KuppingerCole Report

MARKET COMPASS

By Anne Bailey
February 28, 2020

# Decentralized Identity: Blockchain ID & Self-Sovereign Identity Solutions

The KuppingerCole Market Compass provides an overview of product or service offerings in a certain market segment. This Market Compass covers decentralized identity, specifically Blockchain Identity and Self-Sovereign Identity (SSI) solutions. This is a very dynamic space filled with visionary and innovative vendors that are applying decentralized identity to real enterprise use cases. Their development marks the entrance of blockchain technology into mainstream enterprise Identity and Access Management (IAM), and their progress will indicate the future evolution of digital identity.

By **Anne Bailey**
aba@kuppingercole.com

# Content

# 1 Management Summary

The KuppingerCole Market Compass provides an overview of a market segment and the vendors in that segment. It covers the trends that are influencing that market segment, how it is further divided, and the essential capabilities required of solutions. It also provides ratings of how well these solutions meet our expectations.

The KuppingerCole Market Compass Decentralized Identity: Blockchain ID & SSI Solutions covers solutions for managing identities (ID) based on blockchain technology. This includes solutions for self-sovereign identity (SSI), enabling individuals to securely access and interact with other parties based on the principles of Privacy by Design and Security by Design. It also includes solutions with a primary target of supporting and simplifying Know Your Customer (KYC) processes, specifically by making KYC information reusable. Furthermore, several solutions have an emphasis on a reusable authentication, with less emphasis on the KYC and SSI angle. Some of these, as well as some of the SSI solutions, are targeting the promise of delivering a Universal ID, i.e. an ID that can be used globally and across a broad variety of business cases.

Blockchain presents a previously untested opportunity for digital ID management. The current but contradictory push for both data privacy and transparency poses a challenge for traditional Identity and Access Management (IAM), but has created the competitive space for Blockchain ID and SSI to emerge. The rising consumer demand for SSI is a direct result of recent data breaches and misuse of private data, and blockchain is a timely technology development that makes it possible to move ownership and storage of PII data to edge devices. By leveraging its immutable and time-stamped ledger, blockchain can create an Identity Fabric that enables the secure sharing of information without divulging private data.

The market, as of today, is very heterogeneous with respect to both the technical approaches of the vendors and the maturity of these companies. We expect that only few of today's player will survive, while others will be acquired or simply disappear from the market. Furthermore, we expect that the market will evolve rapidly, driven by the business models that prove successful but also impacted by the current phase of disillusion in the overall Blockchain technology market. While we expect that to change, being a typical stage in every market evolution after an initial hype, this will affect also the decentralized ID market.

Notably, the decentralized ID vendors compete with a variety of other solutions, such as Identity Verification technologies e.g. based on video identification approaches, and with other approaches for delivering reusable and potentially universal ID schemes. However, this Market Compass looks specifically at the decentralized ID market as a specific segment, where the underlying blockchain technology can deliver specific benefits regarding the trustworthiness and, based on that, the security of IDs and – in the SSI context – Personally Identifiable Information (PII).

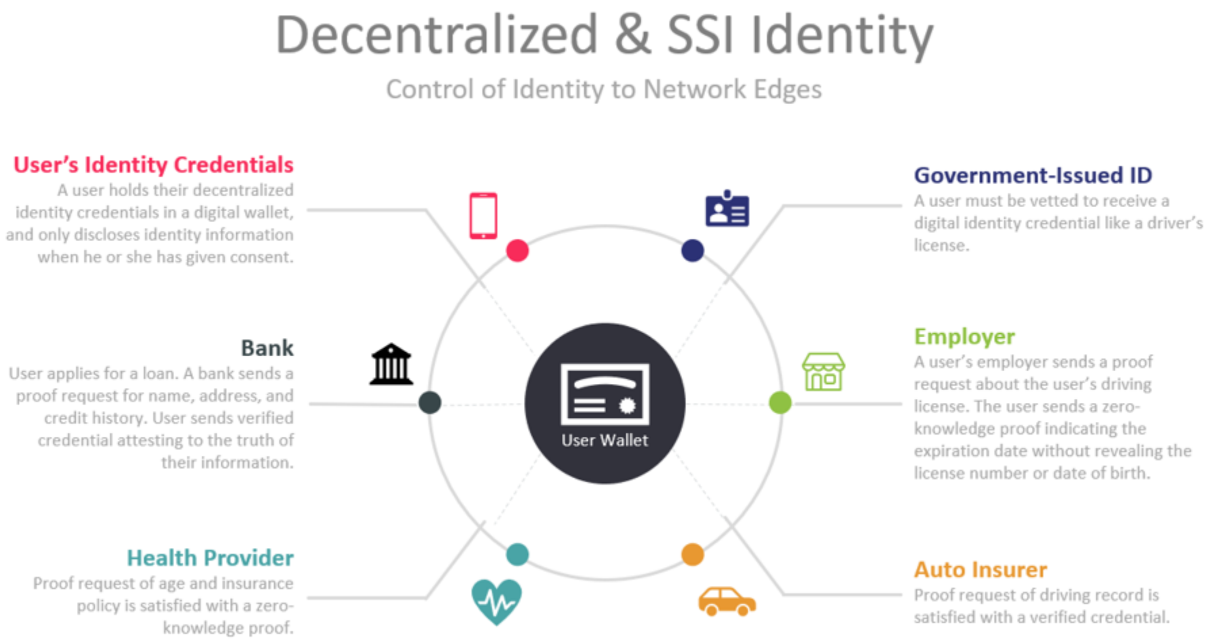
# 2 Market Segment

The decentralized identity segment, including blockchain ID and SSI solutions, includes solutions that use blockchain technology to deliver digital identity management. The breadth of identity solutions offered by vendors in this segment is wide because there is not yet a standard way of introducing SSI concepts to existing identity management. This market segment is generally very inclusive but excludes vendors that do not use blockchain as a central aspect of achieving SSI, or have not yet released their solution on the market.

## 2.1 Market Description

This market segment is defined by the provision of blockchain-based digital identity management to accomplish the goal of delivering self-sovereign identity (SSI). Although there is no standard definition yet in the market segment, this report uses the following working definition of SSI: an individual or organization has complete ownership of their PII data, stored only on their devices, and shared only with expressed consent.

The terms SSI and blockchain identity are often used interchangeably because a blockchain framework is a common way to ensure that a user has self-sovereign identity. Blockchain is not essential to delivering an SSI solution, but there are many points of overlap between the concepts that make a good match. Building an identity ecosystem on blockchain technology enables decentralized management of identity ownership, which is the foundational principle in SSI. Blockchain also allows highly secure peer-to-peer transactions, proof that information shared via blockchain has not been tampered with, and the ability to selectively share information without divulging it. These inherent traits of blockchain technology make it a compelling tool in achieving self-sovereign identity.



Decentralized & SSI Identity

Control of Identity to Network Edges

**User's Identity Credentials**
A user holds their decentralized identity credentials in a digital wallet, and only discloses identity information when he or she has given consent.

**Government-Issued ID**
A user must be vetted to receive a digital identity credential like a driver's license.

**Bank**
User applies for a loan. A bank sends a proof request for name, address, and credit history. User sends verified credential attesting to the truth of their information.

**Employer**
A user's employer sends a proof request about the user's driving license. The user sends a zero-knowledge proof indicating the expiration date without revealing the license number or date of birth.

**Health Provider**
Proof request of age and insurance policy is satisfied with a zero-knowledge proof.

**Auto Insurer**
Proof request of driving record is satisfied with a verified credential.

Figure 1: Decentralized & SSI Identity

Decentralized ID adds value to the overall IAM portfolio, such as capabilities for authentication and verification, but remains a solution built for the individual, leaving B2E IAM or certain aspects of CIAM unaddressed. This market segment is still in its nascent stages, and thus there is no dominant application for SSI and blockchain ID in enterprises. There are several major use cases that solutions have been developed for, which make up the subsegments of this market:

- **Universal ID** – the creation of a large-scale digital identity management system that connects individual identity holders with enterprises across multiple industries to facilitate the verification and exchange of identity credentials.
- **New Customer Onboarding** – enables enterprises to quickly onboard new users by accepting the identities verified by other entities, eliminating username, password, and sign-up forms.
- **SCA** – provides Strong Customer Authentication for enterprises without the need for passwords. Blockchain-enabled SCA solutions typically involve a combination of biometric, username, QR code, and/or verified and encrypted credentials attested on the blockchain. This is sometimes referred to as a single-sign-on product.
- **Reusable KYC** – equips an enterprise to verify that a user's stated identity is correct by allowing the user to share previously verified identity credentials with the enterprise in question.

## 2.2 Market Direction

This market has evolved significantly since its beginnings in 2017. It grew slightly in market size in 2018 and 2019, riding the hype of blockchain and public demand for more control over personal data. We predict that the decentralized ID market will grow and mature in response to this outcry for SSI. The market size is still relatively small and most companies are only in their first few years of operations. It will be several years before this market is fully mature.

This market has some strong players that offer clear gains for enterprises. However, this segment is still viewed as an “alternative” solution to IAM, bringing additional value to the overall IAM portfolio but does not include areas like B2E IAM and CIAM. Before this segment can experience dramatic growth and entrance into the mainstream, the hype and skepticism for blockchain solutions will have to decrease. The hype unfortunately propels underdeveloped solutions to launch prematurely, which feeds the skepticism from enterprises that blockchain does not deliver on all its promises. The success stories of forward-thinking companies embrace the uncertainty of a new identity fabric will help the SSI movement gain traction. Consumer preference for more articulate control over their PII data will also help drive growth in this market.

The subsegments that we expect to see the largest growth in are SCA and reusable KYC. Both of these use cases can increase the security and reduce costs of managing customer accounts, and offer appealing and improved user experiences when logging into an account. The benefits of new customer onboarding are encompassed by achieving SCA and reusable KYC, and so will be a positive side effect. This supports the emerging trend of providing identity services for each digital service an enterprise provides, relying on an identity fabric rather than a single legacy system. The remaining subsegment – Universal ID – is a philosophical goal that motivates many vendors, but does not have the strong business case that the other subsegments do. Universal ID will rely on the voluntary participation of a few visionary companies and nonprofits to develop such a distributed identity infrastructure.

