One Person, One Identity, Multiple Tokens, One Lifetime

Olatunji Durodola, Technical Consultant

National Identity Management Commission
Mind Map
Solving Nigeria’s Identity Challenges

Problems
- Intrusive KYC
- Multiple Identities
- Fraud
- Lack of Healthcare
- Identity Theft
- Illegal Migration
- Multiple ID Tokens
- Sex Trafficking
- Document Forgery
- Poor Security
- Tax Evasion

Solution
- Harmonise ID Tokens
- Simplified Identity Verification
- Help Identify Vulnerable Persons
- Offer Robust eServices
- Inter-agency Interoperability/Mutual Recognition
- Promote Single Source of Truth
- Deploy Simple Mobile Apps
- Deploy Simple Mobile Apps

- Promote Single Source of Truth
- Deploy Simple Mobile Apps
Brother, brother... or brother?
The Challenge
Resolving Identity in Nigeria

Multiple Enrolments
The Challenge
Resolving Identity in Nigeria

Multiple Tokens

www.nimc.gov.ng
© 2018 National Identity Management Commission. All Rights Reserved.
National Identity
eServices Built on Blockchain ecosystem

Blockchain ecosystem

One Identity, Multiple Tokens

NIN

BVN

Token-x

Base58 Blockchain

Digital Identity

Valid for 10 minutes

www.nimc.gov.ng

© 2018 National Identity Management Commission. All Rights Reserved.
# How the Blockchain Addresses are generated

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>01</strong></td>
<td><strong>Digital Token</strong> representing the NIN is presented to the <em>private permissioned</em> blockchain.</td>
</tr>
<tr>
<td><strong>02</strong></td>
<td><strong>A Blockchain-style Digital Wallet</strong> is created, which is like a keychain which stores the Digital Tokens.</td>
</tr>
<tr>
<td><strong>03</strong></td>
<td><strong>Blockchain Addresses</strong> are generated from a double Hash (SHA256) and a seed only known to the NIDB.</td>
</tr>
<tr>
<td><strong>04</strong></td>
<td><strong>Public/Private Keypairs</strong> are generated for each Digital Token, with a prefix to identify the respective agency.</td>
</tr>
<tr>
<td><strong>05</strong></td>
<td><strong>Private Keys</strong> are stored securely on dedicated Hardware Security Modules.</td>
</tr>
</tbody>
</table>
The Result
One Identity, Truth+ Trust

01
Person Identity
Starting point is the issuance of the National Identification Number as the Single Source of Truth.

02
Harmonisation
All the Stakeholders agencies submit their functional tokens and biometrics to the NIMC for harmonisation with the National Identity Database at NIMC, which in turn will return a Blockchain-style pseudonymous ID representation of that functional token.

03
Truth
As a result of the synchronised and harmonised data, coupled with robust verification services, a credible Single Version of Truth will be established.

04
Trust
Building on having tapped into a Single Version of Truth, the Private Blockchain infrastructure will establish Trusted Tokens for requesting clients, building a reliable layer of trust that will cross borders and regions over time.
Advantages of the Blockchain ecosystem

Private Blockchain means that only authorised agents, MDAs and organisations will have access to view or carry out transactions using Smart Contracts.

System is built on an Ethereum-style Blockchain engine, making Smart Contracts easy to deploy for respective MDAs such as FRSC, FIRS and so on.

ecosystem is meant to complement, not compete against the online NIN and Biometric verification systems at NIMC. The immutable nature of the ecosystem will also provide a fool-proof audit trail of all Identity Management transactions.

Data Privacy is of a passionate concern to all at NIMC. The pseudonymous nature of the token IDs on the Blockchain engine will further enhance strict compliance to confidentiality and securing Person Identity.
do list

1. Virtual SmartCard
   NIMC is working on issuing a Virtual SmartCard to be available on both Smartphones, Tablets and Feature phones, making extensive use of the National PKI

2. Revised NIN Slip
   The NIN Slip is being revised so it can be verified using Digital Hashes and the National PKI domiciled at the NIMC Datacentre

   The Next Generation National eID Card will come with a Dual Interface (contact & contactless) and have DESFire Emulation built-in

4. African Digital Identity Blockchain-based Ecosystem
   Develop an African-wide cross-border common identity ecosystem with mutual recognition, produced by Africans - for Africans
Virtual SmartCard Features

- Will be available for download from the Google PlayStore, or Apple App Store.
- For feature phones, will have digital hashes which revolve and expire after each use, and will rely heavily on the National PKI based at NIMC.
- Two apps will be available: One for End Users, the other for verification ONLY.
- Only subscribed users will be able to use the verification app. Each verification will attract a transaction fee, payable to NIMC.

Available in Q3 2018

- Download on the App Store
- GET IT ON Google Play

Revolving Keys
Will contain very strong encryption from provisioning to verification to prevent forgery.

Design
Will not be a 100% visual replica of the physical SmartCard and will contain latent components.

Ubiquity
Will instantly provide access to millions of persons awaiting the issuance of the physical National Identity Card.

Plan
Verification service requires a Subscription Plan, payable to NIMC.
Revised NIN Slip

Verifiable, reliable, realtime

Federal Republic of Nigeria
National Identification Number Slip

First Name: PROUD
Middle Name: NIGERIAN
Surname: CITIZEN
Gender: M
Tracking ID: S7Y0NFIZ00001AB

National Identification Number
1234567098

MySignature

National Identity Management System

HASH: f7482cb6e226c132a2e12bc2704441af0a90674d

[1] Please verify the information on this document by scanning the barcode above;
[2] This NIN slip remains the property of the Federal Republic of Nigeria and MUST be surrendered on demand;
[3] This NIN slip does not imply nor confer citizenship of the Federal Republic of Nigeria on the individual the document is issued to;
[4] This NIN slip is valid for the lifetime of the holder and DOES NOT expire.
Trust… but verify

Thank You