The Emerging Era of Decentralized Identity

Sean Brown, Program Director, IBM Security
Please note

• IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

• Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

• The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

• The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

• Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
The landscaping is changing, putting new focus on IAM

IAM is more complex
More devices, applications, information, users entitlements and relationships

IAM is facing more regulation
New standards and requirements for accessing and sharing sensitive information

IAM is under more pressure
Increasing expectations to protect information and deliver a better user experience
We need to change the way we think about users

Most users should be given frictionless access to resources.

**Less than 1%**

are suspected to be rogue and should trigger additional authentication measures.

Source: IBM Trusteer Research Case Study from Top 25 Global bank
The best security is the kind users don’t see

**Today’s Password-only Approaches**

Hello, can I enter?

What’s the password?

It’s “Security”

Wrong!

Ugh! it’s “Security” with a “1” instead of the “i”

You may enter

**Tomorrow’s Risk-based Approaches**

Hello…

I see you are on your enrolled phone which is not jail broken or rooted, you are connecting from the usual region with no signs of malware and your activity is in a low-risk area. Come on in!

Nice!!!
Trends driving the need for Decentralized Identity

**Simplifying consumer engagements**
- User frustration with limited control & multiple verification methods for each need
- Users will migrate to services that offer the best consumer, omni-channel experience

**More stringent regulatory requirements**
- Regulators are demanding increased transparency, privacy and accuracy in the identity information
- Liable for inaccurate or missing information (e.g. GDPR, PSD2)

**Large scale fraud, identity theft and data breaches**
- Unable to distinguish real user vs. fraudster and the financial / reputational damage

**Increasing online transaction volumes and complexity**
- Identity-dependent transactions are growing exponentially and increasing connectivity between entities
Securing digital identities in the era of cloud and mobile

Identity and access controls are **decentralized** and **external**

**Application Identities**
- SaaS

**Bring Your Own Identities**
- Cloud IAM
  - Customers, Employees, Consumers

**Device Identities**
- IaaS / PaaS

Enterprise IAM
Increased focused on privacy is driving and evolution in identity management

Identity Today

- Users/Consumers
  - Multiple providers and custodians of identity information (Govt. Banks, Bureaus, etc.)
  - No visibility and control over identity and identity information usage, theft, privacy
  - Friction and frustrating experience for millennials

- Organization/Providers
  - Point-to-point relationship with consumers and hefty investments to manage trust
  - Increased risks and costs of managing consumers identity information
  - Unsustainable and declining business due to technology and business disruptions (Mobile, Cloud, Blockchain, FinTech, etc.) and frustrated consumers

Reimagine Identity

- Users/Consumers
  - Users will create and control their identity and provide consent to providers and monetize on its usage
  - Frictionless experience and native digital engagement model
  - Self-sovereign Identity will be supported by Decentralized Trusted Network Ecosystems

- Organization/Providers
  - Decentralized identity networks will create new shared economy & strong trust models
  - Reduced costs, risks of compliance and regulation as liabilities will be distributed across the ecosystem
  - New technologies and innovations will drive new opportunities with revolutionary self-sovereign identity and verification services

#DATACENTERWORLD | DATACENTERWORLD.COM
We need to solve the problem, that physical credentials have already solved

**Physical Credentials**

- Portable and easy to verify through human judgement

**Digital Credentials**

- No standard way to verify
  - The format
  - The source and integrity
What is self sovereign identity?

- The individual **completely owns, controls** and **manages** their identity (i.e. the individual is their own identity provider)
- The infrastructure needs to be open and provide distributed trust (i.e. not belonging to any single organization).

### Self-Sovereign Identity Principles

<table>
<thead>
<tr>
<th>User Control</th>
<th>Existence Persistence Control Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portability</td>
<td>Interoperability Transparency Portability Access</td>
</tr>
<tr>
<td>Security</td>
<td>Protection Minimization</td>
</tr>
</tbody>
</table>

### Service Providers

- **Govt.**: DMV, Police, ...
- **Finance**: Bank, CC, Pay, ...
- **Travel**: Hotel, Airline, Car, ...

**Self Sovereign ID Network**

- User Wallet, Digital ID, Profile
- User Verification & Attribute Exchange

**Distributed Ledger Technology with the performance and scalability of DNS**

**Identity Custodians**

- i.e. Proof, Attribute Exchange, etc.

**Externalize identity from SP**
An emerging decentralized identity ecosystem

Motivation:
• Native Digital Consumers have changing preferences, needs and concerns on Identity.
• They seek full control and consent over Identity Data and their identity interactions.
• They want the potential opportunity to monetize their data as well.

Why Now:
• Users are seeking control, reduce passwords and simplify interactions.
• Regulatory pressures on identity & cost of identity information is increasing.
• Digital engagements need to resolve this tension between users and providers.

Motivation:
• Taking advantage of shared economy by take out costs (costs of ID infrastructure, operations, protection and compliance).
• Leverage the ecosystem for ID verification services to better target digital consumers.

Why Now:
• Competitive threats from disruptive technologies and vendors.
• Declining customer satisfaction and revenues.
• Other key drivers that enforce new approaches and participation into ecosystem.

Motivation:
• Create a new shared economy with trusted ecosystem participants (govt. banks, telco, etc.) via verification business services that reach new consumer markets, segments and drive transactional revenue.