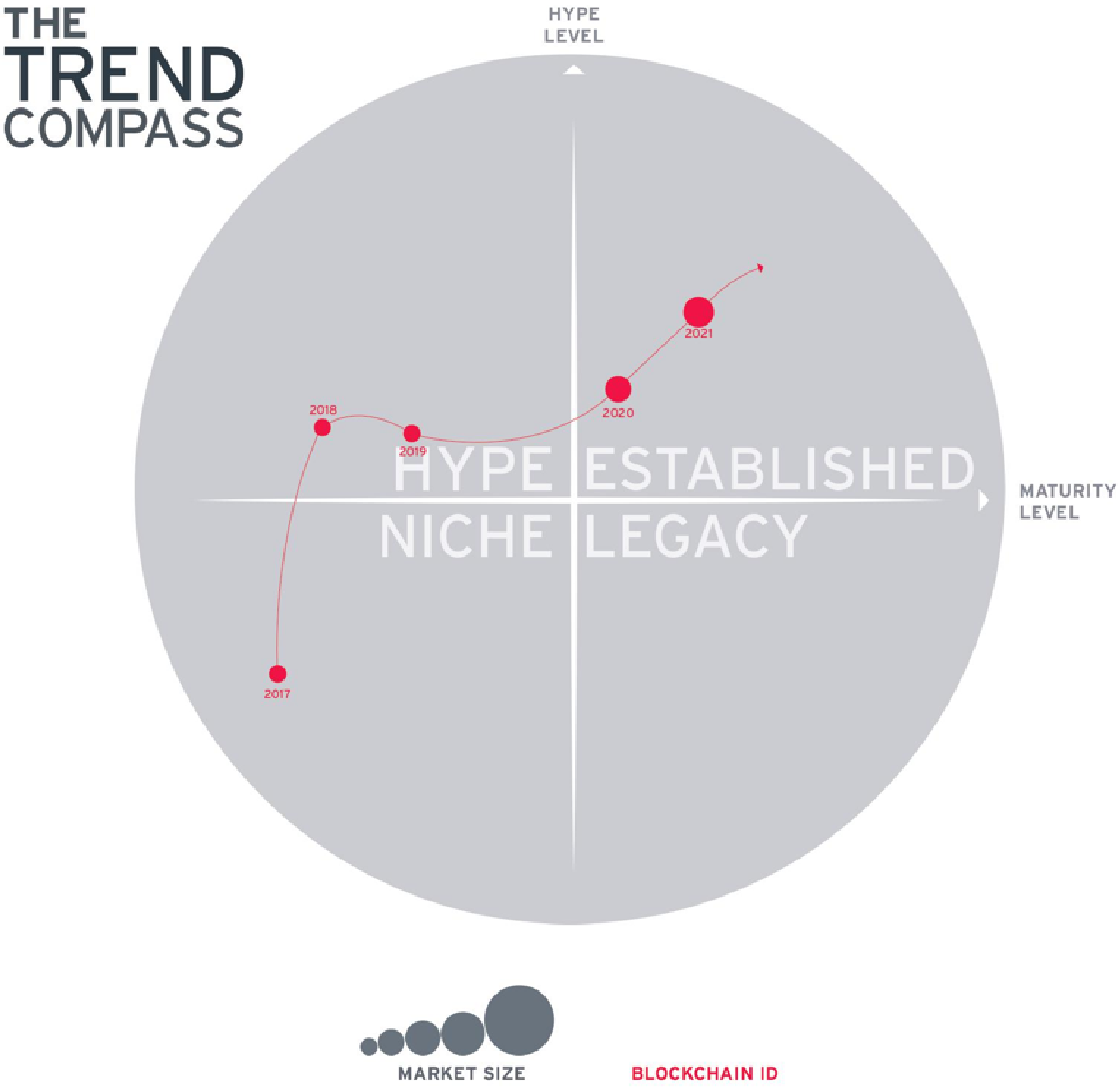


Figure 2: Trend Compass, Mapping Blockchain ID Hype and Maturity

## 2.3 Capabilities

There are some standard capabilities that decentralized ID and SSI solutions have. Others are dependent on their specific subsegment, but there is still significant crossover of capabilities between subsegments. The following sections detail the basic and advanced capabilities that are generally required, followed by summaries of capabilities required in each of the decentralized ID & SSI subsegments.

### 2.3.1 Basic Capabilities

There are certain capabilities that we expect to see in each product. They enable the core functions of decentralized ID & SSI solutions, and thus should be used as a baseline for assessing the comprehensiveness of any solution. These basic capabilities are listed below.

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Self-Sovereign Control** | SSI means that an individual owns all of their respective identity attributes. | Essential | X | X | X | X |
| **Location of PII Data** | Because blockchains are known for being “immutable”, no PII data should ever be stored on-chain. The vendor’s choice between on-premise, cloud, or local storage should match your enterprise goals and data management strategies. | Essential | X | X | X | X |
| **Support for KYC Processes and Reuse** | The solution can create efficiencies and cost saving by supporting KYC processes, and creating solutions for the reuse of previous KYC verifications. | Essential | X | X | | X |
| **Third-Party Verification** | Verification of identity attributes should be based in real-world authority. Documents should be verified by qualified and trusted entities and in line with standards specified for levels of assurance. | Essential | X | X | X | X |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Compliance** | The backed-up data as well as the backup and restoration process should be compliant with the laws and regulations required by the organization using it. | Essential | X | X | X | X |

## 2.3.2 Universal ID Subsegment

Many of the vendors have the ultimate mission of introducing a new paradigm of digital identity. This relies heavily on SSI principles of user-owned data, selective sharing rights, and zero-knowledge proofs or storage.

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Verifiable Claims** | The solution should enable the exchange of verifiable claims. Verifiable claims should be cryptographically secured and are usually exchanged on the blockchain. | Essential | X | | | |
| **Zero-Knowledge Proofs** | ZKPs cryptographically enable individuals to prove an identity characteristic to be true without divulging any information, such as proving age without showing the year of birth. | Essential | X | | | |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Selective Sharing Rights** | A user should be able to select certain identity attributes to share, instead of only being able to share an entire identity document (i.e. sharing date of birth instead of entire passport) | Essential | X | | | |
| **Interoperable Protocol** | Solutions that are network agnostic allow functionality on private or public blockchains, or even support interaction between different blockchain protocols. Greater interoperability allows for greater direct networking effects from a vendor's decentralized identity solution. | Essential | X | | | |
| **Public, Permissioned Protocol** | A public blockchain protocol allows for general and widespread usage, while permissioned protocols control what types of actions are permitted on the ledger. | Recommended | X | | | |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Multiple Device Synchronization** | Decentralized identity solutions typically move storage of PII data to the user's personal devices, stored in an identity wallet app. The wallet should have sufficient security to prevent a breach, strong customer authentication (SCA) and other features to secure wallet apps. | Recommended | X | | | |
| **Biometrics** | Integrating biometrics is common practice in traditional IAM, and is one method of authentication. Inclusion of biometric authentication adds flexibility to a vendor's blockchain identity solution. | Recommended | X | | | |
| **Information Recovery** | Blockchain solutions pose challenges to account information recovery because typical password recovery services are not possible in a decentralized architecture. Vendors have varying ways to enable information recovery. | Recommended | X | | | |

## 2.3.3 New Customer Onboarding and Reusable KYC Subsegments

In the lifecycle of a customer's relationship to a business, onboarding new customers and performing KYC checks are closely related. In a decentralized identity ecosystem, they rely on similar processes to create a heightened customer experience and satisfy regulatory risk mitigation.

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Verifiable Claims** | The solution should enable the exchange of verifiable claims. Verifiable claims should be cryptographically secured and are usually exchanged on the blockchain. | Essential | | X | | X |
| **Zero-Knowledge Proofs** | ZKPs cryptographically enable individuals to prove an identity characteristic to be true without divulging any information, such as proving age without showing the year of birth. | Optional | | X | | X |
| **Selective Sharing Rights** | A user should be able to select certain identity attributes to share, instead of only being able to share an entire identity document (i.e. sharing date of birth instead of entire passport) | Recommended | | X | | X |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Interoperable Protocol** | Solutions that are network agnostic allow functionality on private or public blockchains, or even support interaction between different blockchain protocols. Greater interoperability allows for greater direct networking effects from a vendor's decentralized identity solution. | Recommended | | X | | X |
| **Public, Permissioned Protocol** | A public blockchain protocol allows for general and widespread usage, while permissioned protocols control what types of actions are permitted on the ledger. | Recommended | | X | | X |
| **Multiple Device Synchronization** | Decentralized identity solutions typically move storage of PII data to the user's personal devices, stored in an identity wallet app. The wallet should have sufficient security to prevent a breach, strong customer authentication (SCA) and other features to secure wallet apps. | Recommended | | X | | X |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Biometrics** | Integrating biometrics is common practice in traditional IAM, and is one method of authentication. Inclusion of biometric authentication adds flexibility to a vendor's decentralized identity solution. | Recommended | | X | | X |
| **Information Recovery** | Blockchain solutions pose challenges to account information recovery because typical password recovery services are not possible in a decentralized architecture. Vendors have varying ways to enable information recovery. | Recommended | | X | | X |

## 2.3.4 Strong Customer Authentication Subsegment

Blockchain ID and SSI solutions are often able to provide SCA options for enterprises. These capabilities rely more on the development of a secure storage for identity credentials, supported by biometric "liveness" checks to streamline the login process.

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Verifiable Claims** | The solution should enable the exchange of verifiable claims. Verifiable claims should be cryptographically secured and are usually exchanged on the blockchain. | Recommended | | | X | |
| **Zero-Knowledge Proofs** | ZKPs cryptographically enable individuals to prove an identity characteristic to be true without divulging any information, such as proving age without showing the year of birth. | Optional | | | X | |
| **Selective Sharing Rights** | A user should be able to select certain identity attributes to share, instead of only being able to share an entire identity document (i.e. sharing date of birth instead of entire passport) | Optional | | | X | |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Interoperable Protocol** | Solutions that are network agnostic allow functionality on private or public blockchains, or even support interaction between different blockchain protocols. Greater interoperability allows for greater direct networking effects from a vendor's decentralized identity solution. | Recommended | | | X | |
| **Public, Permissioned Protocol** | A public blockchain protocol allows for general and widespread usage, while permissioned protocols control what types of actions are permitted on the ledger. | Recommended | | | X | |
| **Multiple Device Synchronization** | Decentralized identity solutions typically move storage of PII data to the user's personal devices, stored in an identity wallet app. The wallet should have sufficient security to prevent a breach, strong customer authentication (SCA) and other features to secure wallet apps. | Recommended | | | X | |

| Capability | Description | Relevance | Universal ID | New Customer Onboarding | SCA | Reusable KYC |
|---|---|---|---|---|---|---|
| **Biometrics** | Integrating biometrics is common practice in traditional IAM, and is one method of authentication. Inclusion of biometric authentication adds flexibility to a vendor's decentralized identity solution. | Essential | | | X | |
| **Information Recovery** | Blockchain solutions pose challenges to account information recovery because typical password recovery services are not possible in a decentralized architecture. Vendors have varying ways to enable information recovery. | Recommended | | | X | |

# 3 Vendors & Products

The vendors in this market covered by this report are those that currently offer blockchain-based products to enable at least one use case associated with SSI. These use cases are universal ID management, new customer onboarding, SCA, and reusable KYC.

