KuppingerCole Report

MARKET COMPASS

By Anne Bailey
March 19, 2021

Providers of Verified Identity

The KuppingerCole Market Compass provides an overview of the product or service offerings in a certain market segment. This Market Compass covers the Providers of Verified Identity market, and solutions with specific functionality in identity verification with potential for digital identity reuse. The rise of reusable, verified identity for use cases like remote employee onboarding and KYC for high value transactions can aid in a company's digital transformation, as well make significant progress towards better privacy and user-centric identity management.

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.

This Market Compass considers the future of identity. Enterprises face the dilemma of deciding how to enable customers, employees, and partners to interact securely with their systems, especially with the increasing pressure for identity to be digital, privacy-forward, user-centric, and reusable. KuppingerCole views identity verification as an enabler of future identity ecosystems that opens up new use cases for enterprises, such as remote onboarding for employees and partners, remote verification for KYC/AML, and more. The Market Compass on Providers of Verified Identity presents the vendors who are active in providing identity verification with potential to support verified identity reuse.

The Providers of Verified Identity that are covered in this Market Compass are vendors that deliver solutions to verify that a digital identity corresponds to a real-world identity. These vendors provide an employee, end-user, device, or legal entity with a digital identity that may be used across multiple platforms, services, or with multiple companies. The Providers of Verified Identity Market Compass is a future-oriented assessment at how onboarding and continued relationships between entities will be handled for the highest privacy, compliance for KYC/AML regulations, and ease of use.

There are multiple approaches to providing a verified digital identity, and just as many approaches to transform a verified digital identity into a reusable one. For this reason, KuppingerCole considers this a highly heterogeneous market, and each vendor should be considered for its individual efforts to achieve the goal of providing a verified identity.

Readers of this Market Compass should consider vendors based on the internal requirements of their organization’s use cases, and use this report as guidance to shortlist vendors.

Highlights:

- KuppingerCole predicts a major trend towards verified identity to support reuse of consumer and employee identities in the near future
- The ability to automate identity document verification is required, and is increasingly offered by identity verification vendors
- Biometric data collection is a supportive technology to enable verified identity reuse
- Interoperability with standard authentication sources and directory services is expected

- No single dominant method has emerged, but the market promises rapid and dynamic change

2 Market Segment

This Market Compass covers the Providers of Verified Identity, which is a look into the future of identity. This report identifies the trends that are influencing the identity provider market to favor digital identities that are verified and reusable. The market segment is defined, the technological approaches to providing a reusable verified identity are described, the major use cases are highlighted, and the trends are discussed. The rest of the report covers the range of vendors that are active in this segment offering ratings and comparisons of capabilities.

2.1 Market Description

The Providers of Verified Identity that are covered in this Market Compass are vendors that deliver solutions to verify that a digital identity corresponds to a real-world identity. These vendors provide an employee, end-user, device, or legal entity with a digital identity that may be used across multiple platforms, services, or with multiple companies. The Providers of Verified Identity Market Compass is a future-oriented assessment at how onboarding and continued relationships between entities will be handled for the highest privacy, compliance for KYC/AML regulations, and ease of use.

The technology that Providers of Verified Identity use to facilitate digital-only onboarding and identity verification is varied, and the identity may use passwords, certificates, biometrics, eTokens, federation of trusted sources, Decentralized Identifiers, or be supported by Artificial Intelligence (AI). But the services that Providers of Verified Identity bring are foundational to delivering the security required for IAM, the streamlined solutions required for CIAM, and the means to adhere to strict AML and KYC requirements in highly regulated industries.

The inclusion criteria for this report are:

- Digital-only onboarding is facilitated
- An identity verification step is included in the onboarding process
- Digital ID is created with the possibility for reuse in other contexts
- The secure storage and protection of identity data is included

Capabilities that are often found in these solutions include authentication, verification of physical and/or government-issued IDs, other document verification, support for national and/or other eIDs, customer self-service, single sign-on (SSO), and electronic signatures. These extra capabilities are often delivered by

Verified Identity Provider products but are not required for inclusion in this report.

The exclusion criteria for this report are:

- Vendors that only provide ID verification are excluded
- Vendors that only provide a national ID for the use of one country or region's citizens are excluded
- Vendors that provide digital IDs that have no potential for reuse in the upcoming roadmap are excluded

A reusable verified identity has the potential to change the trust afforded to credentials from other systems, the storage of user data, the effort needed to adhere to privacy and compliance regulations, and ability to prevent fraud. There is the potential to create much more user-centric identity systems while increasing their portability. These are disruptive proposals, and the many vendors who are active in delivering such solutions take varying technological paths to achieve them. The dominant technological approach is not yet clear – many products are newly launched, and others are adapting their established and familiar approaches to adjust to the changing trends. These technological approaches are presented in this Market Compass:

- **Fraud Detection:** The vendor uses a collection of indicators to positively identify the user during the registration or login process to determine that the user is not a bot, is the individual he or she claims to be, and a decisioning component that recommends whether additional proof of identity is needed. Fraud detection factors include detection of malware, device intelligence, geolocation, behavioral factors such as keystroke analysis, biometric information, and more. The decisioning component is often supported by AI and Machine Learning to deliver a confidence score, and recommendation of step-up authentication factors.
- **Document and Video Verification:** This method is the initial transition from face-to-face identity verification to remote, digital verification. The user conducts a video call with a trained document checker, who verifies that the user does possesses a valid identity document that corresponds with their real identity. Automated methods enable the user to scan their identity document to check against authoritative government sources, and triangulate data collected via the Machine-Readable Zone (MRZ), biometric chip via NFC, and OCR. This information is compared with a real-time video selfie of the user to check for liveness and that the photo ID matches the individual in possession of it.
- **Federated Identity Hub:** An API-driven identity hub that is situated between trusted identity providers and enterprise systems. A strong emphasis is put on integration with standard authentication sources such as SAML, OpenID Connect and OAuth2 as well as decentralized protocols like DID and Verifiable Credentials enable digital identities from a large variety of trusted

sources to be used to register, verify, or authenticate the user in an enterprise system.

- **Decentralized Identity Verification:** This method builds off automated methods to verify a user's identity documents and biometrics by facilitating the storage and reuse of the digital identity. Using decentralized architectures like blockchain, DAG, etc., the user's identity attributes from their identity document are verified against authoritative government sources. The proof that the information is verified is hashed and stored in the decentralized ledger, while the identity information itself remains in the user's mobile device. The proof of verification is shared in peer-to-peer interactions or between the user and business entities. Standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) harmonize the way identity attributes are described for increased interoperability.

2.2 Major Use Cases

Providers of Verified Identity are enabling higher security, trust, and privacy beyond what traditional identity interactions could afford. The main applications of this solution in the market are:

- **New customer onboarding:** Targeting CIAM, a new user completes a digital onboarding process using a previously created and trusted identity – such as an eID or BankID – or onboards a government-issued ID and biometric information to create a verified, reusable identity with which the user can repeatedly interact with their service provider with a heightened level of assurance.
- **Verification uplift for KYC/AML processes:** The trust in a user's identity can be uplifted for a critical transaction by verifying a preexisting digital identity. Using document scans, connection with biometric information, and/or video identification, KYC and/or AML requirements can be fulfilled remotely. In advanced cases, this verification can be reused.
- **New employee or B2B partner onboarding:** Targeting IAM, a new employee or partner presents evidence of their identity and can be remotely provisioned and issued access rights. Integrations with authentication sources and interoperability of verified identity attributes are critical here.
- **Verified identity as an authentication factor:** For CIAM and IAM scenarios, a verified identity can be created by proving that an identity document is connected with the biometric data of an individual in the real world. When authenticating, the user can present the biometric data as a second factor, which is linked to the existence of a verified identity document.
- **Share identity attributes or credentials with relying parties:** Extending beyond the typical identity attributes such as name, date of birth, address, contact information, ID document number, customer

or employee ID, etc., sharable identity attributes include employment experience, education experience, health records, ownership records, intellectual property rights, and much more. Connected to a verified identity and formatted in a standardized manner, these identity attributes or credentials can be shared with other parties in peer-to-peer transactions or between business entities. The sharable attributes or credentials can be trusted to be valid.

2.3 Market Direction

Several trends are setting the stage for reusable verified identity. Digitalization is an ongoing megatrend that impacts how consumers interact and receive services and how employees and business units collaborate internally and with external partners. The global pandemic has increased the need to operate remotely, which has accelerated the digital transformation of many companies and exposed the gaps in digital capabilities. Remote identity verification for high value transactions, onboarding employees and partners, or many other use cases is foundational to enabling further digital transformation of both enterprise operations and customer interactions.

