks of ID systems

making access to social programs or voting conditional on a particular ID — risks further marginalizing vulnerable people who may not be covered by the system

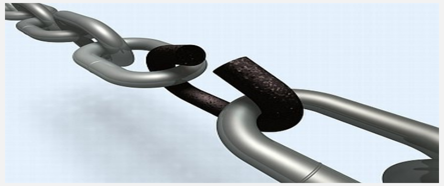
Inherent in the capture, storage, and use of sensitive personal data are risks associated with privacy violations, data theft and misuse, identity fraud, and discrimination


Exclusion
Privacy and security violations
POTENTIAL RISKS
Vendor or technology lock-in
Unsuitable or unsustainable technology and design choices

Dependency on a specific technology or vendor can result in “lock-in” and/or dependency, increasing costs and reducing flexibility of the system to meet a country’s needs as they develop

In many cases, countries have adopted high-cost systems that have failed to achieve development goals because they were unsuitable for the context or unsustainable in the medium or long term

Challenges specific to low- and middle-income countries



Weak civil registration (CR) systems

Limited connectivity and other infrastructure

Lower literacy levels

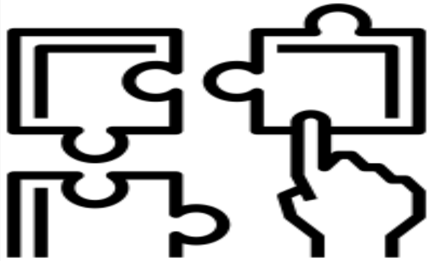
Lower government capacity and/or trust

Poor procurement

Insufficient national cybersecurity capacity

Success factors

Outcome and context-based design



Coordinated governance and sustained political commitment.

Strong legal, regulatory, and operational frameworks

A “privacy-and-security-by-design” approach

Success factors

Specific strategies and efforts to reduce the risk of exclusion during enrollment and authentication

Public engagement and consultation

A holistic approach to CR and ID

Use of international standards

Digital Identity Planning Roadmap

STATUS QUO → VISION → CONSTRAINTS → COSTS & BENEFITS → RISKS

STATUS QUO

Current ID systems operating within the country and their strengths and weaknesses.

VISION

The main goals of creating a new or improved ID system, benefits for the people, the government, and the private sector.

CONSTRAINTS

Anticipated obstacles or challenges to the planned ID system.

COSTS & BENEFITS

Anticipated financial impact of the planned ID system.

RISKS

Mitigate potential risks of planned ID systems related to privacy, security, and exclusion.

CTU

Shaping Caribbean Communications

Joint 41st Executive Council and 23rd General Conference of Ministers

Considerations for a Caribbean Digital ID Implementation Playbook

“Digital Identity Roadmap”

Junior Mc Intyre
ICT Consultant, CTU