Why Now:
• Identity Information & Interactions create strong “network effects”. Disrupt the “status quo” to create a new market place for Digital Identity and Compliance services.
• Technologies like Blockchain, mobile & cloud help develop new industry ecosystems that could fuel growth opportunity with native and empowered Digital Consumers.

Examples

#DATACENTERWORLD | DATACENTERWORLD.COM
Why blockchain and why now?

- **Blockchain enables scale and trust**
  - Users will create and manage identities which are cryptographically generated – no central registration authority
  - This removes a failure point of centralized issuers, and allows identity to scale at the edges
  - To establish trust and build new connections, users can verify the identity of a person, organization, or thing on the public ledger

- **Blockchain provides privacy**
  - Zero knowledge proofs to only disclose the information that is needed to be shared
Why blockchain for decentralized identity?

**As-Is**

**Distributed**: Synchronized ledger available for verification rather than dependency on single CAs

**Peer to Peer**: No call back to any entity but instead establish trust through a web of trust rooted in blockchain

**Selective Disclosure**: Share only what is needed with whom rather than sharing everything

**To-Be**

#DATACENTERWORLD | DATACENTERWORLD.COM
Example use case: Applying from a college to a job

**Use Cases**

Alice is vetted by Faber College to obtain invite to enroll. Upon graduation she is issued a transcript which she can use to apply for employment with Acme Corp.

**Actions**

**Examiner:** Faber College non-digital vetting of Alice as part of registration process.

**Issuer:** Alice is issued credentials from both Faber College and Acme Corp.

**Holder:** Alice stores her credentials from her relationships in her digital wallet. Alice presents credentials from her wallet when she needs to prove her identity (e.g., prove college graduation to Acme Corp). This is a peer-to-peer interaction.

**Verifier:** Acme Corp uses decentralized identifiers and verifiable credentials to perform identity verifications to greatly simplify KYC processing.
Example use case: Applying from a job for a loan

**Use Cases**

Now that she has graduated college and obtained employment, Alice can apply for a loan with Thrift Bank using her education and employment credentials.

**Actions**

**Issuer:** Alice is issued credentials from Thrift Bank after her loan is approved.

**Holder:** Alice stores her credentials from her relationships in her digital wallet. Alice presents credentials from her wallet when she needs to prove her identity (e.g., prove college graduation and employment to Thrift Bank as part of loan application).

**Verifier:** Thrift Bank uses decentralized identifiers and verifiable credentials to perform identity verifications to greatly simplify KYC processing.
IBM Clients Exploring Decentralized Identity

Government

“The paper/plastic approach to identification is plagued with stale/incorrect data. I want to issue one digital identity for my citizens that can be shared across agencies.”

“Mobile convenience and cross-industry interoperability are paramount to a digital identity solution.”

Healthcare

“I want to work with other providers and insurance companies to improve patient healthcare by implementing universal medical records.”

“I want to maintain a relationship with my customer while supporting their need to own their own identity.”

Banking

“There is a world of many blockchain identity networks. I need help validating an individual who may participate in multiple networks.”

“I want to reduce fraud by providing enhanced security beyond user/password with 2FA for digital transactions.”
An open approach to decentralized identity

"I want to work with other providers and insurance companies to improve patient healthcare by implementing universal medical records."

"I want to maintain a relationship with my customer while supporting their need to own their own identity."

**IBM PoV**
- IBM Announcements / Participation
  - DIF (http://identity.foundation)
  - Sovrin Foundation (https://bit.ly/2F0elEY)
  - Hyperledger (Fabric and Indy)

---

- Foundation of self-sovereign identity providers — building the missing identity layer (protocol)
- Focus on identity registration, identity hubs, and resolving of identifiers
- Community driven, community supported (Sovrin, Uport, Microsoft, etc)
- IBM is a member

- Non-profit foundation governing network to achieve self-sovereign identity
- Member of DIF
- Contributor of Indy codebase
- IBM is a member

**Powered by Open**

---

- Standards specification of verifying and exchanging credentials
- Standardizing schemas and operations for Decentralized Identifiers (DIDs)
- IBM is an Observer/Contributor

---

**sovrin**

**DIF**

**HYPERLEDGER**

**W3C**

**OASIS**

---

#DATACENTERWORLD | DATACENTERWORLD.COM
IBM Clients Exploring Decentralized Identity

**Government**

“The paper/plastic approach to identification is plagued with stale/incorrect data. I want to issue **one digital identity** for my citizens that can be **shared across agencies**.”

“Mobile **convenience** and cross-industry **interoperability** are paramount to a digital identity solution.”

**Healthcare**

“I want to work with other providers and insurance companies to improve patient healthcare by implementing **universal medical records**.”

“I want to maintain a relationship with my customer while supporting their need to own their own identity.”

**Banking**

“I want to reduce fraud by providing **enhanced security** beyond user/password with 2FA for digital transactions.”

“I see a world of many blockchain identity networks. I need help validating an individual who may participate in multiple networks.”
Thank you!

- Sean Brown
- IAM Program Director, IBM Security

- brown.sean@us.ibm.com
- +1-859-409-1179
- ibm.com
Learn more about Self Sovereign Identity using Sovrin

Key links for more information

- Self-Sovereign Identity and Verifiable Claims
- Sovrin Intro
- Foundational Specifications
  - W3C Decentralized ID
  - W3C Verifiable Credentials Use Cases
  - W3C Verifiable Credentials Data Model
  - Decentralized Key Management (DKMS)
- Open Standards Projects
  - Decentralized Identity Foundation
  - Hyperledger Indy