Regulations, ranging from fraud prevention to privacy, drives the need to reimagine identity management. The list of relevant regulations is long and puts increasing pressure to both know more about customers and partners while also ensuring their data is private and secure. Achieving both with current identity management methods is challenging and creates a compelling case for reusable verified identity. Below is a non-exhaustive list of relevant regulations:

- EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (most commonly referred to as eIDAS)
- ISO/IEC 29115 Entity Authentication Assurance Framework establishes the specifications for assurance levels for electronic identification. ISO/IEC TR 29156:2015 provides guidance for specifying performance requirements to meet security and usability needs in applications using biometrics.
- Money Laundering and Terrorist Financing 2017 applies to most organizations including financial institutions, trust or company service providers, cryptoasset exchange providers, and custodian wallet providers.
- International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents, Council Regulation (EC) No 2252/2004 describe the specifications that a MRTD should follow, the latter being specifically for EU Member states.
- German Federal Financial Supervisory Authority (BAFIN) Circular 3/201722: For biometric and

liveness detection tests, the BAFIN requires end-to-end encryption on communication channels and verification of the security features on an ID document.

- NIST 800-63-3 Digital Identity Guidelines sets standards for digital identity systems, the requirements that are necessary to achieve a particular identity assurance level (IAL), authentication assurance levels (AAL), and federated identity architectures.
- The Pan-Canadian Trust Framework is establishing a set of requirements for business and technology to identify, authenticate, and authorize users in digital interactions.

User-centricity is another trend that will shape the future of identity. Letting the user manage their own private information while enterprises can still gain compliant insight from the data is a win-win for all parties. Onboarding becomes a less painful process, as well as compliance for the increasing number of privacy regulations.

Reuse is a topic that KuppingerCole predicts will become more critical to digital identity. Currently identity verification is restricted to one time use, as there is no generally accepted way to store a verification for future use. This is changing with the arrival of decentralized solutions that store timestamped, immutable proofs that an identity attribute was issued and approved by a trusted party. The advent of reusable identity dovetails with increased automation in identity verification. Verification via video call, which relies on trained human experts to check an ID document while on a video call is still held as the highest level of assurance after face-to-face verification in countries like Germany, but in many other countries preference for fully automated methods of identity verification is rising. When a digital identity can be verified for multiple uses, this will likely trigger large savings for companies in identity management, but also open new markets for credential exchange.

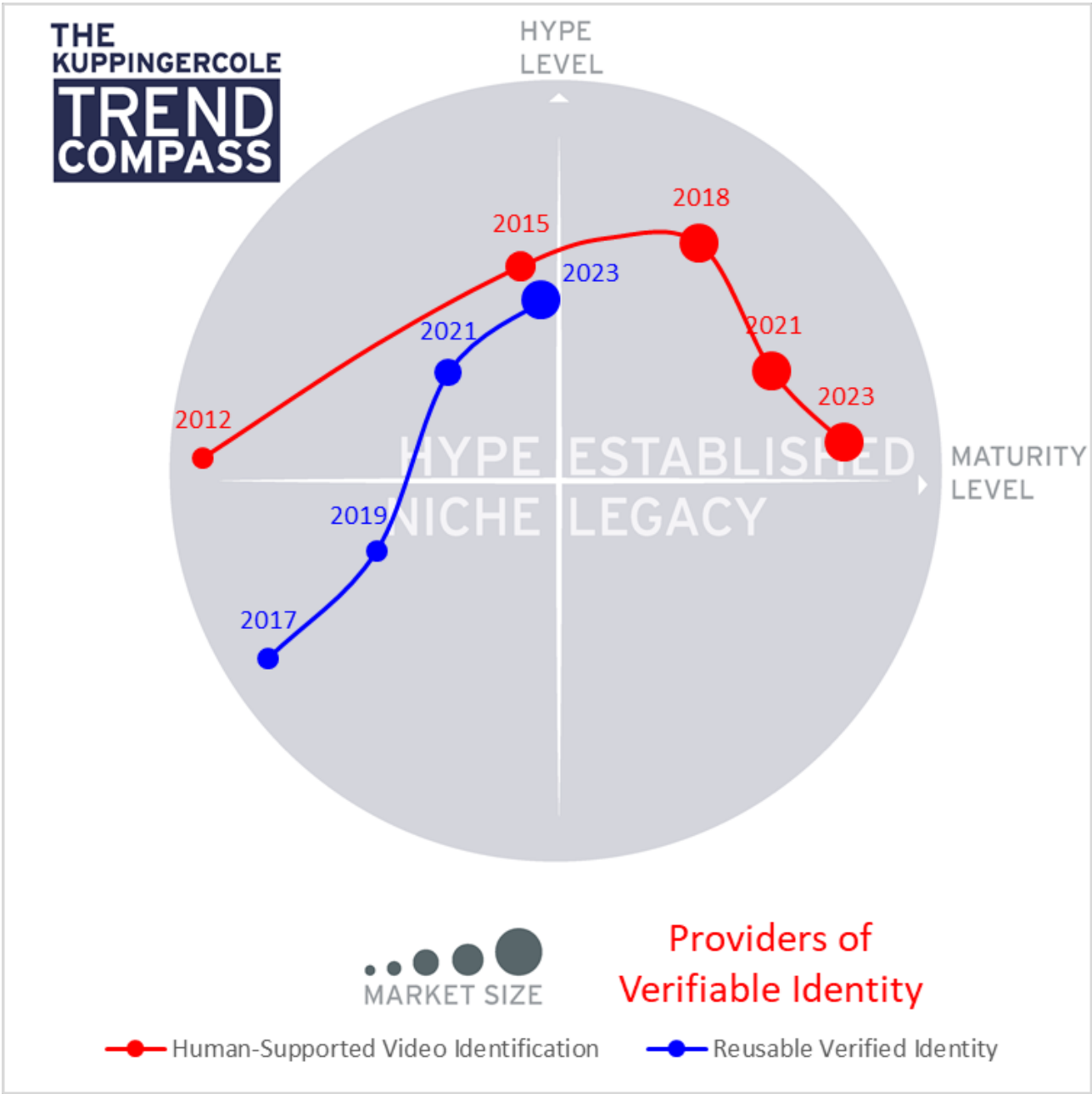


Figure 1: The KuppingerCole Trend Compass for Reusable Verified Identity

The KuppingerCole Trend compass shows the rise and growth of video identification, following the need for verified digital identity. However, methods for reusable verified identity will likely gain traction in the coming years, displacing the need for manual video verification for a one-time verification for multiple uses.

3 Capabilities

The Market Compass is designed to profile and compare vendors across numerous capabilities. This section details the capabilities that one should expect to see in this market segment and breaks them down according to relevance per use case.

3.1 All Capabilities

The Providers of Verified Identity segment has a collection of standard capabilities that most solutions should include. These are listed in the table below.

Capability	Description
Identity Document Processing	Ability to process multiple types of identity documents, from different regions, in different forms (updates, versions) and be checked for authenticity against authoritative sources such as a national registry database. Triangulating data from OCR, smartphone NFC of embedded chip, and the MRZ of identity documents to increase the confidence level that the document is valid and authentic.
Video Identification	Establish web-based video call with trained identity document professional for remote face-to-face identification.
Biometric Data Collection	Collect and process an authoritative sample for face, voice, and/or fingerprint for initial verification and for later authentication.
Liveness Check	Additional check that the individual being identified is present at the time of verification/spoofing attacks. Analyze a selfie video where the individual is requested to look or move in a certain way.
Identity Attribute Collection	Collect, verify, and share standard identity attributes (name, DOB, address, contact info, identification numbers, account numbers) and nontypical identity attributes (education credentials, employment credentials, health records, etc.)
Fraud Detection	Ensure that identity documents and biometric data is not falsified, including IP address collection, GPS, behavioral features, keystroke analysis, etc. Confidence scoring often accompanies Fraud Detection capabilities, determining that the user logging in is the individual that the account has been associated with, and is typically supported with AI/ML.
Verified Identity Reuse	Enable reuse of a verified identity. Can be achieved with verified credentials and wallets, federating trusted digital IDs, leveraging APIs and orchestration.

Capability	Description
Authentication Based on Verified Identity	Apply verified identity to authentication as a second factor using biometrics, step-up, fact-based. Interoperability with authentication sources and use of standards is critical.
Secure Data Storage	Secures the identity data on behalf of the user or establishes secure methods for the user to store their own identity data. Could include private cloud, blockchain/DAG, secure enclave on mobile device. Data should be encrypted at rest and in transit.
User-Centricity	Position the user to be in control of their identity data, approve transactions, ability for self-service account recovery, accessibility for disabled users.
Privacy	Specific attention to end-user privacy in solution design, information collection, storage, and transactions, including collecting appropriate consent from users, ability to revoke access to identity attributes, accessing a history of what entities have record of or accessed their identity attributes, etc.

Table 1: Standard Capabilities of Providers of Verified Identity

3.2 Capabilities Recommended per Use Case

The Providers of Verified Identity segment is evolving to meet several distinct use cases, as described in section 2.2. Each of these use cases require heavier dependence on certain capabilities than others to succeed. Below, the capabilities are displayed according to their relevance for each use case.

