Architecting a Modern Identity Solution

Richard Esplin
October 2019
Agenda

- What is self-sovereign identity
- Verifiable credentials
- Governance
What is Self Sovereign Identity?
Carriers of Identity: Clothing
Carriers of Identity: Possessions
Carriers of Identity: Documents
A Useful Credential

Carried by the individual as a possession

Issued by a relevant authority (including self-issued)

Presented by the individual (or can be withheld)

Presentation of credential can be private

Hard to forge

Can be revoked, but still presented

Can be verified
On the Internet, nobody knows you're a dog

"On the Internet, nobody knows you're a dog" is an adage and meme about Internet anonymity which began as a cartoon caption by Peter Steiner and published by The New Yorker on July 5, 1993.[1][2] The cartoon features two dogs: one sitting on a chair in front of a computer, speaking the caption to a second dog sitting on the floor listening to the first.[3] As of 2011, the panel was the most reproduced cartoon from The New Yorker, and Steiner had earned over US$50,000 from its reprinting.[1][4][5]
Account Based Identity Model

You ➔ Account ➔ Org
Federated Identity Model

You -> Identity Provider -> Org
Digital Identity

- Sign in with Facebook
- Sign in with Google+
- Sign in with Twitter
- Sign in with LinkedIn
- Sign in with Amazon
AND INTRODUCED TREMENDOUS PROBLEMS
A year-long investigation into Facebook, data, and influencing elections in the digital age

Key stories

Facebook’s week of shame / The Cambridge Analytica fallout

“Politicians can’t control the digital giants with rules drawn up for the analogue era
Andrew Rawnsley

‘Did they just use me? Was I naive?’ Brexit whistleblower speaks out
Will Facebook be fined after hack attack?

Facebook could face up to $1.63 billion fine for latest hack under the GDPR

Following the revelation that up to 50 million Facebook accounts may have been accessed in an attack due to a weakness in the platform’s code, many questions remain about the breach.

Facebook’s stunning disclosure of a massive hack on Friday in which attackers gained access tokens to at least 50 million accounts—bypassing security measures and potentially giving them full control of both profiles and linked apps—has already stirred the threat of a $1.63 billion dollar fine in the European Union, according to the Wall Street Journal.
Ten Principles of Self-Sovereign Identity

1. Users must have an independent existence.
2. Users must **control their identities**.
3. Users must have access to their own data.
4. Systems and algorithms must be **transparent**.
5. Identities must be **long-lived**.
6. Information and services about identity must be **transportable**.
7. Identities should be as **widely used** as possible.
8. Users must agree to the use of their identity.
9. Disclosure of claims must be minimized.
10. The **rights of users** must be protected.

Christopher Allen, 2016
Self-Sovereign Identity is ...
Also Known As

User-Centric Identity
User-Controlled Identity
Bring Your Own Identity
Portable Digital Identity
Decentralized Identity
Verifiable Credentials
W3C Verifiable Credentials Ecosystem

Issuer

- Signs Credential
- Issues Credential

Holder

- Wallet
- Countsigns Credential
- Presents Credential

Verifier

- Verifies Signatures

Decentralized Identifiers (DIDs)

Public Blockchain or other Decentralized Network
Sovrin Verifiable Credentials Ecosystem

Issuer

- Signs Credential
- Issues Credential

Prover

- Wallet
- Countersigns Credential

Verifier

- Verifies Signatures
- Presents Credential

Pairwise Pseudonymous DIDs

Decentralized Identifiers (DIDs)

Public Blockchain

sovrin
Sovrin Verifiable Credentials Ecosystem

Issuer

Signs Credential

Zero Knowledge Encoding

Prover

Issues Credential

Countersigns Credential

Wallet

Presents Credential

Verifies Signatures

Verifier

Decentralized Identifiers (DIDs)

Public Blockchain
The Trust Triangle

- Issuer
- Holder/Prover
- Verifier

- Verifiable Credential
- Proof
- Trust
- Ledger
Buying a fish
Aaliyah’s International

Friendly fish, sustainable and responsibly distributed!

Verify our story!

Connecting to:
Aaliyah’s International
Basic Concept: DIDs

Decentralized Identifiers: a new type of globally resolvable, cryptographically-verifiable identifier.

$$\text{did:ssov:}3k9dg356wdcj5gf2k9bw8kfg7a$$

- **Method**
- **Scheme**

Method-Specific Identifier

Generated as defined by the DID method specification
Credential from: Marine Stewardship Advocates

Claim: fish sold by Aaliyah’s International are sustainably caught or bred

Inspection Date: December 8, 2018
Inspection Number: 1576295029659
Basic Concept: VCs

With a Verifiable Credential, the relying party can instantly check:

- Who issued the credential.
- Was it actually issued to the presenter.
- Has it been tampered with.
- Has it been revoked.

All without contacting the issuer.
Thank you for purchasing! Please use your phone to finalize the transaction...

Credential request: Aaliyah’s International

Would like:
- Proof of age
- Permit for owning an exotic species
- Certification of veterinary availability

Verifier

Proof Request

Holder
Credential from: Salt Lake City, Utah, United States

Claim: Richard Esplin is permitted to possess an exotic species within our city.