## 3.1 Vendors Covered

The vendors covered in this report are:

- 1Kosmos is a US-based company focused on providing a leading digital identity platform to enable SSI with solutions that cover enterprise, consumer, and identity verification use cases.
- Authenteq was founded in Reykjavik, Iceland with the goal to provide identity verification services that support SSI concepts, with an emphasis on new customer onboarding and single sign-on use cases.
- Cambridge Blockchain is a US-based enterprise that focuses on providing enterprise software for optimizing identity authentication and KYC processes for financial services using the blockchain.
- Civic is based in San Francisco that works to create a secure identity ecosystem and open sourced marketplace for blockchain identity verification services.
- Evernym was founded in Salt Lake City, USA with the primary goal to create a new identity paradigm where users are in complete control of their identity information.
- KnowMeNow, based in Malta, was founded with the primary aim of improving KYC efficiency during onboarding by offering reusable KYC and is designed to allow other Identity Verification Service Providers to issue their certificates on the blockchain.
- Nuggets is based in London, UK and provides solutions for new customer onboarding including KYC, Access, Payment, ID verification, eCommerce and Secure Documents without sharing or storing data.
- SelfKey Foundation makes an opensource digital identity and digital asset wallet app and marketplace with extensive SDKs available to the public to implement this blockchain universal ID solution. It is based in Mauritius.

- ShoCard is based in the US with the main mission to equip government entities, businesses, and individuals to manage the digital identity lifecycle.
- uPort is based in the US and serves to develop universal SSI solutions for users and enterprises.

It should be noted that some of these vendors specialize in solutions for a single vertical, such as eCommerce, while other vendors aim to provide wide usage in universal ID ecosystems.

## 3.2 Featured Vendors

Some vendors are better positioned to meet narrow use cases, while others have stronger offerings across the range of decentralized ID use cases. We have identified a few vendors that are notable for their unique strengths that may not be apparent in the table above. Vendors are featured for capabilities, innovation, scalability, and for reusable KYC.

### 3.2.1 Featured for Capabilities: ShoCard

ShoCard is our featured vendor for capabilities because of its generally strong performance across all categories. It is designed to bring widespread SSI functionality to the enterprise and the individual, bringing a solid business case for enterprise adoption of SSI.

ShoCard presents a compelling solution to enterprise authentication with several targeted solutions that ShoCard has designed for enterprise use, overcoming the barrier of creating an SSI solution primarily for the individual. These generally applicable use cases include password-less login and single sign-on, credentialing for financial services, travel processes, call center authentication, identity verification, proof of age, and others. ShoCard demonstrates its strength in security, delivery, interoperability, and usability across narrow and ecosystem-wide solutions.

FEATURED FOR CAPABILITIES
DECENTRALIZED IDENTITY: BLOCKCHAIN ID AND SELF-SOVEREIGN IDENTITY SOLUTIONS
KUPPINGERCOLE ANALYSTS AG, FEB 2020
MARKET COMPASS 2020

### 3.2.2 Featured for Innovation: Authenteq

Authenteq is our featured vendor for innovation. While the market seems to be stabilizing on four general use cases, Authenteq has found an additional application for decentralized ID: combating online trolling and bullying. Anonymity is a coveted right of the internet, but it can easily shield individuals from taking responsibility for harassment and criminal action.

Authenteq's supplementary product, Trollteq, uses its core digital ID verification technology to allow users to create verified online identities based on a government-issued ID. Because technology supporting SSI like zero-knowledge proofs allow users to share identity credentials without disclosing any details, a user can still set up an anonymous account online while verifying that they are a real human. If that user ever abuses the account, such as posting threatening or harassing messages, their account – linked to a real but anonymized identity – can be banned. Their verified credential – although all personal information is cryptographically hidden – would be recognized by the site as a banned individual. That user would be unable to open a new account on the same site, even with a new anonymous persona.

FEATURED FOR INNOVATION
DECENTRALIZED IDENTITY: BLOCKCHAIN ID AND SELF-SOVEREIGN IDENTITY SOLUTIONS
KUPPINGERCOLE ANALYSTS AG, FEB 2020
MARKET COMPASS 2020

### 3.2.3 Featured for Scalability: 1Kosmos

1Kosmos is our featured vendor for capabilities because of its use of the DAG protocol, its use of both in-house cognitive AI for biometric authentication and third-party verification. Scalability is a constant question regarding blockchain solutions. While many current solutions rely on first-generation blockchain technology that have created work-arounds for slow transaction speed or high transaction costs, 1Kosmos works partially with the Directed Acyclic Graph which actually increases transaction speed as the number of users increase.

1Kosmos also combines the use of in-house authentication methods with third-party authentication. Third-party authentication is necessary because it increases trust in an identity ecosystem when banks, eCommerce platforms, or hospitals can trust that a user’s identification was verified by a trusted independent source. Combining external trust with in-house biometric capabilities brings additional capabilities to users with devices that are not already equipped with biometric scanners. Using in-house biometric creates independence from the limitations that device manufacturers may have in designing biometric features.

FEATURED FOR
SCALABILITY
DECENTRALIZED IDENTITY: BLOCKCHAIN ID AND SELF-SOVEREIGN IDENTITY SOLUTIONS
MARKET COMPASS 2020
KUPPINGERCOLE ANALYSTS AG, FEB 2020

### 3.2.4 Featured Vendor for Reusable KYC: Cambridge Blockchain

Cambridge blockchain is our featured vendor for reusable KYC. It is a solution designed for financial institutions to help them meet the high regulatory standards. It works within a narrower ecosystem of users, financial institutions, and trusted third-party verifiers. But within this narrow space it can prioritize the regulatory needs of the finance industry and reduce redundancy in performing KYC checks.

FEATURED FOR
VENDOR FOR REUSABLE KYC
DECENTRALIZED IDENTITY: BLOCKCHAIN ID AND SELF-SOVEREIGN IDENTITY SOLUTIONS
MARKET COMPASS 2020
KUPPINGERCOLE ANALYSTS AG, FEB 2020

## 3.3 Vendors to Watch

In addition to the vendors covered in detail in this report, we observe some other vendors in the market that will likely emerge as strong players. These vendors have either been acquired recently and are undergoing rebranding, or are vendors that will soon publicly launch their product. We provide some useful information about these vendors below:

- Blockchain Helix was founded in Frankfurt a.M., Germany. It specializes in providing blockchain ID solutions for individuals and enterprises with its featured product, Helix ID. Helix ID is in its pilot phase. Helix ID establishes a framework for digital identity that is blockchain agnostic, working primarily with consortium blockchains. Watch out for when it becomes publicly available, as it will be a strong contender.
- IBM is a multinational corporation based in the US, and is building foundational technologies, tools, and services to enable organizations to operate decentralized identity networks and for organizations and individuals to participate in decentralized identity ecosystems. It is currently in a technology preview. Keep an eye on this option as an alternative to other blockchain solutions.
- Microsoft is developing a decentralized identity solution, which will supplement cloud identity systems with SSI principles. Demos are available of their early-stage solutions. Its reputation for developing strong products will make it a potential competitor when it becomes publicly available.
- Sovrin Foundation is a nonprofit foundation that governs an open-source public permissioned ledger

for SSI solutions. While it does not provide ready-made solutions, it is a main provider of underlying SSI blockchain technology and participates in setting global standards. Stay up to date with their version releases and proposals for global standards.

- Workday recently acquired Trusted Key, a startup founded in Seattle, USA that provided a platform for identity ecosystems. It is currently being rebranded as Workday Credentials for use in issuing and using HR-related verified digital credentials for employees, applicants, students, etc. When it is ready for market release, it will offer interesting solutions to complement IAM.

# 4 Ratings at a Glance

This section provides an overview of the various products we have analysed within this KuppingerCole Market Compass on blockchain identity and SSI. Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 1.

| Product | Security | Interoperability | Usability | Ease of Delivery | ID Management | Reusable KYC | SCA | Device Synchronization | Scalability |
|---|---|---|---|---|---|---|---|---|---|
| 1Kosmos Block ID | ● | ● | 🟢 | ● | ● | ● | ● | 🟢 | ● |
| Authenteq ID Solution | 🟢 | 🟢 | ● | ● | 🟢 | 🟢 | 🟢 | 🟠 | 🟢 |
| Cambridge Blockchain IDBridge | 🟢 | ● | 🟢 | 🟢 | 🟢 | ● | 🟢 | 🟠 | 🟢 |
| Civic Secure Identity Platform | 🟢 | 🟢 | 🟢 | ● | ● | 🟢 | ● | 🟠 | 🟢 |
| Evernym Verity Suite | 🟢 | ● | ● | ● | ● | ● | ● | 🟠 | 🟢 |
| KnowMeKnow | 🟡 | 🟢 | 🟡 | 🟢 | 🟢 | ● | ● | 🟠 | 🟢 |
| Nuggets | 🟡 | 🟢 | ● | 🟢 | 🟡 | 🟡 | ● | 🟢 | 🟢 |
| SelfKey | 🟢 | 🟢 | 🟡 | 🟢 | ● | ● | 🟠 | 🟢 | 🟢 |
| ShoCard Identity Management Platform | ● | ● | 🟢 | ● | ● | ● | ● | 🟠 | 🟢 |
| uPort Serto/Open | ● | ● | 🟢 | ● | ● | ● | 🟢 | 🟠 | 🟢 |
| Legend | | | | | | 🔴 critical 🟠 weak | 🟡 neutral | 🟢 positive | ● strong positive |

# 5 Product/Service Evaluation

In addition to the ratings for our standard categories we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the Market Compass. For this Market Compass, we look at the following five areas:

- **ID Management**
  How well the product/service achieves SSI goals and provides for enterprise needs when managing the identities of internal and external participants.
- **Reusable KYC**
  How well the product/service enables the reuse of KYC information within an enterprise and between enterprises
- **SCA**
  How well the product/service supports passwordless SCA.
- **Device Synchronization**
  How well the product/service enables synchronization with multiple mobile and desktop devices.
- **Scalability**
  How well the product/service can scale from single solutions to supporting enterprise-wide identity ecosystems.