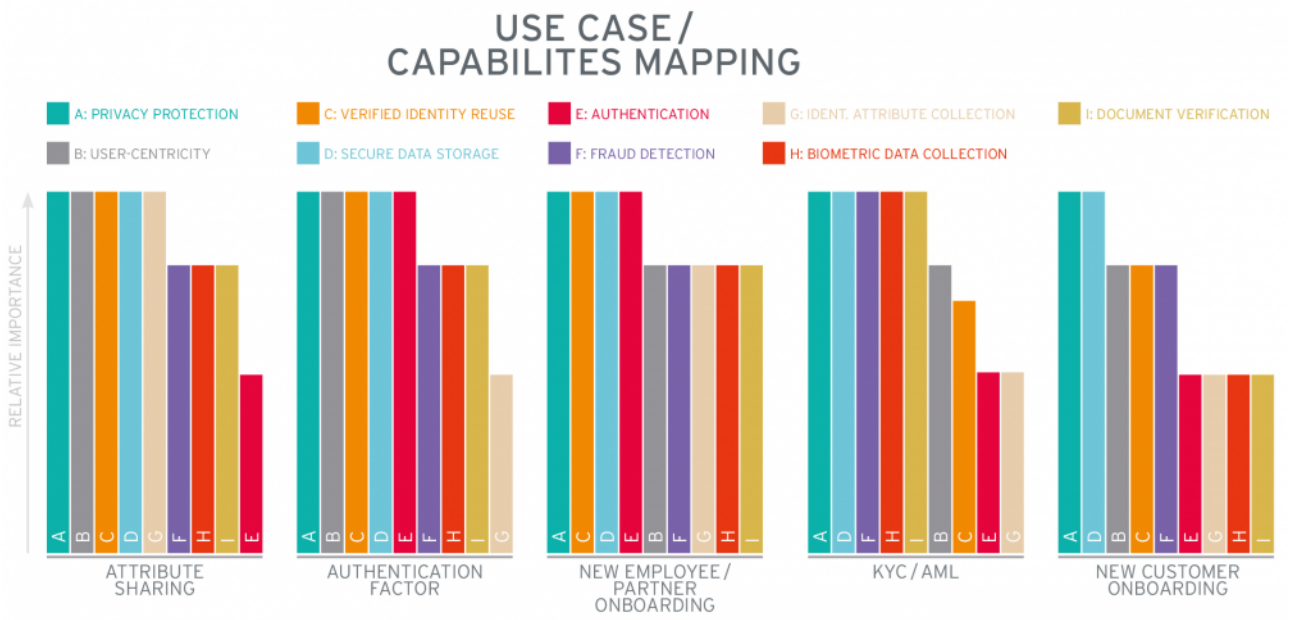


Figure 2: Relevance of Capabilities to Top 5 Verified Identity Use Cases

The use case for sharing identity attributes with another party, such as proving the user's age to access age-restricted services puts emphasis on the protection and mobility of identity attributes. Therefore, capabilities such as identity attribute collection and verified identity reuse are essential to delivering this use case. Having a variety of independently sharable attributes – a user's age – instead of grouped attributes – such as all the information provided by a driver's license – also contributes to the usability. Secure storage, fraud detection, and privacy are paramount here, as private and personal information is exchanged. Supporting capabilities are document verification and biometric data collection, which often underpin solutions that enable the attribute sharing use case.

Using identity attributes as an authentication factor is another rising use case. Verified identity reuse is critical here, as it is the foundational capability to demonstrate that an identity attribute is an adequate and trustable authentication factor. Support for standard authentication sources and interoperability for using verified identity attributes as an authentication factor is also very important to delivering this use case. Other requirements include the secure data storage, user-centricity, and privacy protection of the information. Fraud detection is an additional support to delivering a high-quality authentication solution, and document verification and biometric data collection support the overall feasibility of delivering solutions for this use case.

The use case for onboarding new employees/partners combines elements of attribute sharing and authentication use cases. For new employees to be onboarded remotely, they must be able to present documentation and credentials in a secure way and establish authentication methods that should include identity attribute options. Verified identity reuse is essential in such solutions, supported by secure data storage and privacy protection. User-centricity is still desired, though not as essential here, and likewise with document verification, biometric data collection and fraud detection.

KYC/AML use cases center on the veracity and reliability of data. Thus fraud detection, document verification, biometric data collection, secure data storage, and privacy protection are essential capabilities. User-centricity is a desired capability, as well as verified identity reuse though this capability may increase in importance as verified identity reuse becomes more widely available. Identity attribute collection is of middle importance here. Breadth of coverage for many identity attributes is less important than collecting the specific attributes required by regulators. Authentication is also of middle importance.

The use case for new customer onboarding must place privacy protection and secure data storage at the forefront to establish user and relying party trust. This is closely followed by user-centricity of verified identity reuse, which go hand-in-hand. With large volumes of users, the need for robust fraud protection becomes more essential. Depending on the level of assurance required by the use case, capabilities such as document verification, biometric data collection, identity attribute collection, and authentication are of middle importance.

4 Ratings at a Glance

This chapter provides a comparative overview of the participating vendors for five categories: security, deployment, interoperability, usability, and market standing. It also highlights the outstanding performers in each of the nine capabilities that were assessed.

4.1 General Product Ratings

Based on our evaluation, a comparative overview of the ratings of the general standing of all the products covered in this document is shown in the table below.

Product	Security	Interoperability	Usability	Deployment	Market Standing
1Kosmos BlockID Verify	strong positive	positive	strong positive	strong positive	neutral
Avoco Identity Trus-T	strong positive	strong positive	strong positive	positive	positive
Callsign Intelligence Driven Authentication	strong positive	strong positive	strong positive	positive	neutral
Consensys Mesh Veramo	positive	positive	neutral	weak	weak
esatus SeLF	strong positive	strong positive	positive	strong positive	neutral
Experian CrossCore	strong positive	neutral	positive	strong positive	strong positive
Jumio KYX Platform	strong positive	neutral	strong positive	strong positive	strong positive
KYC-Chain SelfKey	strong positive	strong positive	positive	strong positive	neutral
Microsoft Azure Active Directory Verifiable Credentials	strong positive	positive	positive	strong positive	strong positive
Octopus Self Sovereign Identity Solution	positive	neutral	positive	positive	neutral
Onfido Identity Verification	strong positive	positive	strong positive	strong positive	positive
Oxyliom Solutions GAiA Trust Platform	strong positive	positive	positive	strong positive	neutral
Ping Identity PingOneVerify	strong positive	positive	positive	strong positive	strong positive
SecureKey Technologies Verified.Me	positive	positive	positive	positive	neutral
Signicat	strong positive	strong positive	positive	strong positive	positive
Thales Remote Identity Verification and Mobile ID	strong positive	strong positive	positive	strong positive	strong positive
Verimi	strong positive	positive	positive	positive	neutral
WebID	strong positive	positive	neutral	positive	strong positive
Yes Platform	positive	positive	positive	strong positive	neutral
Yoti	strong positive	positive	strong positive	positive	neutral
Legend		critical	weak	neutral	positive	strong positive

4.2 Noteworthy Vendors for Specific Capabilities

Some vendors are better positioned to meet narrow use cases, while others have stronger offerings across the range of this market segment. We have identified a few vendors that are notable for their strengths for specific capabilities. A vendor has been selected as outstanding based on information collected during our neutral research and rating process.

4.2.1 Outstanding in Verified Identity Reuse: Microsoft & Ping Identity

Although its product is just freshly on the market, Microsoft has a strong potential to apply verified identity reuse to several different use cases, including remote employee and partner onboarding and authentication, onboarding and authentication for consumers, and educational credential creation and sharing. Microsoft also has a strong enough market presence to quickly gain a mass usership.

Ping Identity, a major player in IAM and CIAM services, expanded the use of digital, decentralized identities that can be onboarded and verified with the acquisition of ShoCard. The expertise gained from this acquisition led to PingOneVerify and the ability to integrate Verifiable Credentials with typical enterprise systems. In doing so, they have integrated remote self-service verification capabilities for user, employee, and partner onboarding, as well as a variety of other use cases, and to verify an unlimited number of identity attributes for later use in that verified relationship.

Figure 3: Outstanding in Verified Identity Reuse: Microsoft & Ping Identity

4.2.2 Outstanding in User-Centricity: 1Kosmos & Verimi

1Kosmos centers its services around the user. User identities are self-attested or onboarded from identity documents, then verified with authoritative sources. The identity data is held by the user, stored in the secure enclave of their mobile device. The user has access to a full record of identity transactions to know which identity attributes have been shared with which entity, when.

Verimi enables users to build a digital identity for onboarding and authentication with customer services. The user's Verimi account with more than 30 ID attributes from 10+ external ID sources or verification services is synchronized and accessible across all devices, with offline use cases also enabled. In addition, the user's data is individually encrypted by external trusted services so user profiling is prohibited. Users provide consent before any data is shared, and can access a full list of which identity attributes have been shared with which entities as stored within Verimi. A user can delete their account, related data, encryption keys, and transactions at any time.

