Common Digital Identification Project

Anonymous authentication system using Absolute Identifier & Decentralized OTP
1. Challenge

The need for a global solution for Common Digital Identity

Many of countries around the world are developing digital Identification system that can be authenticated globally and introducing them to local governments.
## Electric Identifier & Vaccine Passport

### Various certificate and verify services based on smart devices are flooding due to the COVID-19 crisis

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td>Electronic identification (eID) for secure online services in European countries ('14~) Establishing an eIDAS (eIDAS) for electronic transactions that can guarantee eID systems ('14.07) - Announcement of *ESSIF Framework for Self-Sovereignty in Mobile ID Cards ('20.06) * The goal is to implement SSI capabilities that allow users to create and control their identity across borders without relying on centralized authorities.</td>
</tr>
<tr>
<td>Estonia</td>
<td>IC card-based electronic identification (eID) ('14~) Distribute IC card-based electronic identification cards to all citizens. Mobile identification and electronic signatures based on standardized Subscriber Identification Module (SIM) since 2014</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Self Sovereign ID ('18~) Blockchain-based digital ID goal that can be identified with minimal personal information - Enhance privacy by introducing a function to check only necessary information through QR codes</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Digital eID for Smart Government Administration ('20~) The goal is to improve the quality of life of the people and to establish an efficient and smart government administration system. Promotion of introduction of a digital identification system based on blockchain technology (-2023.3)</td>
</tr>
</tbody>
</table>

*Source: [https://www.kisa.or.kr]*

**< Current progress of Digital Identification System by some countries >**
2. Problem

Human Rights alienation due to Legacy Identity Systems

* I, Daniel Blake (2016, 100min)
A film directed by Ken Roach. The film is set in Newcastle, England, and features criticism of the modern welfare system.

< Myanmar's citizens staging peaceful protests against the government forced into power in a military coup >
No Identity solution for Underprivileged Commons

< Hong Kong's civil movement, faced with limitations due to sanctions through the legal identity system >

Digital availability status by Age group
(average of total : 100%)

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 19</td>
<td>109</td>
</tr>
<tr>
<td>20 ~ 29</td>
<td>126.4</td>
</tr>
<tr>
<td>30 ~ 39</td>
<td>123.5</td>
</tr>
<tr>
<td>40 ~ 49</td>
<td>113.7</td>
</tr>
<tr>
<td>50 ~ 59</td>
<td>100.8</td>
</tr>
<tr>
<td>60 ~ 69</td>
<td>75.6</td>
</tr>
<tr>
<td>Over 70</td>
<td>26</td>
</tr>
</tbody>
</table>

[Source : https://www.nia.or.kr]
Requirements of Common Digital Identity

1. Easy to use including Senior, Poor and Disabled People
2. Strictly distinguish between Public and Private Usability
3. Self-Sovereign authenticate without Established Forces
AID: Absolute Identifier

Not only does it provide basic identity authentication for smart devices, but it also provides the use of web services supported by WebAuthn through an external certification system called CTAP. Unlike AID, which plays an absolute role, there is a difference that CTAP is an auxiliary role for FIDO servers.

[Reference] FIDO2 (WebAuthn + CTAP)
Not only does it provide basic identity authentication for smart devices, but it also provides the use of web services supported by WebAuthn through an external certification system called CTAP. Unlike AID, which plays an absolute role, there is a difference that CTAP is an auxiliary role for FIDO servers.
Activation scheme using Credential Data

< Authorized certificate Legal permitted to use private companies in South Korea >

source: https://blog.naver.com/dldvk9999
< Authentication scheme of Credential Data and DID using AID >
1. Authenticator : AID
2. Agent : Node
3. Verifier : Application

→ Authenticate the **AID as a Subject**, Verify the **Node as an Agent**
3. Solution [2/3]

Mobile Platform: Self-Sovereign Credential Manager
* PoE : Proof of Existence

< Status of Global Navigation Satellite System (GNSS) >

※ SBAS(Satellite Based Augmentation System) :
A System that support more precise measurements of GNSS through ground station reinforcement signals.

Record Location info and Time values based-on One's own AID & Node (False Screening through Integrity Check)
Utilization of Anonymous through End-to-End Encryption

**Method**

- **Step 1:** Message
- **Step 2:** Encryption through Secret Key
- **Step 3:** Ciphertext

*Homomorphic Encryption:*
The form of encryption that permits users to perform computations on its encrypted data without first decrypting it. These resulting computations are left in an encrypted form which, when decrypted, result in an identical output to that produced.

< Public service need to de-identification of personal information on platform server >
It was expected to be a future authentication alternative to OTP, but it follows existing central custody approaches. And it also failure to differentiated usability and secure proper durability has led to be eliminated in the market.