These spider graphs provide comparative information by showing the areas where the products are stronger or weaker. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only the specific features are required. Other services deliver strong capabilities across all areas, thus being a better fit for strategic choice of product.

## 5.1 1Kosmos

1Kosmos was founded in December 2016 and is headquartered in New Jersey, US. 1Kosmos’s main purpose is to establish BlockID as the leading digital identity platform to return secure identity control to the user, with an emphasis on reducing fraud. 1Kosmos presents a suite of products for enterprise use (BlockID Workforce), private consumer use (BlockID Customer), and for identity verification (BlockID Verify).

BlockID Workforce supports a migration to a password-less enterprise as well as integrating with major SaaS and SSO solutions, and BlockID Customer addresses all major use cases. It uses aspects of the ADEPT system and Directed Acyclic Graph as a blockchain-like protocol, but remains blockchain agnostic by using atomic swap smart contracts to facilitate transactions between different blockchains. It functions with the use of a user app that validates and stores all identity documents on the user’s device in the phone’s secure enclave. Users can synchronize identity data across multiple devices with a seed phrase. Users are paid in BlockID Tokens for use of the app.

1Kosmos is a strong provider of blockchain ID services for enterprises and the individual. BlockID Verify achieves level 3 assurance for Customer and Workforce users in accordance with NIST.SP.800-63A. Its architecture is API and microservices-based. It does offer selective services like B2B biometric login options as well as giving users access to a Universal ID ecosystem. Biometric authentication is a prominent feature of the BlockID solution by implementing its own machine learning-based cognitive AI for facial, voice, and fingerprint recognition instead of relying on the user’s device capabilities.

| | |
|---|---|
| Security | ● ● ● ● ● |
| Interoperability | ● ● ● ● ● |
| Usability | ● ● ● ● ○ |
| Ease of Delivery | ● ● ● ● ● |
| ID Management | ● ● ● ● ● |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ● ● ● |
| Device Synchronization | ● ● ● ● ○ |
| Scalability | ● ● ● ● ● |

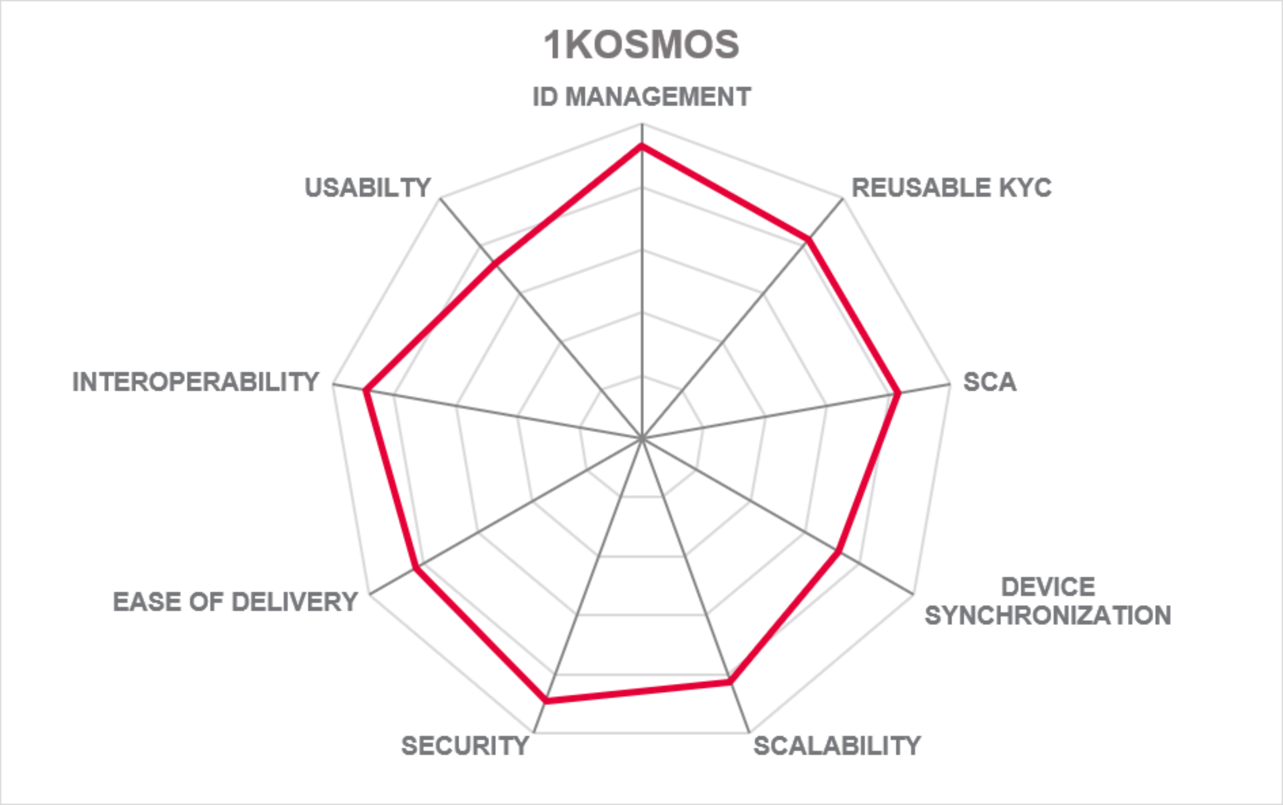
1KOSMOS BlockID

## Strengths

- Biometric authentication is powered independently from device biometric capability.
- Provides a strong enterprise use case to bypass need for critical mass of users
- Use cases include IoT device management
- Has backend integration with institutions like the US postal service to verify identity credentials
- Process for user data recovery is in place

## Challenges

- Does not yet support import of existing digital IDs, such as social logins
- Limited whitepaper publication and public documentation
- Although a robust choice, company still must convert a critical mass of users and enterprises to establish its ecosystem


1KOSMOS
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.2 Authenteq

Authenteq was founded in Reykjavik, Iceland in 2015 and publicly launched its blockchain identity verification service in 2018. Their main goal is to provide identity verification services that support SSI concepts. Their primary product is the Authenteq ID Solution, with a secondary product called Trollteq.

The Authenteq ID solution takes a different approach to providing verification services, relying on live facial recognition technology rather than third-party verifiers to continually prove that the person requesting access is real. When the user wants to interact with a service provider that requires identity information, the user authenticates their previously stored identity data with a selfie. Identity credentials are stored fully encrypted off-chain in a user wallet app. Authenteq ID uses a private version of blockchain protocol IPDB.

Authenteq ID satisfies the standard use cases of Universal ID, SCA, and KYC but also brings new applications to the table. It offers ready to implement solutions to prevent online trolling. There is room for growth, as Authenteq ID still only supports government issued IDs and not other identity features such as trainings, credentials, etc.

authenteq

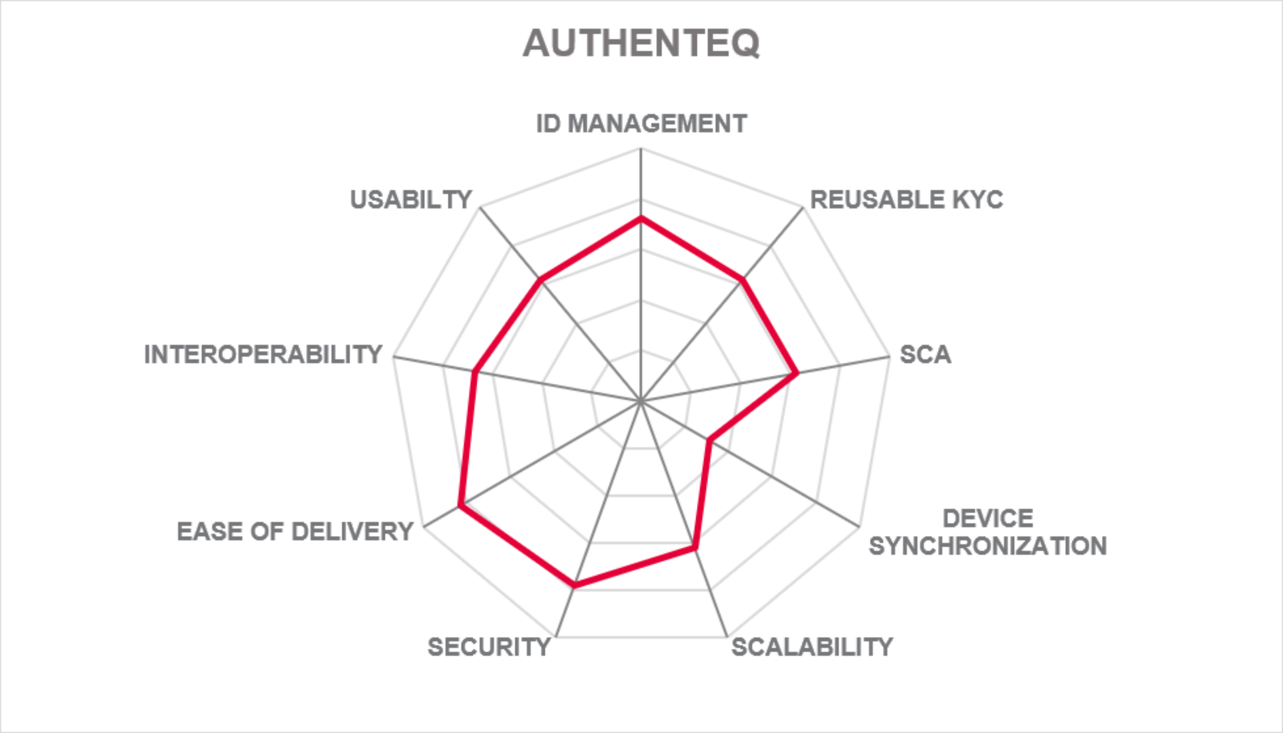
| | |
|---|---|
| Security | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ○ |
| Usability | ● ● ● ● ● |
| Ease of Delivery | ● ● ● ● ● |
| ID Management | ● ● ● ● ○ |
| Reusable KYC | ● ● ● ● ○ |
| SCA | ● ● ● ● ○ |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

## Strengths

- Additional use cases such as reducing online trolling
- 60 second initial identity verification and 3second for repeated authentications
- AI-driven facial recognition with anti-spoofing and liveness detection**

## Challenges

- A private blockchain implementation does not achieve full decentralization
- Does not support identity credentials like trainings or qualifications
- Does not support fingerprint biometrics yet
- No mention of zero-knowledge proof or storage is made in public documentation


AUTHENTEQ
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.3 Cambridge Blockchain

Cambridge Blockchain is based in Cambridge, MA, USA and was founded in 2015. The company focuses on providing enterprise software for optimizing identity authentication and KYC processes using the blockchain. It has multiple projects in development for IDBridge, including a private beta-testing.