Figure 4: Outstanding in User-Centricity: 1Kosmos & Verimi

4.2.3 Outstanding in Document Verification: Thales

Thales supports document verification for digital identity onboarding in a variety of ways: face-to-face or remotely, and from a smartphone. Depending on the ecosystem and legal framework, the identity verification can be done by capturing the data from a non-electronic ID document. Facial biometric technologies with passive liveness and auto-capture check both the authenticity and of the document as well as the identity of the document owner. This is made possible due to a document templates data base with more than 2,000 unique types of ID documents (passports, identity cards, driver's license cards, etc.). Alternatives include NFC reading of an electronic document from a smartphone or selfie which is matched on a biometric database, national registry with a 1:1 or 1:n matching. Those solutions benefit from AI-powered document and identity verification software.

Figure 5: Outstanding in Document Verification: Thales

4.2.4 Outstanding in Biometric Data Analysis: Onfido

Onfido collects biometric and liveness data with close attention to the trustworthiness of that data. Dedicated efforts with the UK's ICO have worked to identify and reduce algorithmic racial bias. AI/ML models are used to detect for face insertion, photo of a photo detection, spoofing detection, video submission, and font anomalies. A dedicated team of ML developers maintain and improve on these capabilities.

Figure 6: Outstanding in Biometric Data Analysis: Onfido

4.2.5 Outstanding in Identity Attribute Collection: Avoco & Octopus

Avoco provides an identity hub which is situated between the data sources and a relying party and uses an identity API to call identity data for verification, authentication, etc. when needed. Avoco's connectors to major identity systems including ForgeRock, Ping Identity, and thousands of BankIDs are available out of the box, as well as compatibility with decentralized identity standards. With this widespread compatibility, an unlimited variety of identity attributes can be called for and used in identity transactions.

Octopus supports the onboarding of government-issued identity documents as well as verifying many other attribute types between trusted parties, including employment credentials, educational credentials, etc. Octopus' decentralized architecture allows users to have a secured identity vault per relationship, creating separation between the different professional, public, and private aspects of a user's life. Each identity vault can be set as public, private, or shared catalogs. Anonymous interactions are possible.

Figure 7: Outstanding in Identity Attribute Collection: Avoco & Octopus

5 Product / Service Details

In the following section, each participating vendor is profiled with particular attention paid to the functionality of its product. Several important capabilities for providing Verified Identity have been selected and rated, displayed as a spider chart. For this Market Compass, we look at the following nine areas:

- Secure Data Storage
  Considers how the identity data of a user is stored, including the location, the security measures taken to protect it at rest and in transit, etc.
- Verified Identity Reuse
  Considers the application of and feasibility of different identity reuse use cases, such as using the digital identity across different ecosystems, age verification, storing and sharing Verified Credentials, etc.
- User-Centricity
  Considers the positioning of the user in relation to their identity data, including the control over what attributes are input into the system, their ability to approve sharing those attributes, etc.
- Privacy Protection
  Considers the level of privacy afforded to the user over their identity data, including collecting appropriate consent from users, accessing a history of what entities have record of or accessed their identity attributes, etc.
- Document Verification
  Considers the regional reach of documents able to be verified, the cross-referencing ability between MRZ, OCR, Biometric chips, etc.
- Biometric Data Collection
  Considers the types of biometric data collected, where it is stored, and its application towards secure digital identity reuse.
- Identity Attribute Collection
  Considers the range of other digital identity attribute inputs that may be possible, including onboarding with eIDAS, BankID, sharing and storing Verified Credentials, etc.
- Fraud Detection
  Considers the processes taken to ensure that identity documents and biometric data is not falsified, including IP address collection, GPS, behavioral, keystroke analysis, etc. Also considers the emphasis on positively identifying a user compared to fraud detection efforts.

- Authentication
  Considers the use of verified identity for authentication use cases.

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 2018 and is headquartered in New Jersey, United States. It provides digital identity and passwordless authentication solutions for enterprises and consumers. BlockID Verify enables an entirely digital onboarding and identity verification for its BlockID Workforce and BlockID Customer products. Regional coverage is for North America, Western Europe, India, Middle East, Singapore, and Australia.

BlockID Verify creates a verified digital identity for use in various onboarding, authentication, and consumer transactions. To initiate a verified onboarding process, the user is prompted by the service they are accessing (for example, an ecommerce platform) to scan a QR code with their mobile device to download the free BlockID app. The app functions as an ID wallet, allowing the user to verify their passport and driver's license by scanning the front and back of each document, and verifying that these photo IDs belong to the individual holding the phone by verifying a face scan and liveness check. Proprietary AI classifies the document and checks for fraud, while also reading embedded RFID chips. This verification satisfies NIST 800-63-3 for Identity Assurance Level 3 and Authenticator Assurance Level 3. BlockID is also FIDO2 and NIST certified.

BlockID Verify operates on a blockchain-agnostic Directed Acyclic Graph (DAG). The user's identity and biometric data is stored encrypted on their device's secure enclave, managed by a private key. The data is also sharded and stored in IPFS, encrypted at rest and doubly encrypted in transit. Only hashes of identity verification transactions are stored on the DAG. It uses atomic swap smart contracts to maintain high scalability and manage between-blockchain transactions. Users can synchronize identity data across multiple devices with a seed phrase. Additional authentication factors include a PIN, voice recognition, and fingerprint recognition. The user is required to have a smart mobile device with camera functionalities.

Security	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●
Market Standing	●●●○○

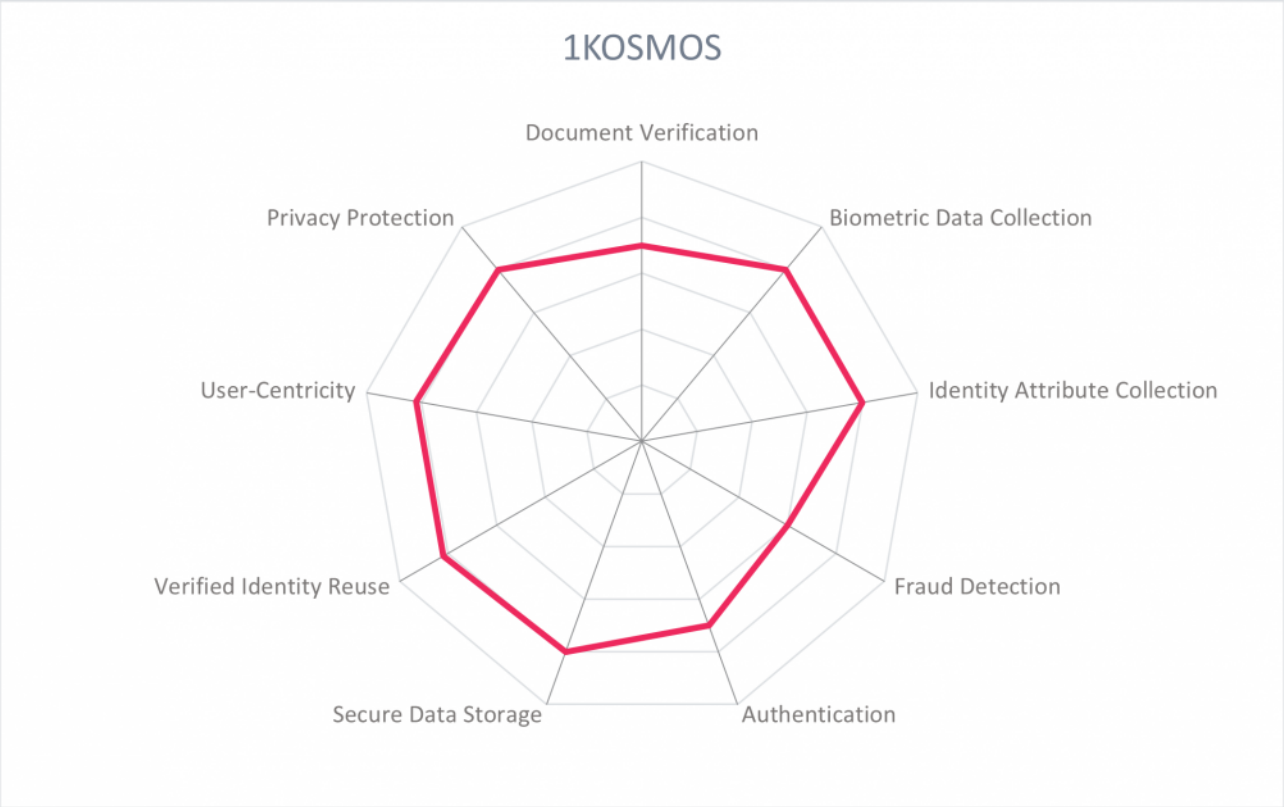
1KOSMOS BlockID

Strengths

- Biometric authentication factors include face, voice, and fingerprint, and are independent from device biometric capability
- Has backend integration with trusted governmental institutions to verify ID documents
- Provides strong enterprise workforce authentication to achieve critical mass of users
- Process for user data recovery is in place
- Uses standardized Verified Credentials and Decentralized Identifiers for credential storage and sharing
- Supports AD, LDAP, JWT, OAuth, OIDC, and SAML

Challenges

- Support for eIDAS is on the roadmap
- Requires the user to have a smart mobile device with camera functionalities
- Is a small vendor with some restrictions on regional document coverage

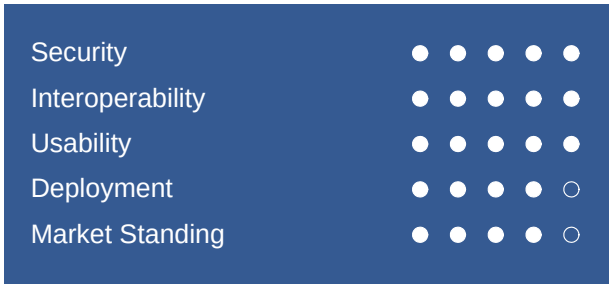

1KOSMOS
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.2 Avoco Identity

Avoco Identity is based in the UK and has been delivering identity solutions since 2003. It leverages Open Banking and other authoritative identity attribute providers with its proprietary identity API to deliver verified identity services, packaged as an identity hub: Trust-T. Its regional focus is on the United Kingdom, but has compatibility with some Western European countries and plans of expansion.

