ID & Authentication Systems in Digital Financial Services

Paul Makin, 19th April 2017
Introduction

• This presentation summarises a report prepared by Consult Hyperion on behalf of the International Telecommunications Union (ITU) to identify and evaluate digital ID and authentication systems, both private and state-led for their use and impact on Digital Financial Services (DFS) and financial inclusion.

• Updates have been made to reflect recent developments since the publication of that report.
PRINCIPALS

Terminology and Techniques
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>A unique individual (or organisation) distinguishable from others</td>
</tr>
<tr>
<td>Attribute</td>
<td>An item of verified personal data linked to an identity</td>
</tr>
<tr>
<td>Credential</td>
<td>A digital certificate or equivalent that can be used to assert ownership of an identity or attribute.</td>
</tr>
<tr>
<td>Relying Party</td>
<td>The party that wants to determine identity (that it is the same one seen before) or establish some attribute. <strong>NOTE: Current focus is almost exclusively in one direction</strong></td>
</tr>
<tr>
<td>Identity Provider</td>
<td>Organisation or service assisting individual (or organisation) in managing identity and attributes.</td>
</tr>
<tr>
<td>Attribute Provider</td>
<td>Organisation or service that can verify and assert a specific attribute. Note organisations may be both APs and RPs.</td>
</tr>
<tr>
<td>Level of Assurance</td>
<td>A measure of the strength of identification and authentication in the identity or attribute assertion.</td>
</tr>
<tr>
<td>Federated Identity</td>
<td>Asserting an identity or attribute established in one context in a different context, e.g. Social logon, GSMA Mobile Connect</td>
</tr>
</tbody>
</table>
What do we mean by digital identity?

Static

Identity Proofing
- Establish identity

Authentication
- Assert identity

Authorisation
- Use identity

Dynamic

Recognition

Reputation

Relationship
Different Flavours

**TOP DOWN**
A core digital identity created out of a national identity scheme or similar, which is based on the formal establishment of identity and enables a wide variety of services.
Many examples: Aadhaar (India), NADRA (Pakistan), NIMC (Nigeria)

**BOTTOM UP**
A digital identity arising from the needs of a particular sector (usually the financial sector). Can also be a method of giving control back to the individual – ‘self-sovereign’ identity.
Examples: BVN (Nigeria), SecureKey (Canada), Gov.UK Verify
Digital Identity and DFS: Desirable Characteristics

- The digital identity, of whatever type, must present a Unique ID.
- Supports the development of richer financial services and thus economic development.
- Must offer strong authentication to tie the person or entity presenting the identity to the original registrant. Biometric authentication is increasingly desirable.
Level of Assurance

Level of assurance is a measure of the quality of a digital identity, based on:

1. The quality of the steps taken to verify the claimed attributes
2. The robustness of the authentication credentials established.

Ranges from LoA 1 (minimal confidence) to LoA 4 (very high confidence), as defined by ISO/IEC 29115.
Existing Services

EXAMPLE IDENTITY SERVICES
India: Aadhaar

• The foundation of many Governmental and fintech initiatives in India

• Every resident has a digital identity, biometrically authenticated via a centralised service

• Supports eKYC, Aadhaar-enabled bank accounts, payment services, merchant payments, etc – all made even more effective through the PMJDY bank account initiative
Pakistan: NADRA

• Every **citizen** has a digital identity, held both on a smartcard (CNIC) and at a centralised service, biometrically authenticated
• Supports offline authentication
• Every mobile phone SIM is linked to a NADRA ID (not necessarily that of the user) – makes Mobile Connect a valuable proposition
Nigeria: NIMC, BVN

• NIMC (top down) based on lessons learnt from NADRA and Aadhaar; card-based, with data replicated at a centralised service. Did not translate as well as expected to Nigeria.
• BVN (bottom up) arose as a response from the financial sector – biometrically authenticated via a centralised service. No card is issued.
• BVN underpins the mCash mobile payments service.
• NIBSS report that the BVN will be migrated into NIMC when that service is ready.
Services and Technologies Offering Significant Potential

EMERGING IDENTITY SOLUTIONS
Mobile Connect

- Developed by the GSMA to enable customers to create and manage a universal digital identity via a single log-in solution
- A major undertaking by the GSMA and its members with the objective of establishing secure digital identities and consented data sharing, leveraging the security afforded by the SIM
- Uses a federated model, built around the OpenID Connect specifications
- Depending on implementation, can offer from LoA 2 to LoA 4
Self-Sovereign Identity

- The individual is their own identity provider — there is no external party who can claim to “provide” the identity for them because it is intrinsically theirs.
- A self-sovereign identity can include attributes/endorsements from traditional identity sources, such as passport providers, the purpose of which is to strengthen the LoA associated with the identity.
- So even in the context of self sovereign identities, the conventional 'identity providers' will not vanish - but instead of providing you with your identity they will instead be verifying and attesting to the validity of some aspects of your self-asserted identity.
DLT for Identity

An area of significant potential. Examples:

• Self-sovereign identities (Sovrin)
• Identities as smart contracts (uPort)
• Sovereign identities and KYC sharing (Tradle)
• Government-issued identities, DLT and Mobile Connect (ShoCard)
CONCLUSIONS
Conclusions

- Top down identity services are in many cases desirable, but they are not always the best fit.
- They can take many years to establish; in the interim, bottom up solutions should be embraced.
- Initiatives such as Mobile Connect, and services based around DLT, demonstrate that non-governmental solutions can be agile and meet the needs of individuals and the relying parties.
- The sector is fast-moving and innovative, and should be monitored closely.
- This should be backed up with appropriate policy initiatives by governments and supervisory bodies.