IDBridge is a B2B software solution for financial institutions to securely share KYC information. Service providers can access the identity attestations of verified customers to complete KYC checks. Identity credentials are verified by third-party providers. IDBridge operates on SSI principles and can be deployed in private or public, permissioned or permissionless configurations. It incorporates industry-standard cryptography and is able to implement newer solutions such as zero-knowledge proofs.

IDBridge is a promising solution for B2B networks. It offers strong potential to reduce friction in storing and reusing KYC information. Front-end and authentication solution integration is straightforward. Its focus on providing solutions primarily for the financial institutions reduces its ability to address the universal ID use case.

| | |
|---|---|
| Security | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ● |
| Usability | ● ● ● ● ○ |
| Ease of Delivery | ● ● ● ● ○ |
| ID Management | ● ● ● ● ○ |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ● ● ○ |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

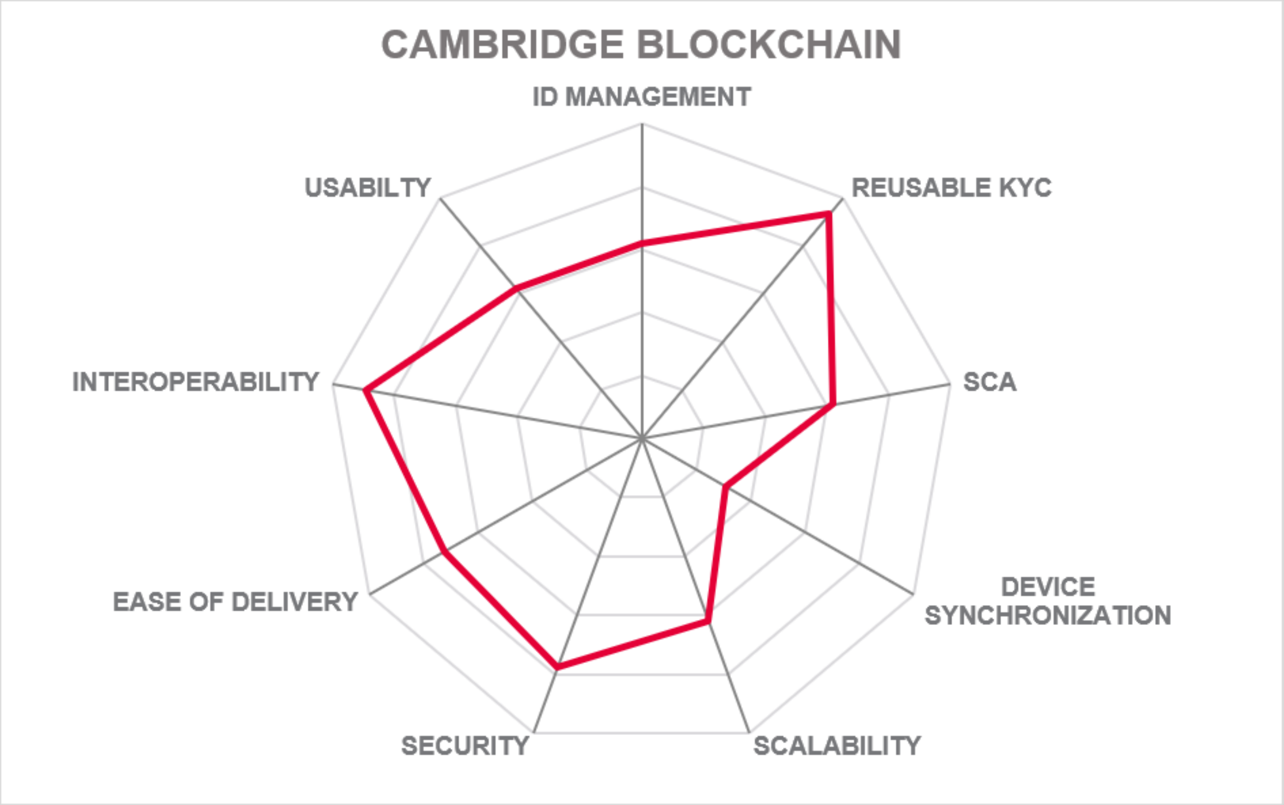
Cambridge Blockchain

## Strengths

- Strong potential to interoperate with changing standards in the financial sector
- Protected blockchain network for efficient KYC checks
- SDKs available for financial service providers and third-party validators

## Challenges

- User journey is ambiguous
- Privacy of the user may be protected against external service providers, but will be relatively accessible from within the private blockchain
- No internal use of biometrics or other SCA methods to achieve multi-factor authentication


CAMBRIDGE BLOCKCHAIN
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.4 Civic

Civic is based in San Francisco, CA. It was founded in 2015, and raised over $33m during its Initial Coin Offering (ICO) in 2017. Its primary focus is to create a secure identity ecosystem, hosted on the identity.com landing page as an open sourced marketplace for blockchain identity verification services. This report covers Civic's Secure Identity Platform (SIP).

The SIP provides a secure means of verifying identity without losing control of personal data. The platform is accessed through the associated app, where users upload, verify, and store their digital identity. The app on edge devices stores all PII data, secured with elliptic curve cryptography and biometric locks. Verification of the user's identity data is completed by Civic, then written to the blockchain. These attestations of verified identity can be requested by participants to the SIP through a QR code to be scanned with the user's app, where the user selects identity characteristics to share and approves the request. The SIP also provides Reusable KYC information to businesses.

SIP is a well-rounded solution that meets a wide variety of enterprise use cases, ranging from age verification to managing and participating in a blockchain identity ecosystem. Civic has several notable enterprise customers with a wide user base. Customer usability will improve when the user app is accessible from multiple devices.

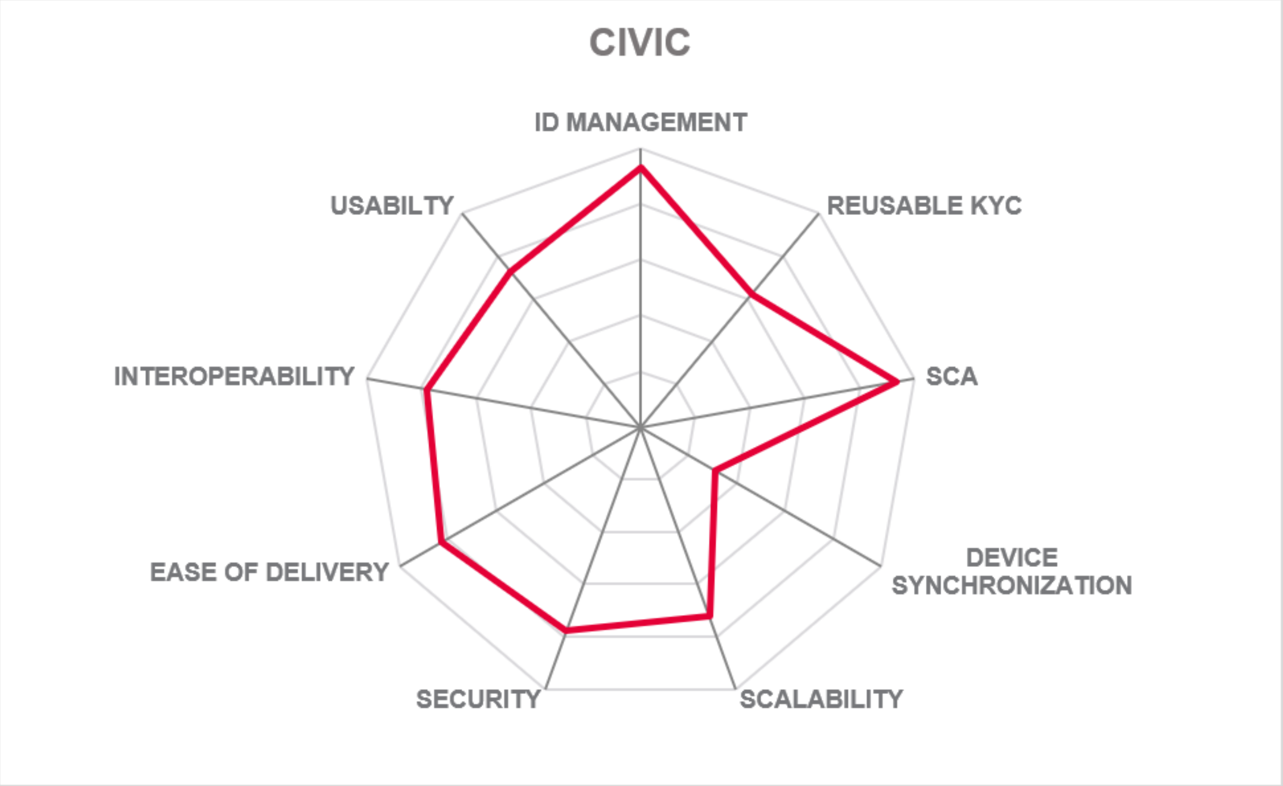
| | |
|---|---|
| Security | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ○ |
| Usability | ● ● ● ● ○ |
| Ease of Delivery | ● ● ● ● ● |
| ID Management | ● ● ● ● ● |
| Reusable KYC | ● ● ● ● ○ |
| SCA | ● ● ● ● ● |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

## Strengths

- Mature solution that fulfils enterprise use cases
- Has a user wallet with strong protections
- Is building an identity ecosystem
- All PII data is stored off-chain on edge devices
- User data recovery is possible

## Challenges

- Does not yet support usage from multiple devices
- Does not yet support import of existing digital IDs, such as social logins
- Limited or out of date public documentation


CIVIC
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.5 Evernym

Evernym was founded in 2013 in Salt Lake City, UT, USA. Its primary goal is to create a new identity paradigm where users are in complete control of their identity information. Evernym consists of a suite of products that include Verity, Verity: Auth, Verity Onboard, and the Connect.me wallet app.