Avoco uses its identity hub, situated between sources of data and relying parties (RP) to enable identity collection from trustworthy sources for verification, authentication, consent management, account management, etc. An RP customer, for example a bank or a retailer, selects which trusted identity providers – connected via Avoco's API to the Trus-T identity hub – to use for onboarding and authentication. The user is then prompted to onboard with the selected identity providers, typically a bank ID. The hub is rule-based, able to customize requirements such as selectively calling the necessary identity attributes for that customer's transaction. Connections to decentralized ledgers for storing the user's assurance level for future use is also possible. Document checks for drivers' licenses, passports, and optionally for other documentation can be conducted with a document scanner offered through partners or manual input to be checked against a government database. Face-to-face verification is possible at designated locations. Biometric verification is an option for real time security uplift from partners including Thales, matching a document photo against a selfie or collecting behaviorally biometric data.

The identity hub is hardened against several vulnerabilities such as SQL Injection. No data is stored with Avoco but stored based on the customer's requirements. A consent UI can be configured to a user journey to match the specific requirements of each transaction, which can be supported by the programmatic method Variable Claims for selective attribute sharing. Privacy and consent management is rule based, configurable based on the needs of relying parties, including dynamically updated and automatic re-consent requests if needed. Pairwise pseudonymous identifiers are used to obfuscate personal data in transactions. Deployment is available on premise or in the cloud. The licensing structure based on transaction volume, tiered by the trust level provided and additional fraud checks and security features chosen by the customer.

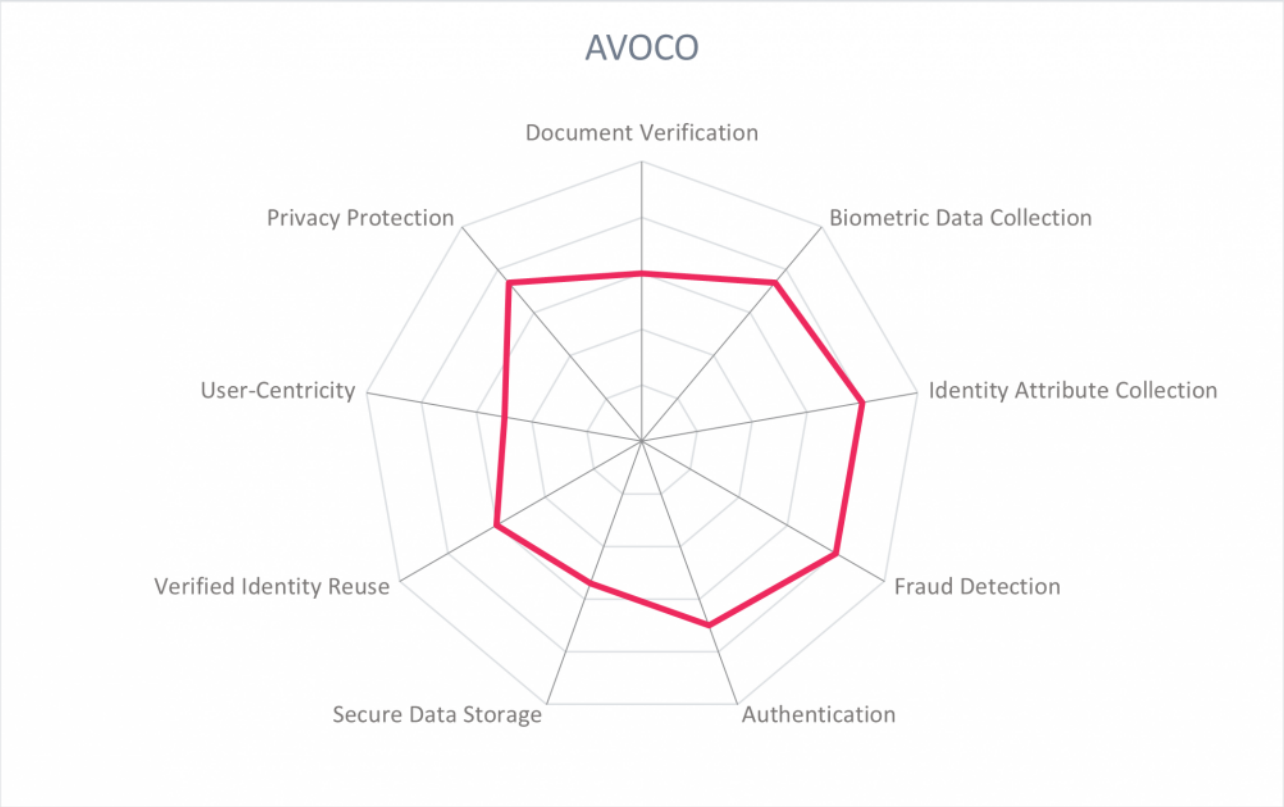


Strengths

- Is a streamlined option to benefit from already verified bank IDs and other digital identities
- An innovative approach to enabling reuse across identity ecosystems
- Connects to decentralized solutions to enable reuse of verified identities
- Hub supports online environments, mobile apps, in-person interactions, phone, and keyboardless devices
- Has solutions for disabled users
- A highly customizable solution to meet a wide range of requirements, use cases, and industries

Challenges

- A focused solution for the UK with limited support for Western Europe, with wider expansion as a long-term goal
- A less user-centric approach, structured around the relying parties preferred data sources


AVOCO
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.3 Callsign

Callsign, founded 2012 in London, UK, provides verified identity through strong fraud detection and adaptive authentication methods. Its Intelligence Driven Authentication is an identity platform that first detects and block threats, then positively identifies the user, and facilitates the user's identity lifecycle. While not an identity provider, Callsign's product acts as an enabler for identity providers to securely interact with the user. Regional coverage is global.

Intelligence Driven Authentication supports a customer's authentication processes behind the scenes. When a user logs into their account, Callsign first identifies whether the session is secure by detecting malware, checking for compromised devices, SIM swaps or SS7, and location intelligence. Once the session has been determined to be secure, the system analyzes the authentication journey determined by the customer, including biometric, device ID, behavioral biometrics, OTPs, QR Codes, Hard and/or Soft Tokens to compile a confidence score supported by proprietary AI/ML. Based on the individual confidence scores (for example, of a new location which prompts a lower score), step-up authentication can be prompted. This policy engine and decisioning element is customizable based on customer and industry requirements, with A/B testing, and is fully auditable. For use cases that require identity verification, document scans, or video identification are possible via technology partnerships with multiple identification and verification providers. Identity Assurance Level 3 can be achieved.

Callsign takes a SaaS platform approach, but can deploy on premise. Web and mobile SDKs are provided, compatible on all browsers. Out of the box integrations include ForgeRock, Ping, OIDC, and SAML. The mobile app can be white labelled. Data is encrypted at rest, with sensitive fields encrypted with a key, uses SSL in transit. All PII is hashed on the client side before leaving the user's device. Attributes like GPS location are fuzzed for privacy, and uses robust API connectors. Callsign has support for ISO27001, and is dedicating significant investment to GDPR/CCPA initiatives. Reuse is envisioned within a customer's brand ecosystem where a user can be issued a unique ID that is portable between brands, and is positively identified during authentication by device, location, and behavior. Although the identity itself is verified in real time at each authentication, it offers a compelling model for a secure, trustable ID in different contexts.