Date: January 10, 2019

Credential from: Utah Aquatic Veterinarians

Claim: Richard Esplin is a customer of our business in good standing.

Date: December 15, 2018
Credential from: Utah Division of Motor Vehicles

Claim: Richard Esplin is licensed to drive

Address, Birthdate, Restrictions …

Issue Date: December 15, 2018

Selective Disclosure

Claim: Older than 18

Provided by: Utah Department of Motor Vehicles
Credential from: Richard Esplin

Claims:
- Older than 18
  Provided by: Utah Department of Motor Vehicles
- Permit for owning an exotic species
  Provided by: Salt Lake City, Utah, United States
- Certification of veterinary availability
  Provided by: Utah Aquatic Veterinarians
Your delivery will be done by: **Speedy Delivery Incorporated**

Credential from: **Aaliyah’s International**

Claim:
an employee from **Speedy Delivery Incorporated** may act on our behalf

Date range:  
January 16, 2019 to January 31, 2019
Connect to
arrange delivery

Connecting to:
Speedy Delivery
Incorporated

Credential from:
Aaliyah’s International

Claim:
an employee from
Speedy Delivery
Incorporated
may act on our behalf

Date range:
January 16, 2019
to
January 31, 2019
Credential from: Richard Esplin

Claim:
an employee from Speedy Delivery Incorporated may access a porch delivery box in my possession.

Date range:
January 16, 2019 to January 31, 2019
Update from: Aaliyah’s International

Message: Your delivery service has changed. Delivery will be completed by: Advanced Delivery

January 28, 2019

Credential from: Aaliyah’s International

Claim: an employee from Speedy Delivery Incorporated may act on our behalf

Date range: January 16, 2019 to January 31, 2019

Revoked Credential from: Aaliyah’s International

Claim: an employee from Advanced Delivery may act on our behalf

Date range: January 16, 2019 to January 31, 2019

Issuer ➔ Ledger ➔ Verifier

Revocation Registry

Proof
Credential from: Richard Esplin

Claim: an employee from Speedy Delivery Incorporated may access a porch delivery box in my possession.

Date range: January 16, 2019 to January 31, 2019

Credential from: Richard Esplin

Claim: an employee from Advanced Delivery may access a porch delivery box in my possession.

Date range: January 16, 2019 to January 31, 2019
Credential from: Aaliyah’s International

Claim: the following employee of Advanced Delivery is acting as our representative

Name: Julio Valdez

Date range: January 28, 2019 to January 30, 2019

Credential from: Richard Esplin

Claim: a porch delivery box in my possession accepted a package

From: Julio Valdez, an employee of Advanced Delivery acting as a representative for Aaliyah’s International

Date: January 29, 2019
Credential from: Richard Esplin

Claim: Luciana Black has access to my front door

Number of times: Unlimited
Date range: January 16, 2019 to January 31, 2019

Credential from: Richard Esplin

Claim: Luciana Black has access to a porch delivery box in my possession

Number of times: 1
Date range: January 16, 2019 to January 31, 2019
### Use Cases Include

<table>
<thead>
<tr>
<th>Secure Messaging</th>
<th>Voting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Onboarding</td>
<td>Transportation Security</td>
</tr>
<tr>
<td>Customer Verification</td>
<td>Benefits Disbursement</td>
</tr>
<tr>
<td>Login and Authentication</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Professional Credentials</td>
<td>Certificate of Origin</td>
</tr>
<tr>
<td>Know Your Customer</td>
<td>Customer Loyalty</td>
</tr>
</tbody>
</table>
Hyperledger Projects

Join my talk: “Hyperledger Identity Projects”
More Than Code
All blockchains are governed—whether it is implicit or explicit.
Creating Trust

Moral Pressure
Reputational Pressure
Institutional Pressure
Security Systems

Bruce Schneier, 2012
Liars and Outliers: Enabling the Trust that Society Needs to Thrive
The BLT

Business
Legal
Technical
A credit card network relies on a trust framework to establish trust between the parties.
The trust in any SSI digital credential will depend on the trust framework under which it is issued.
Every digital credential intended to serve more than one issuer/verifier needs a domain-specific governance framework. It specifies what issuers will issue what credentials under what policies to achieve a community’s trust objectives.

— Drummond Reed
Chief Trust Officer, Evernym
Digital Credential

Governance Framework
Governance Frameworks

Holder/Prover

Issuer

Holder/Prover

Governance Authority (Issuer)

Verifier

Verifiable Credential

Proof

Trust

Publishes

Governance Framework
A Modern Digital Identity is Self-Sovereign

Good architecture will:

- Be built on open source and open standards
- Include a decentralized root of authority (blockchain)
- Keep personal data off the public ledger
- Allow selective disclosure
- Prevent 3rd parties from reusing credentials
- Resist correlation
- Exist within a trust framework
Discussion
Appendix
Broadening Contributor Communities

Step 1: Sovrin Foundation
Step 2: Hyperledger Indy
Step 3: Hyperledger Aries
Step 4: ToIP
The Trust Triangle

- **Issuer**
- **Verifier**
- **Holder/Prover**

Flow of Trust:
- Verifiable Credential
- Proof

Trust flows between Issuer and Verifier as well as between Holder/Prover and Issuer.