Verity is an enterprise solution to issue, accept, and verify digital credentials, as well as facilitate single sign-on. Users build and manage their digital identity by uploading government-issued IDs to their wallet app, receive verification by third-party verifiers, establish DIDs for many types of identity characteristics and real-life relationships, and selectively share identity data, in zero-knowledge. There is the possibility to import and export digital identities from other wallets. Evernym uses pairwise identifiers which helps obfuscate the identity of transacting parties.

The Verity Suite is available for on-premise or cloud integration. Evernym uses Hyperledger Indy, Aries, and the Ursa library to build its solution, which are blockchain protocols specifically designed for decentralized identity management.

## evernym

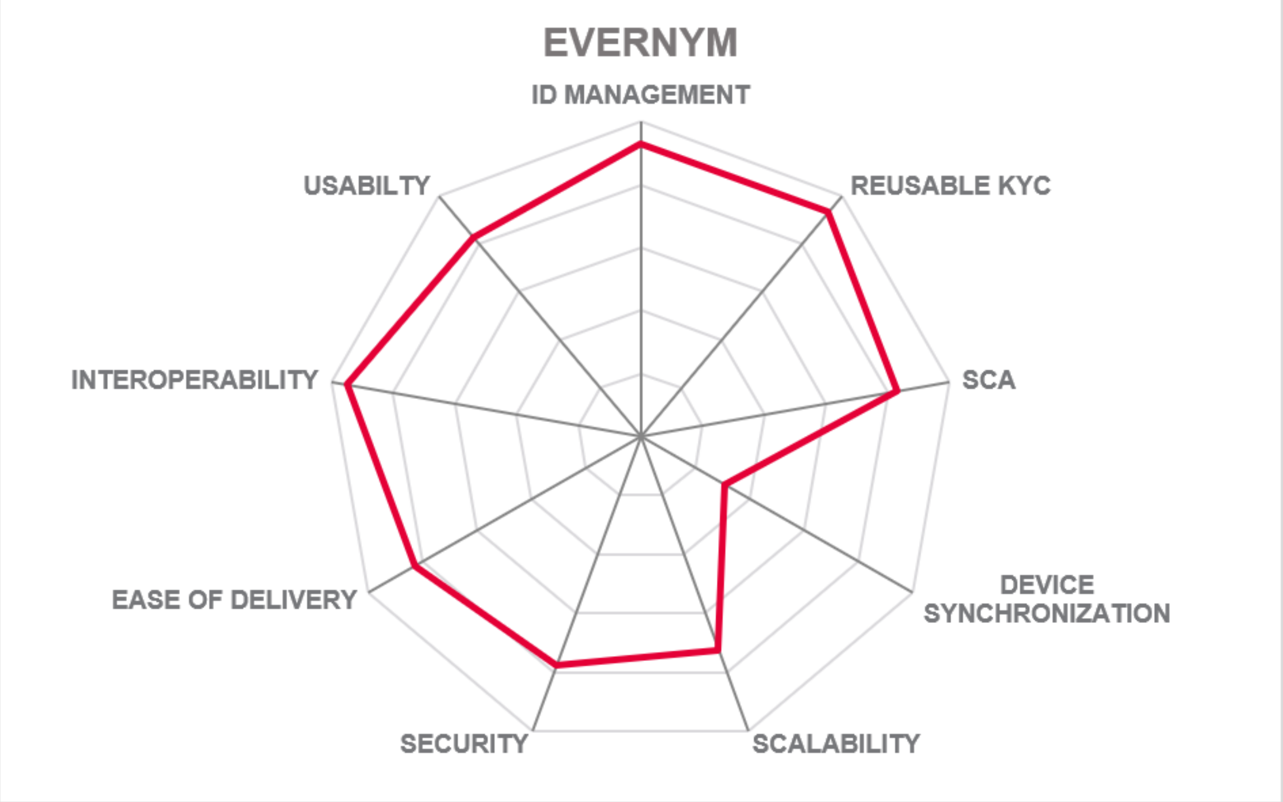
| | |
|---|---|
| Security | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ● |
| Usability | ● ● ● ● ● |
| Ease of Delivery | ● ● ● ● ● |
| ID Management | ● ● ● ● ● |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ● ● ● |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

### Strengths

- Can import and export digital identities from other wallet apps
- Supports and transacts with many types of identity credentials
- Applicable to all standard use cases
- Is part of the Sovrin Network with access to global partners and participation in forming global standards

### Challenges

- Does not yet support usage from multiple devices
- Does not inherently include biometric capabilities
- Although a robust choice, company still must convert a critical mass of users and enterprises to establish its ecosystem


EVERNYM
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.6 KnowMeNow

KnowMeNow was founded in 2017, and is based in Malta. The company has extensive experience as a verification service provider. It focuses on delivering a decentralized identity wallet for users and reusable KYC services for enterprises.

A user downloads the KnowMeNow wallet app, and uploads their government-issued ID, selfie, and general information such as email and phone number. The service provides three levels of assurance (LOA) for identity characteristics. Level one is fully automated, with levels two and three being supported by a human agent. The verification process for level three is approximately 5 minutes. The user can then sign up for services with KnowMeNow partner merchants, such as online gaming or banking services.

KnowMeNow is a promising solution for KYC checks for a wide range of sectors. KnowMeNow uses public Ethereum for access to a fully decentralized model. The solution specializes in being streamlined and user friendly to decrease onboarding abandonment for enterprises.

| | |
|---|---|
| Security | ● ● ● ○ ○ |
| Interoperability | ● ● ● ● ○ |
| Usability | ● ● ● ○ ○ |
| Ease of Delivery | ● ● ● ● ○ |
| ID Management | ● ● ● ● ○ |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ● ● ● |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

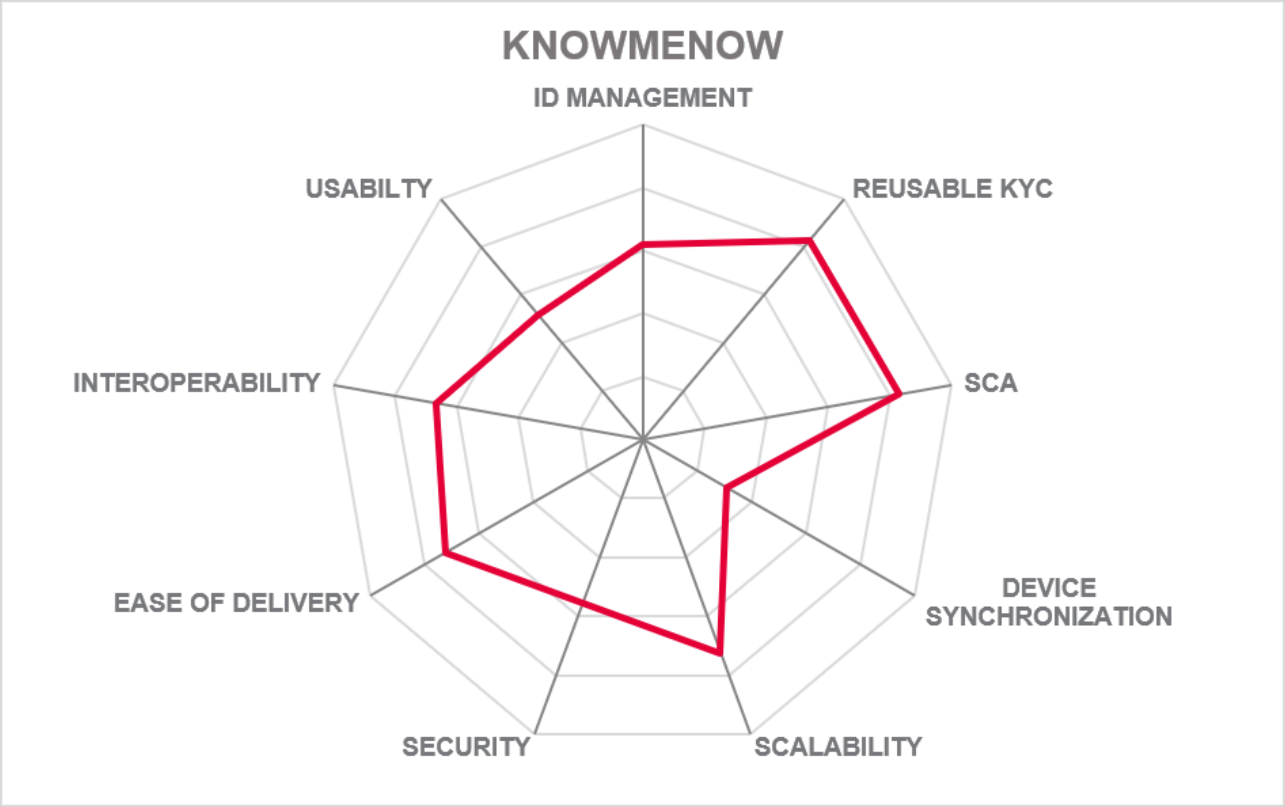
KNOW ME NOW
BLOCKCHAIN ENABLED KYC

## Strengths

- KYC and AML-focused solution
- Biometrics used as an aspect of multi-factor authentication
- High functionality within the network of approved merchants

## Challenges

- Limited to identity cards, passports, and drivers licenses
- No data recovery possible at this point
- Solution is user oriented instead of enterprise oriented, which may slow down adoption rates


KNOWMENOW
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.7 Nuggets

Nuggets was founded in London, UK in 2016. Nuggets believes privacy is a fundamental right and the users should own and control their data. They have built a B2B2C decentralized self-sovereign ID and payment platform powered by blockchain, operating primarily with eCommerce and Payment Service Providers (PSPs) with intentions to extend services to financial institutions and telecommunications. Its primary product is Nuggets, named for the nuggets of identity data that are encrypted and stored with blockchain. Nuggets has launched with controlled numbers of participants.

Nuggets operates with a user app that validates and stores a user’s government-issued ID and credit card information. This is verified and authenticated with biometric fingerprint and facial recognition. Customers are onboarded with a KYC process that is compatible with major KYC providers. Nuggets is powered by the Nuggets Token, which is used to pay the Ethereum blockchain transaction costs, reward users for using the service, and allow merchants to request and pay in tokens for additional and consensually shared identity information, such as the user’s email for marketing purposes.