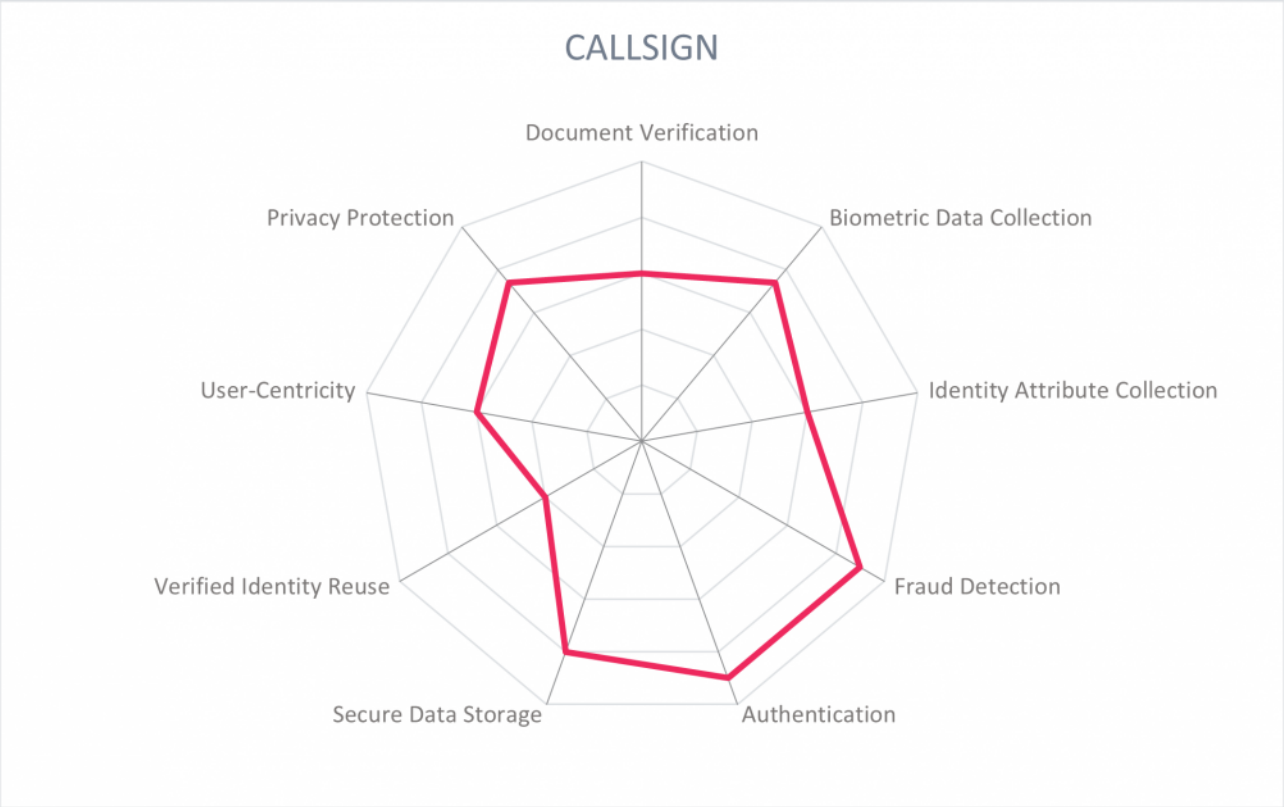
Security	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○
Market Standing	●●●○○

Strengths

- Strong dynamic authentication and fraud prevention solution, supported by identity verification
- Positive identification is achieved through behavioral factors as well as typical document/biometric checks
- Comprehensive REST APIs
- Has a strong privacy focus
- Flexible and easy to configure customer journeys

Challenges

- Identity verification is actively conducted at every authentication, support for verified identity reuse could still be developed
- Could develop more user-centric portability of identity
- Support for FIDO Alliance standards is on the way, due in 2021


CALLSIGN
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.4 Consensys Mesh

The Identity Team at Consensys Mesh was born from the combination of Consensys' uPort, Civil, and Alpine projects to develop open-source decentralized identity solutions. This network of developers, researchers, founders, and investors is contributing to Veramo, among other projects. Veramo is an open-source JavaScript Framework to handle Verifiable Credentials in apps, with the goal of enabling developers to build better trust layers. As an open-source product Veramo is available globally, though more accessible for the English-speaking world.

The Veramo framework enables apps to create and resolve identifiers, issue and revoke credentials, and exchange credentials. The Veramo core is based on ECMAScript and runs natively in the browser with browser-compatible plugins, as well as in hosted server-side applications. Plugins exist for various DID methods, messaging protocols, storage, key management, authentication, etc. The agent orchestrates all plugins and exposes interfaces programmatically and via REST and OpenAPI. The framework offers modules that implement decentralized protocols based on Ethereum. Biometric information can be ingested and processed as Verifiable Credentials.

Veramo is designed with a modular architecture that is very accessible to developers and system integrators and supports various deployments scenarios, e.g., multi-tenancy. Support for additional DID methods, communication protocols, credential formats, and proofing algorithms is in development. The decision to pursue an open-source project instead of a product is based on perceiving identity being a basic necessity, like water. Creating a trustable messaging protocol to exchange verified identity enables use cases for every industry including government, gaming, banking, supply chain, and much more.

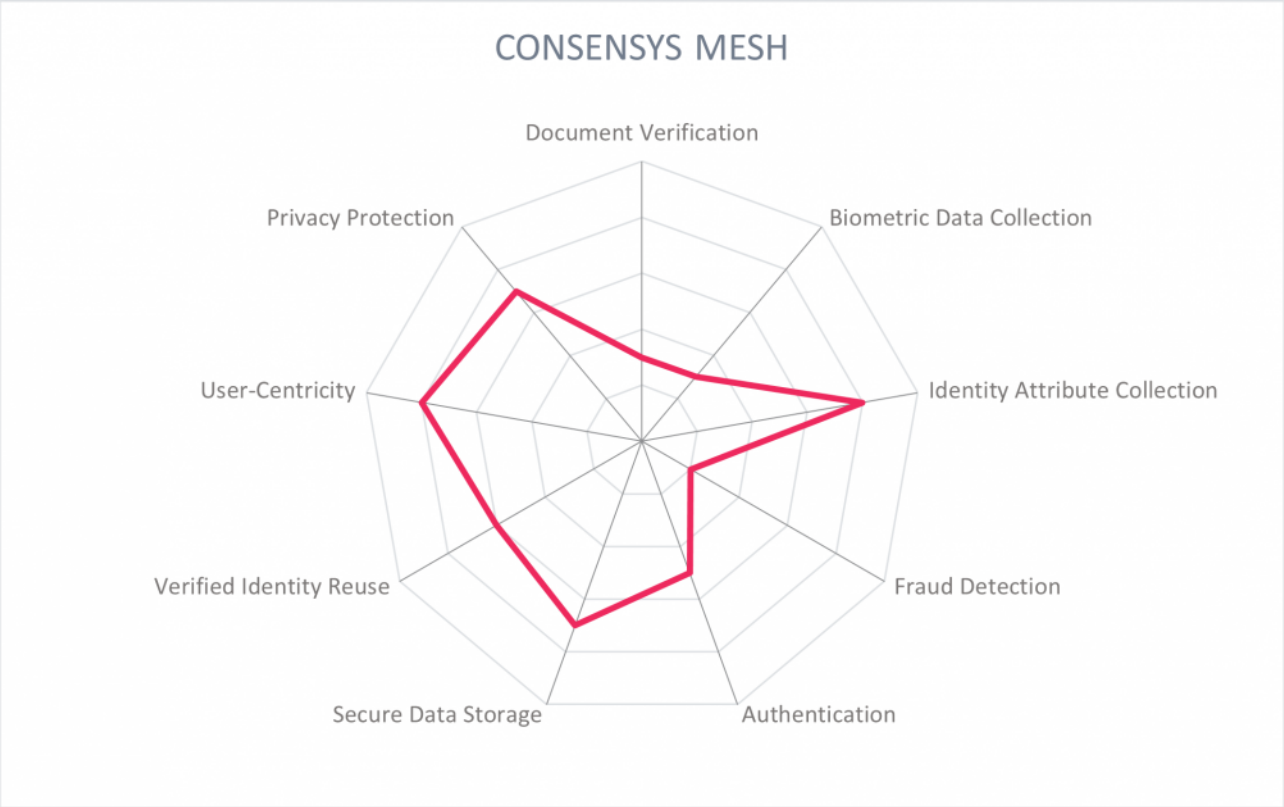
Security	●●●●○
Interoperability	●●●●○
Usability	●●●○○
Deployment	●●○○○
Market Standing	●●○○○

Strengths

- Open-source project, with collaboration with W3C and DIF for high compatibility
- Follows decentralized identity standards
- Public documentation available
- Ambitious project to enable decentralized verifiable credential usage anywhere, with strong support for reuse across ecosystems

Challenges

- Requires developer expertise for implementation
- In public beta, with more development on the roadmap
- CLI tool only supported on Mac and Linux systems, with Windows support on the roadmap
- No document check capability
- Biometric capabilities possible with bootstrapping


CONSENSYS MESH
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.5 esatus

Founded 1999 in Langen, Germany, esatus provides an enterprise IAM suite based on decentralized identity. Its product, SeLF, has an architecture that enables an org to be their own IdP for use anywhere. SeLF sits between the decentralized layer and an organization and builds the connection to typical standards for authentication and authorization, and uses attested facts about a user for authentication. Its geographical focus is primarily the DACH region, but the product is globally applicable with language support for English, German and Spanish.

