Digitalization of a National ID Infrastructure
Identity Ecosystems for Service Delivery

Cédric Huet - Africa Digital ID VP sales
Agenda

01 Why a national digital identity?

02 Building a trusted national digital identity

03 Digital identity in use (demo)

04 Key take-aways

ID4Africa
Johannesburg – South Africa
01
Why a National Digital Identity?
What is Augmented Identity?

A closer look at physical and digital identities

Based on paper-based ID, physical identity was designed to enable face-to-face transactions among entities.

Digital identity enables transactions in the digital world and offers improved functionality for its users.

Augmented identity is an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions.
The Drivers of Digital Identity

Understanding the need to establish trust

**Growth**
- New customers acquisition
- Propose new services & products

**Identity inclusion**
- Social and financial inclusion
- Reach the digital economy last mile

**Compliance**
- AML, KYC, PEP, checks
- Data privacy

**Convenience**
- Accelerate the existing verification processes
- Delivery of a convenient and friendly user experience

**Fight against fraud**
- Identity theft and fraud
- Impersonation

**Operational efficiency**
- Reduce onboarding cost
- Less paperwork
Digital ID benefits citizens, public and private sectors

**Public sector**

**Benefits**
- Political inclusion
- Rights protection
- Social inclusion
- Fraud fighting
- Reduce informal share of economy

**Private sector**

**Benefits**
- Liability shift of identity verification for digital services
- Support to regulation compliancy (KYC)
- Reduce risk exposure
- Access identity attributes and reduce errors and fraud
- Faster service onboarding (digitalization)
- Service personalization (unique identification)
- Increase convenience
Unlocking Digital Value to the Society

The path towards a fully digital society and its benefits

01 Digital Inclusion
Leveraging digital channels to improve access to financial services for individuals and organizations

02 Digital Citizens/consumers
Increasing the interaction between the public and private sectors and citizens/consumers by facilitating the efficient access and delivery of digital services.

03 Digital Lifestyle
Establishing Internet of Things (IoT) as a fundamental for digital lifestyle.

04 Digital Society
Supporting societies to improve the standard of living including health, education, safety and social programs.
Building a Trusted National Digital Identity
Central registries: the ideal foundation for a national ID infrastructure

Central registries: the authoritative roots of digital identity

- Population registry
- Civil registry
- Biometric registry
- Functional registries (passport, driving license,...)

Digital ID

- Document-based
- Smartphone-based
- Biometric-based (e.g. Aadhaar)
Three forms of digital ID

1- Document-based

2 - Smartphone-based

3 - Biometric-based (e.g. Aadhaar)

These 3 forms of digital ID are complementary

Digital usages

Face to face
Usage identification/Attributes

Online
Authentication/Signature/Attributes Exchange

In-person (dematerialized document) use case converging rapidly with online use case
### Three forms of digital ID are complementary

<table>
<thead>
<tr>
<th>Enrollment/Issuance</th>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Digital ID on chip issued together with the physical document</td>
<td>• <strong>Universal issuance</strong> – no prerequisites on citizen</td>
<td>• Usage requires <strong>special hardware</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Usability may hinder adoption by service providers</td>
</tr>
<tr>
<td></td>
<td>• Face-to-face enrollment leveraging processes for physical documents</td>
<td>• <strong>Usability meets today's citizen expectations</strong></td>
</tr>
<tr>
<td></td>
<td>• Remote enrollment leveraging smartphone readable security features or biometric databases</td>
<td>• No hardware deployment – leverages existing smart devices</td>
</tr>
<tr>
<td></td>
<td>• Interactive communication channel</td>
<td>• <strong>Interactive communication channel</strong></td>
</tr>
<tr>
<td></td>
<td>• National biometric enrollment campaign</td>
<td>• <strong>Universal issuance</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Universal issuance</strong></td>
<td>• No hardware deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Three forms of digital ID are complementary.
03

National Digital Identity In Use / South Africa
South Africa – Leveraging on HANIS
ID verification for public sector

- Fingerprint authentication for the government
- Success stories include
  - Curbing medical fraud in the Department of Health
  - Enabling Knowing Your Patient at Chris Hani Baragwaneth Hospital – 3rd biggest hospital in the world.
  - Eliminating ghost workers in Gauteng

1. Enter your ID number in the app
2. Take finger prints
   Biometric verification against the Home Affairs database

Create your Digital Identity
Biometric verification
South Africa – Leveraging on HANIS
ID verification for private sector

- Fingerprint or mobile authentication for private sector
- Useful for:
  - KYC applications such as FICA and RICA compliance
  - Digital consent for sensitive transactions

1. Enter your data in the app or web site
2. Photograph ID or Passport
   Document check against a document authentication service to determine confidence level of it being a true document
3. Take a selfie photo incl. Liveness detection
   Biometric verification against the document photograph and the Home Affairs database
4. Consent vendor access to rich personal data
   Bank statements from source, proof of address from source, etc
Demo

Screenshot of the demo
Deep dive: example of ISSUANCE from population registry to smartphone and blockchain

1. Download mobile app & provide personal identifier

2. Take selfie & check liveness

3. Biometric matching & personal data validation

4. Attribute attestations downloaded to mobile app

5. Attribute attestations downloaded to mobile app

See Debora for animation
Deep dive: example of USAGE sharing Identity attribute with third party

1. Website requests attributes
2. ID holder authenticates to authorize attribute sharing
3. Digital ID provides attribute attestations
4. Website checks attestation status

See Debora for animation
04

Key Take-Aways
Key take-aways

01 Central Registries: the ideal foundation for a national ID infrastructure

02 Use of biometrics to link citizens to their digital ID is essential

03 Digital ID should be built on security and privacy by design principles, as it will become critical national infrastructure

04 Digital ID extends the reach of key public and private sector services to wherever there is network coverage

05 Modern ID back-end systems support modern digital ID front-ends
Thank You

Cédric Huet - Africa Digital ID VP sales

ID4Africa
Johannesburg - South Africa