Nuggets specifically addresses the eCommerce applications of blockchain ID as this is seen as the most vulnerable are for users. Nuggets allows functionality on multiple devices because the user’s PII data is stored in a “personal cloud” by encrypting first, hashing on-chain, and then storing in IPFS instead of being stored exclusively on a single device. Recovery of data is possible with a user’s mnemonic recovery phrase. Nuggets uses a containerized model for delivery.

nuggets

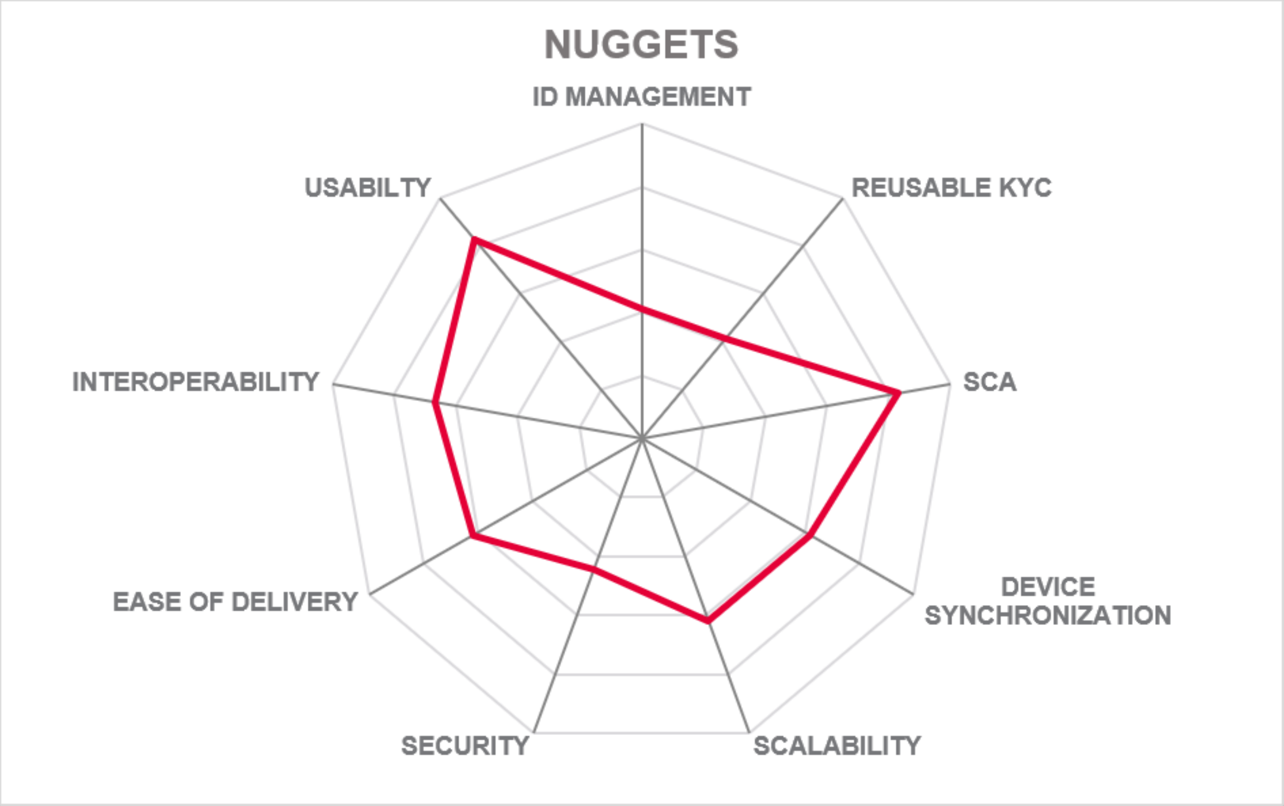
| | |
|---|---|
| Security | ● ● ● ○ ○ |
| Interoperability | ● ● ● ● ○ |
| Usability | ● ● ● ● ● |
| Ease of Delivery | ● ● ● ● ○ |
| ID Management | ● ● ● ○ ○ |
| Reusable KYC | ● ● ● ○ ○ |
| SCA | ● ● ● ● ● |
| Device Synchronization | ● ● ● ● ○ |
| Scalability | ● ● ● ● ○ |

### Strengths

- Focused applicability for eCommerce customers and merchants
- Functionality on multiple devices is possible
- Process for user data recovery is in place

### Challenges

- Private blockchain implementations do not allow for full decentralization
- Limited APIs available
- No import of external digital IDs


NUGGETS
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.8 SelfKey Foundation

The SelfKey Foundation is a nonprofit organization established in Mauritius by the for-profit company KYC-Chain Ltd in 2017 with a mission to promote and facilitate the use of its SSI solution. Its ICO was in 2018, which raised $22 million. The foundation makes an opensource wallet app which allows users to store both their cryptocurrency as well as identity documents. They also provide a corporate wallet which allows businesses to do the same. They have extensive SDKs available to the public to implement this blockchain universal ID solution.

SelfKey operates on the Ethereum public blockchain with the help of the KEY token. The token is used to incentivize proper use of the platform and to purchase identity services within the ecosystem. A user wallet serves as a storage location for identity credentials, attestations, and verifications. Functionality extends to setting up a bank account, incorporating a business in selected jurisdictions, managing cryptocurrency accounts, and building corporate wallets to manage documents, certifications, and other documentation. Device synchronization is enabled with a seed phrase, with other methods of achieving synchronization to be released in early 2020.

SelfKey is a strong universal ID solution with attention to security, recoverability, and compliance with international standards. It is limited to desktop usage, with mobile options in the development pipeline. SelfKey uses identity fragmentation in the place of zero-knowledge proofs.

| | |
|---|---|
| Security | ● ● ● ● ○ |
| Interoperability | ● ● ● ● ○ |
| Usability | ● ● ● ○ ○ |
| Ease of Delivery | ● ● ● ● ○ |
| ID Management | ● ● ● ● ● |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ○ ○ ○ |
| Device Synchronization | ● ● ● ● ○ |
| Scalability | ● ● ● ● ○ |

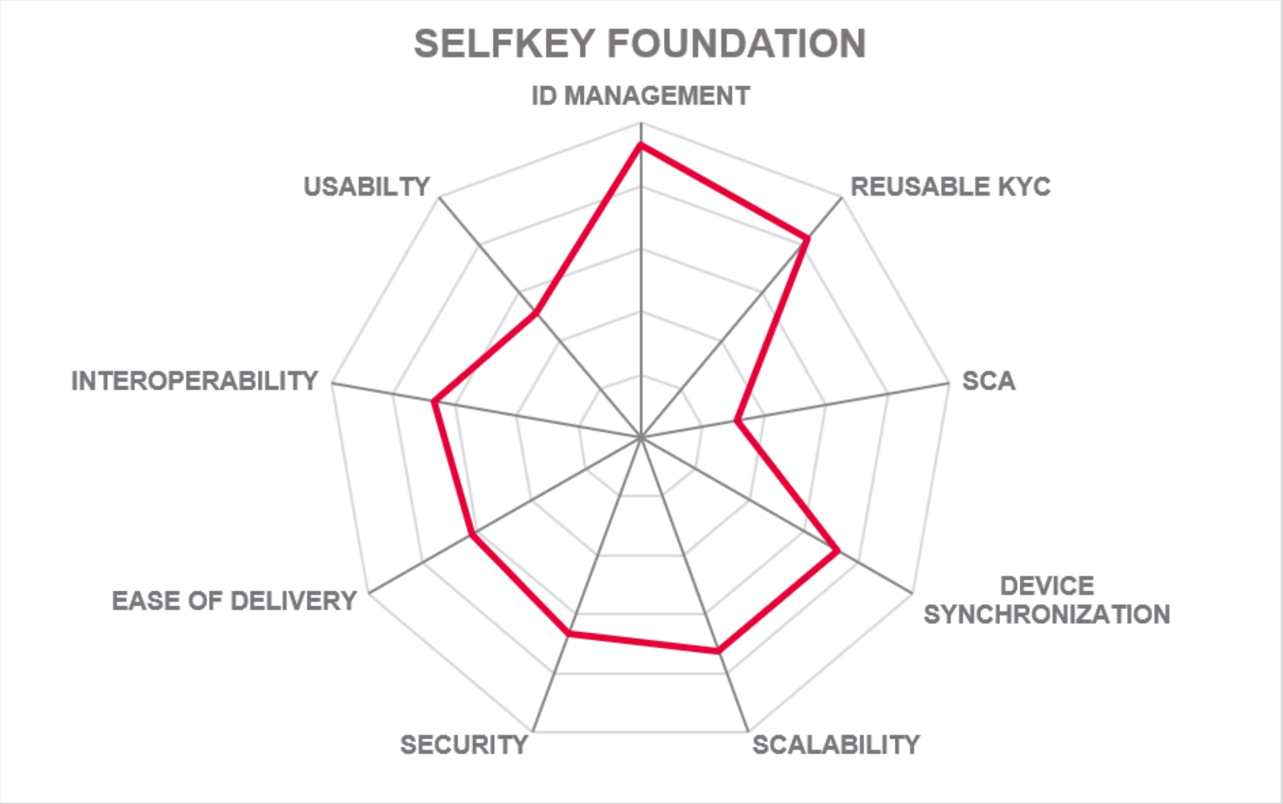
SELFKEY

## Strengths

- Strong focus on compliance and interoperability for global use
- Recovery managed through cooperation with uPort, developing options to recover using biometrics
- IoT identity management is possible
- Goal to make biometric identity characteristics the foundation of digital identity, with the philosophy that identity begins with human life

## Challenges

- Restricted to desktop use, but with mobile app development on the roadmap
- Strong Customer Authentication is not a current capability
- No clear enterprise or government adoption strategy to achieve critical mass


SELFKEY FOUNDATION
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.9 ShoCard

ShoCard was established in 2015 in Cuppertino, CA, USA by founders experienced in online platform development and security. Its main mission is to equip the main identity players – government entities, businesses, and individuals – to manage the digital identity lifecycle. This report covers ShoCard's Identity Management (IM) Platform, which is available as a product in two forms: enterprise-focused identity authentication, and a complete Identity Provider solution.