**NOTICE** Owner of AID must be same as the node, and not delegate his or her authority to the others.
Self-Sovereign Exercise Authentication

- Entering a password in a D-OTP
  - Storing in memory of the D-OTP
  - Encryption with D-OTP
  - Sending to the network module

- Network connection between D-OTP and Node
  - ON

- Confirm password between A and B
  - CHECK

- User authentication when same signal input is confirmed
  - SUCCESS

* It doesn’t matter which process A or B goes first.
**[Workflow 1]**

* Computation of Node A
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption

* Computation of Node B
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption
**Workflow 2**

* Computation of Node A
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption

* Computation of DLT Network
1. Check the AID information of each nodes
2. Confirm transaction integrity of each nodes
3. Register transaction of distributed ledgers

* Computation of Node B
1. Confirm password between AID and NODE
2. Checking AID registered with a server
3. Issue above-based Secret Key, Public Key
4. the others Secret Key, Public Key decryption

---

**Public**

**AID + DID**

Peer A's Secret Key (Based on AID) + Peer A's Public Key

Peer B's Secret Key (Based on AID) + Peer B's Public Key

Password

Authenticate Service

**Node + Credential**

Peer A's Secret Key + Peer A's Public Key

Peer B's Secret Key + Peer B's Public Key

---

**DLT Network**

Secret Key + Public Key

Distributed Ledger

Peer A's Secret Key + Peer A's Public Key

Peer B's Secret Key + Peer B's Public Key

---

**AID + DID**

Password

Authenticate Service

**Node + Credential**

Peer A's Secret Key + Peer A's Public Key

Peer B's Secret Key + Peer B's Public Key

---

**Peer A** (Node's Owner)

Password

Peer B's Public Key

---

**Peer B** (Node's Owner)

Password

Peer A's Public Key

---
Refugee

Loss of identity due to war, coups, political issues, etc.

Displacement situations by country of origin:

- Syria: 6.7
- Venezuela: 3.9
- Afghanistan: 2.6
- South Sudan: 2.2
- Myanmar: 1.1
- DRC: 0.8
- Somalia: 0.8
- Sudan: 0.8
- Central African Rep.: 0.6
- Eritrea: 0.5

Source: UN HCR (end-2020)
Though half the countries in Africa have IXPs, a great majority are yet to boost the levels of Internet traffic that is locally exchanged from 20% to 80%. The following enablers can foster change:

- **Market Reform**: ISPs typically drive the development of an IXP. Basic market reform creates competing access networks, and is the first step toward creating the need for an IXP. The number of ISPs represents a lower limit on the number of connected networks at an IXP.

- **Long-Distance Connectivity**: Terrestrial connectivity enables networks to connect to an IXP. International connectivity also is important to attract regional and global ISPs and international content providers to host content and become members of the IXP.

- **Content Regulations**: In order to increase the amount of local content, a carrier-neutral data center is important, as is training for local content developers. Regulations, including privacy and data protection, also make an IXP attractive to content providers.

- **IXP Policies**: A liberal IXP membership policy as well as awareness and capacity building help increase the number and variety of members, such as content providers, government, business, and other non-traditional networks.

- **Member Traffic**: A high number and diversity of connected networks at an IXP indicate a healthy internet ecosystem, which in turn, drives the amount of localized traffic at the IXP toward the goal of 80%.

---

**World Food Programme (WFP)**: The food-assistance branch of the United Nations. It is the world's largest humanitarian organization, the largest one focused on hunger and food security, and the largest provider of school meals. Founded in 1961, it is headquartered in Rome and has offices in 80 countries.
Indie band: Artist group producing independently from commercial record labels or their subsidiaries, who do-it-themselves perform to recording and publishing.

NGOs: Activist group are usually non-profit organizations, and many of them are active in humanitarianism or the social sciences in independent of government involvement.

< Independant people such as Self-employed, Free-agent >
4. Ecosystem

Technology Forum of Self-Sovereign Identity

- Establishment of technical standards for certification based on Self-Sovereign Identity, operation and management of public servers

- Development recommendations for Absolute Identifier (AID) prototyping, technical partnership, and development recommendations

- Technology patent, trademark acquisition and linked operation strategies, and license issuance
A. Intellectual Property Alliance: Provide and charge Intellectual Property service and server certification by each platform.

B. Self-Sovereign Cooperative: Donates more than 50% of business revenue to Holding Foundation as a income deduction.

C. Press & Media Association: Paying each cooperative member salary and bonus according to their history of evaluation system.

**Public Offer:** Patent only free for joining the Organization or subsidiary.

**Now on Sale:** Below Licenses of patents

* TITLE: IDENTIFICATION DEVICE
  - Application number: KR/10-2021-0050963

* TITLE: CONTENTS WALLET APPARATUS AND SELF-SOVEREIGN IDENTITY AND COPYRIGHT AUTHENTICATION SYSTEM USING THE SAME
  - PCT number: KR2020/016341
  - Registration number: KR/10-2288971
  - Application number: US/17/617,418
Common Digital Identity for Most People

- Modify and supplement to include most developing country
- Partnerships with Global NGO, NPO and Public Funds

Digital identity authentication system available to most people around the world
Thank you

http://www.ahnist.com