The solution fully embraces the principles of Self-Sovereign Identity (SSI), enabling the end user to have their personal information held in a wallet app on their mobile device. For a new employee onboarding use case, an HR member inputs the new employee's user ID, email, and name. The new employee receives an email with an invitation to scan a QR code with their wallet app. With the user's approval, the employer's system connects to wallet app and issues the relevant employment credentials with attributes such as organization, group, department, location, etc. These credentials are stored in the user's wallet and can be managed in the employer's backend system with revocation option. In an authentication scenario, a user would scan a QR code and be requested to share relevant attributes from credentials to gain access, for example being an employee at X company in Y location. The user accepts sharing the requested information, the application checks the validity of the credential, and access is granted. To reflect the multidimensional responsibilities that individuals carry in enterprise settings, one user can hold different roles – such as executive, sales or HR manager, software developer or application owner – depending on the authenticated resource and context.

SeLF offers a fact-based identity management process, removing provisioning, request and approval processes. SeLF can be identified as an IdP with existing directory services, with SAML, LDAP, AD, Azure AD, OAuth2, and OpenID Connect. The decentralized layer is built on Hyperledger Indy technology and thus is compatible with networks such as Sovrin and IDunion. Additionally, the Hyperledger Aries compliant wallet app is multi-ledger compatible, enabling SeLF to interact with other decentralized identity providers and ecosystems. No personal data is stored on the blockchain, only verifiable proofs that an identity credential is valid. Although SeLF does not directly provide identity verification, it is an important architectural step to bring verified reusable identities for use in the workplace. Although SeLF does not aim to provide identity verification services, it is a horizontal IAM component that is active in projects like IDunion to enable compatibility with and sharing of eIDs according to eIDAS. With its strong background in IAM, esatus applies SSI principles to this domain and is applicable to a variety of use cases requiring secure data exchange.

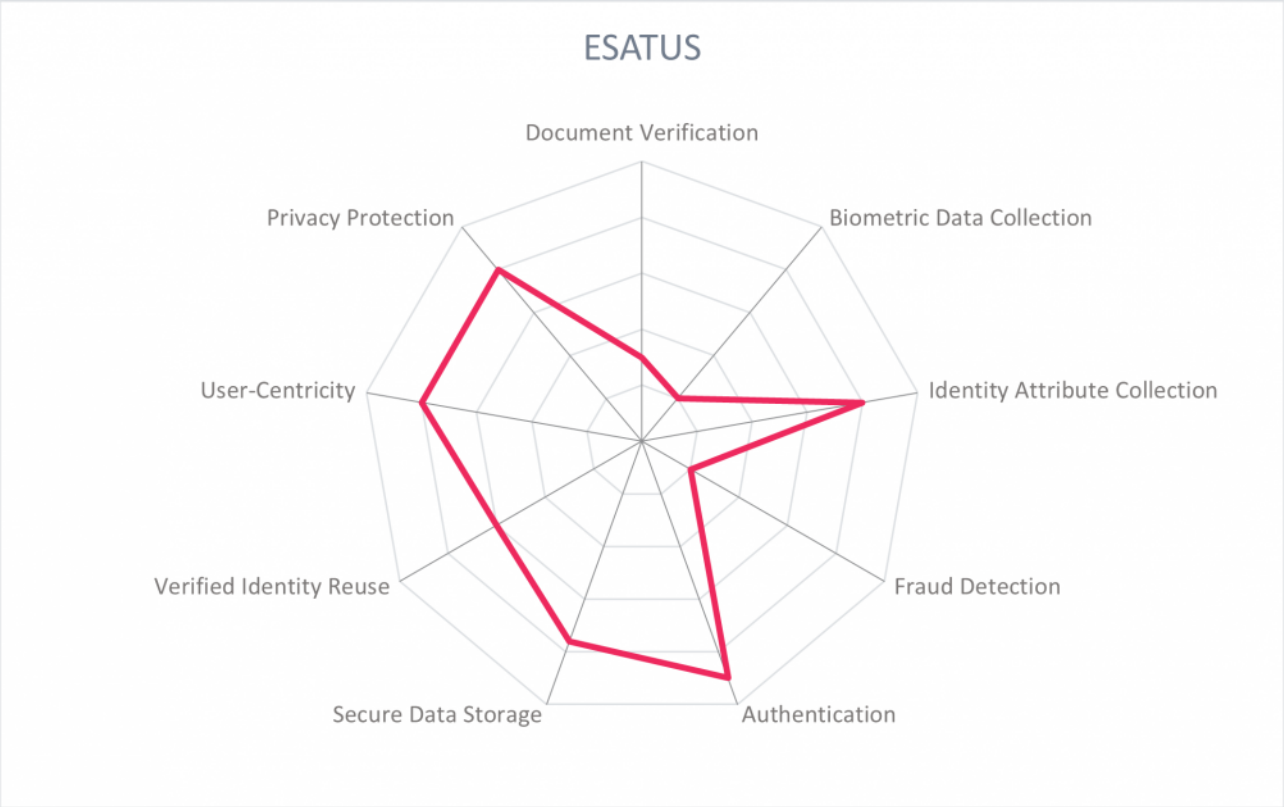
Security	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●●
Market Standing	●●●○○

Strengths

- Modern modular architecture with all components called by API
- Well thought out for enterprise use cases
- MyData Operator status for privacy-forward personal data management
- Wallet app is available in iOS and Android devices.
- Compatible with every Hyperledger Indy network (including Sovrin, IDunion) and supports multi-ledger wallets
- Wallet has backup functionality
- Is GDPR compliant with security and privacy by design principles

Challenges

- Small company but attracting investment for its decentralized solutions
- Requires the user to have a smart mobile device with camera functionalities
- Does not specifically address KYC and high LoA use cases
- No additional fraud detection features


ESATUS
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.6 Evernym

Evernym was founded in 2013 in Salt Lake City, UT, USA. It is a blockchain-based solution that enables organizations to issue and request Verifiable Credentials. Verity may be optionally used with the Connect.Me wallet app for from Evernym for credential storage and sharing, or with a range of other decentralized wallet apps. Evernym is active in North America, the UK, and is expanding into Western Europe.

Verity is managed via a webapp where the customer can configure its issuer settings, define schemas and credentials, issue credentials, request proofs, etc. The customer triggers a credential issuance to an end user via a QR code received via email, SMS, etc. The end user scans the code with Connect.Me or other wallet app. The customer then issues the appropriate credential, for example a DMV issues drivers' license number, a hospital issues health records, etc. When credentials are shared, privacy is ensured by sharing a proof that the credential is true, rather than the credential itself. Several relevant deployments indicate the range of use cases possible: A 2019 pilot project successfully enabled users to onboard their government-issued ID and biometric information as a verifiable credential using Onfido, a digital staff passport for a large health provider is live in over 70 hospitals, call center and contactless in-branch authentication is being used for financial services customers, and an airline industry solution for verifying travel documents and additional health documents is rolling out in March 2021. Identity Assurance Level 3 can be achieved. This enables verified identity reuse in Evernym's ecosystems and will be scaled to production-level in the near future.

The solution is built on Sovrin, a public network operated by the non-profit Sovrin Foundation's permissioned nodes, but is designed to be a general-purpose protocol engine to work easily with other decentralized systems. It uses its own Plenum consensus protocol, a modified RBFT protocol. It handles the scalability of high volume read requests of identity systems by differentiating between observer nodes and validator nodes that process write requests. The identities created are portable and independent of a service provider's system or database. Identity data is stored on the user's own device. No individual identifiers are stored on a public ledger; the ledger is a decentralized key store for issuing organizations to be publicly proven as a trustworthy credential issuer. Deployment is in the cloud, with options for private cloud deployment.

Security	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Market Standing	● ● ● ○ ○