The IM Platform is built to be blockchain agnostic, meaning it can operate on multiple blockchains simultaneously. The platform has public, permissioned access but has the capacity to support private blockchain architectures as well. Identity verifications are handled on sidechains to allow a high throughput. The platform can be integrated into an organization's servers, or downloaded as a user app. Users create a digital identity by taking a photo of a government-issued ID, self-certify that the information is correct, and stores it on their personal device protected with private key encryption. Third-party verification by banks or government agencies establish a base KYC check that is written to the blockchain as a hash, with no PII data included. The user is then able to present these certifications to prove his or her identity.

ShoCard is a mature vendor that is producing live solutions with several high-profile clients. ShoCard's products have patent-protected Account Recovery mechanisms to aid customers in the event of a lost device. Login from multiple devices is possible with ShoCard's enterprise-focused authentication solution, but storage of identity information is still restricted to a single mobile device.

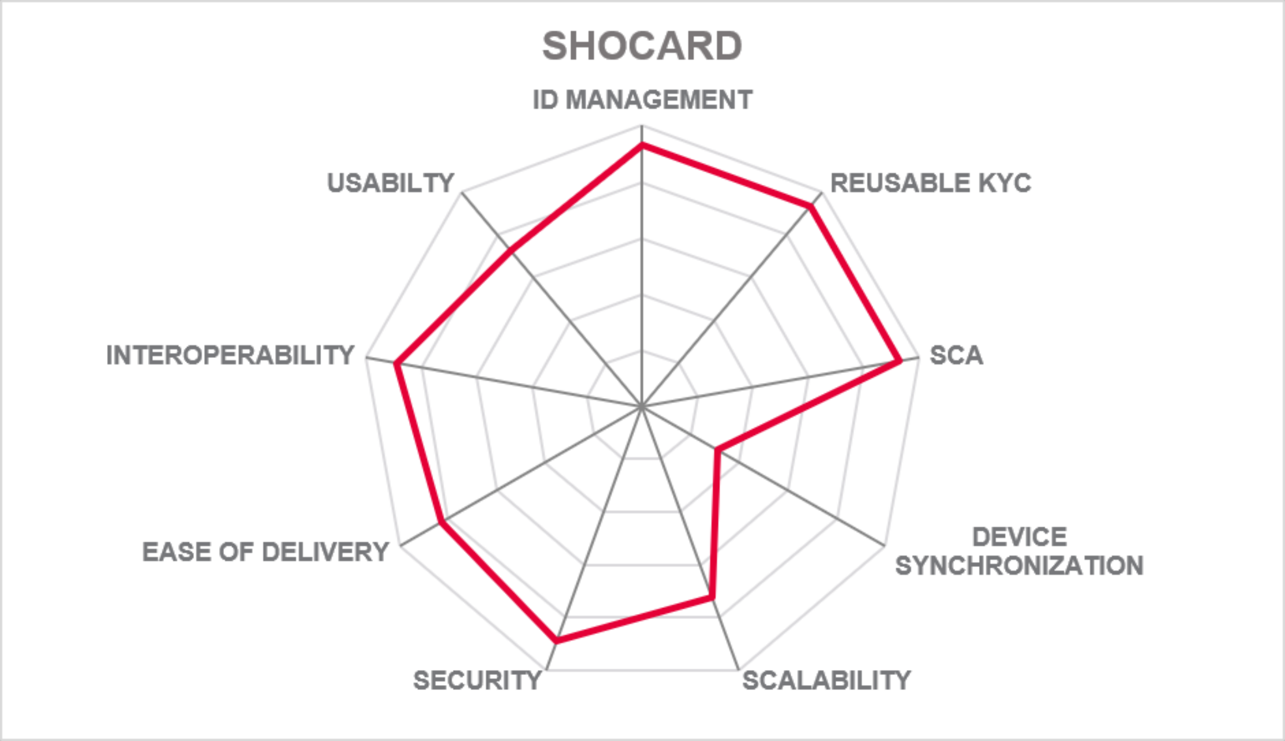
| | |
|---|---|
| Security | ● ● ● ● ● |
| Interoperability | ● ● ● ● ● |
| Usability | ● ● ● ● ○ |
| Ease of Delivery | ● ● ● ● ● |
| ID Management | ● ● ● ● ● |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ● ● ● |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

## Strengths

- Robust option for implementing full identity ecosystem
- Patent-protected Account Recovery mechanism that allows the recovery of a private key and identity credentials without the holding server being able to decrypt the information
- Users have the option to share identity credentials selectively
- Only a hash value of credentials stored on-chain
- Supports Bring Your Own ID (BYOID) concepts

## Challenges

- Blockchain is powered by proof-of-work (PoW) which is an expensive form of consensus
- Offers only large-scale solutions for enterprises, may receive more functionality than is necessary
- Storage of identity information is restricted to a single mobile device


SHOCARD
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

## 5.10 uPort

uPort was founded in 2016 in New York, NY, USA. It serves to develop SSI solutions for users and enterprises. Both its uPort Serto and uPort Open products can be used with consortium ecosystems, Enterprise Ethereum, and public protocols.

uPort developed both of its solutions on the Ethereum blockchain, and both solutions work with a user wallet and enable the secure exchange of identity credentials. While uPort Open has been available and continuously improved since it was released in alpha version in early 2017, uPort Serto will become available in early 2020. Applications for both solutions are managed with Ethereum smart contracts. The solution uses the ERC 1056 smart contract used does not require blockchain transactions unless completing certain operations, such as key rotations.

uPort offers well-designed products for integrating SSI solutions into enterprise identity management and facilitating the exchange of verifiable data in a variety of use cases. The company’s relatively long experience with public protocols adds validity and knowledge to the adjustments made for the enterprise-focused Serto products. It lacks biometric capabilities, has a robust community of partnerships that has led to the access of other important capabilities, such as eID compatibility.

u·port

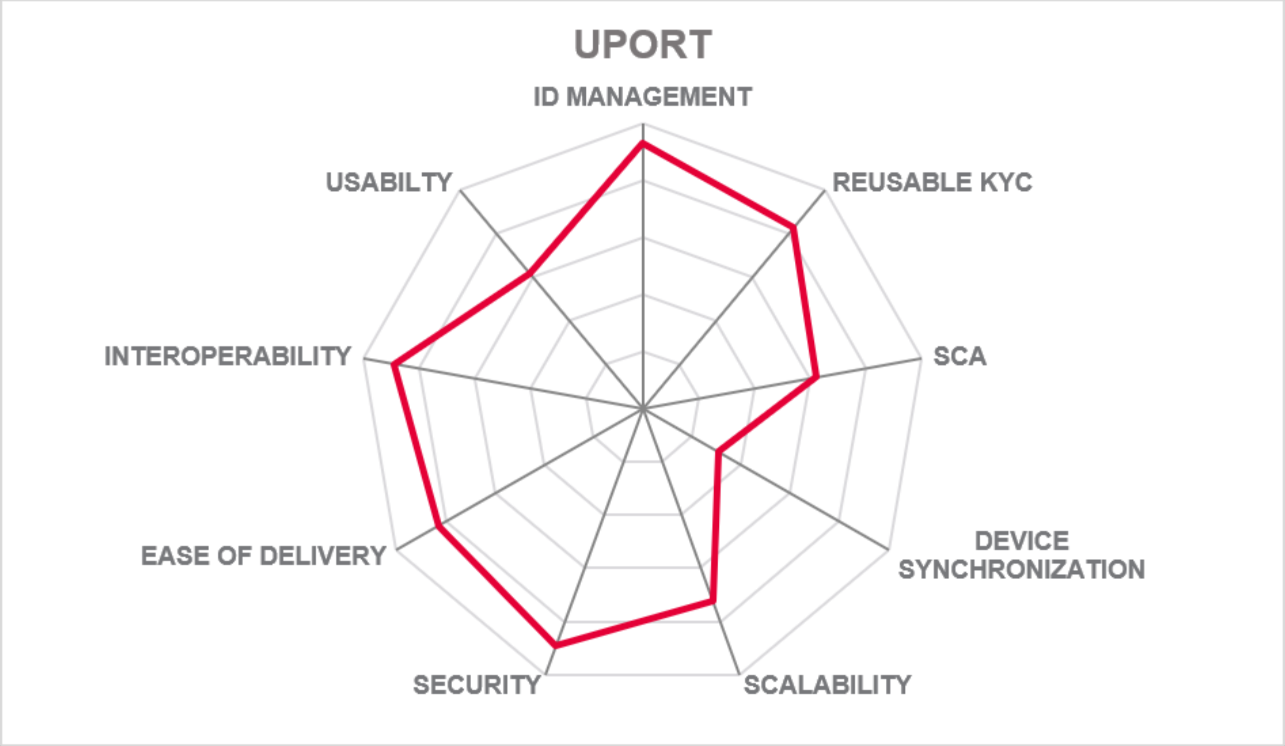
| | |
|---|---|
| Security | ● ● ● ● ● |
| Interoperability | ● ● ● ● ● |
| Usability | ● ● ● ● ○ |
| Ease of Delivery | ● ● ● ● ● |
| ID Management | ● ● ● ● ● |
| Reusable KYC | ● ● ● ● ● |
| SCA | ● ● ● ● ○ |
| Device Synchronization | ● ● ○ ○ ○ |
| Scalability | ● ● ● ● ○ |

## Strengths

- Robust applicability in wide range of use cases for both user and enterprise
- Creates positive networking effects by maintaining strict verification processes
- Data recovery is possible through deploying a Replaceable Controller contract

## Challenges

- Solutions are working towards becoming blockchain agnostic
- Biometric capabilities are lacking
- Options for device synchronization are currently weak


UPORT
ID MANAGEMENT
REUSABLE KYC
SCA
DEVICE SYNCHRONIZATION
SCALABILITY
SECURITY
EASE OF DELIVERY
INTEROPERABILITY
USABILTY

# 6 Related Research

Buyer’s Compass: Blockchain ID – 80050
Leadership Brief: Blockchain ID & Self Sovereign Identity – 80105
Executive View: 1Kosmos BlockID – 79064
Executive View: IBM Decentralized Identity – 80099

# Methodology

### About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.
While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices based **only** on the information provided within this report.
Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn’t provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

### Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.
KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

**Security** is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

**Functionality** is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

**Deployment** is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

**Interoperability** refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

**Usability** is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

### Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are:

- **Strong positive**
  Outstanding support for the subject area, e.g. product functionality, or security etc.)

- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren’t met, while others are well served.

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

# Content of Figures

# Copyright

All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

**KuppingerCole** supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

**KuppingerCole**, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.