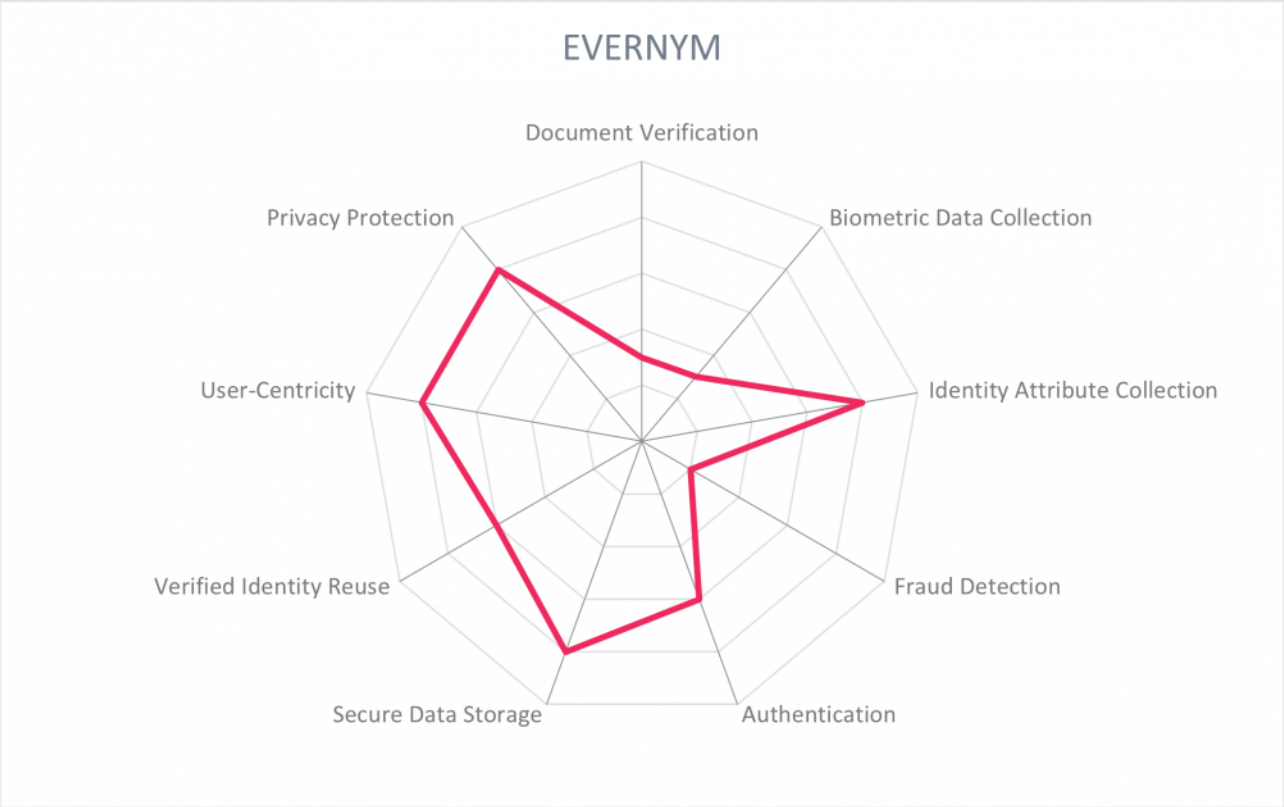
evernym

Strengths

- Supports and transacts with many types of identity credentials
- Is part of the Sovrin Network with access to global partners and participates in forming global standards like DID, W3C, Trust Over IP
- Compelling PoCs with Mastercard, NHS
- Data encrypted at rest and in transit
- Cloud backup to synchronized devices

Challenges

- Moving towards synchronized wallet apps for identity reuse in wider contexts
- Credential revocations on the roadmap for early 2021
- No eID integration yet, but on the roadmap and offers an avenue for eIDAS issuers to deliver IDs with verifiable credentials
- Document and biometric checks not a permanent part of product yet, but partnerships from successful POC exist


EVERNYM
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.7 Experian

Experian was founded in 1996, and is based in Dublin, Ireland. Its product, CrossCore, is a fraud detection and identity verification platform for new account originations, low and high-value transactions (both monetary and non-monetary events) and account management. CrossCore provides the confidence to trust incoming identity attributes from other providers for a variety of use cases and across industries by leveraging its multi-regional bureau-based authenticated identity assets in products – PreciseID in North America, ID Authenticate in the UK, ProveID in EMEA – along with its proprietary device intelligence and additional partner data and insights. Experian's geographical reach enables ID verification globally.

CrossCore used for identity verification analyzes user data during input, generates a fraud risk score, assesses KYC and CIP risk for compliance, and yields a decision to accept or to require additional verification. The user inputs their data for onboarding or application screening, and if required, may also prompt a scan of government-issued ID and a selfie for liveness detection, which is scored by a collection of first-party and third-party fraud and verification applications. Fraud detection includes account compromise confidence scores, credit reporting, detection of synthetic identities, behavioral biometrics, device and context intelligence, and consistency of identity elements in transactions. This process is supported by its growing database of over 1 Billion authenticated identity data assets. The user is then segmented into an appropriate risk group for either successful acceptance or an additional step-up verification before acceptance. This solution follows NIST 800-63-3 for Levels of Assurance, able to dial the level up or down based on the use case.

CrossCore is a SaaS platform. Data storage is compliant with the requirements of financial and government regulated industries, thus the system is configurable to meet the data storage needs of the customer. Experian supports the range of traditional remote and digital verification procedures for both low and high value transactions, including call center verification with knowledge-based questions.

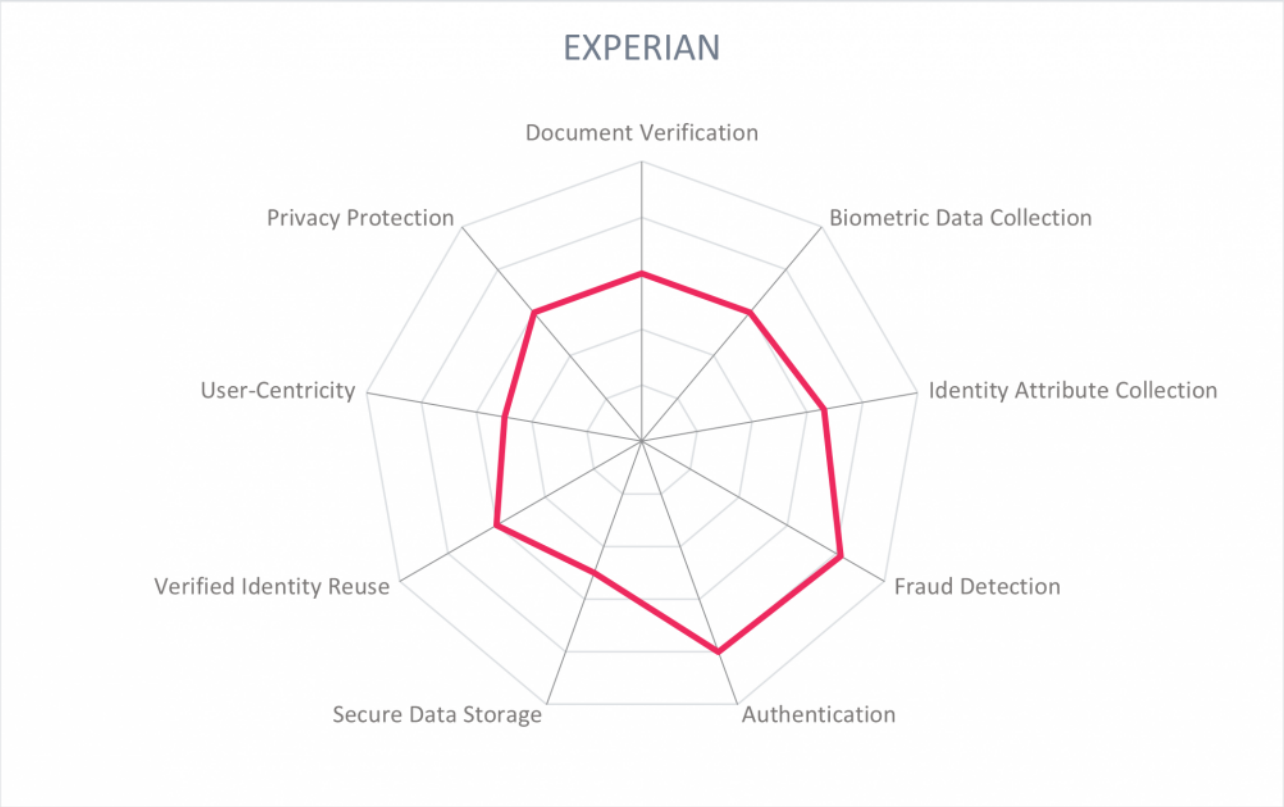
Security	●●●●●
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●●
Market Standing	●●●●●

Strengths

- Established market player in identity verification
- Extensive partner network for global coverage
- Strong fraud detection capabilities
- API-forward architecture
- Decisioning and analytics strengthened with Machine Learning

Challenges

- Has not fully embraced verified identity reuse, limited ability to save and reuse verified identities
- Document and biometric checks offered by third party partners
- A secure but less user-centric approach to data storage


EXPERIAN
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.8 Jumio

Jumio is based in Palo Alto, California but with Austrian roots. Founded in 2010, Jumio's KYX Platform provides enterprises with the means to do KYC checks for individuals, organizations, employees, etc. The KYX Platform can integrate KYC checks and identity verification into onboarding processes, ranging from a fully automated solution for identity verification, a hybrid solution composed of both AI and manual review when needed. Jumio has customers in 200 countries and territories, with coverage of over 3,500 ID document types.

During an onboarding process, the user is prompted to take a photo of their government-issued ID with their smartphone with the associated app or webcam. Jumio extracts and processes the document information supported by its Machine Learning components and checks the information against authoritative sources. Included are spoofing checks, 1:n checks against a blacklist of fraudulent faces, visual detections of document security features, anomaly detections, etc. Secondary documents such as utility bills or bank statements can be captured with a smartphone for address verification. The user then takes a selfie for biometric cross checks with the photo ID, and a liveness detection. Confidence levels are calculated for each verification step and used to yield a decision. Video identity verification is also available to fulfill the highest KYC and Identity Assurance Level 3, with customizable workflows to fulfil the LoA required by the customer.

Jumio operates in AWS private clouds, deleting identity data immediately after transactions have concluded. Jumio hosts only at the customer's request. Jumio supports onboarding and KYC processes on mobile devices and computer web browsers. APIs are available. Compliance capabilities also include AML screening on PEPs and sanctions, and transaction monitoring on suspicious activity, case management and more. Jumio does not yet have a reusable product but is currently working with multiple digital identity wallet providers to enable a reusable digital identity.

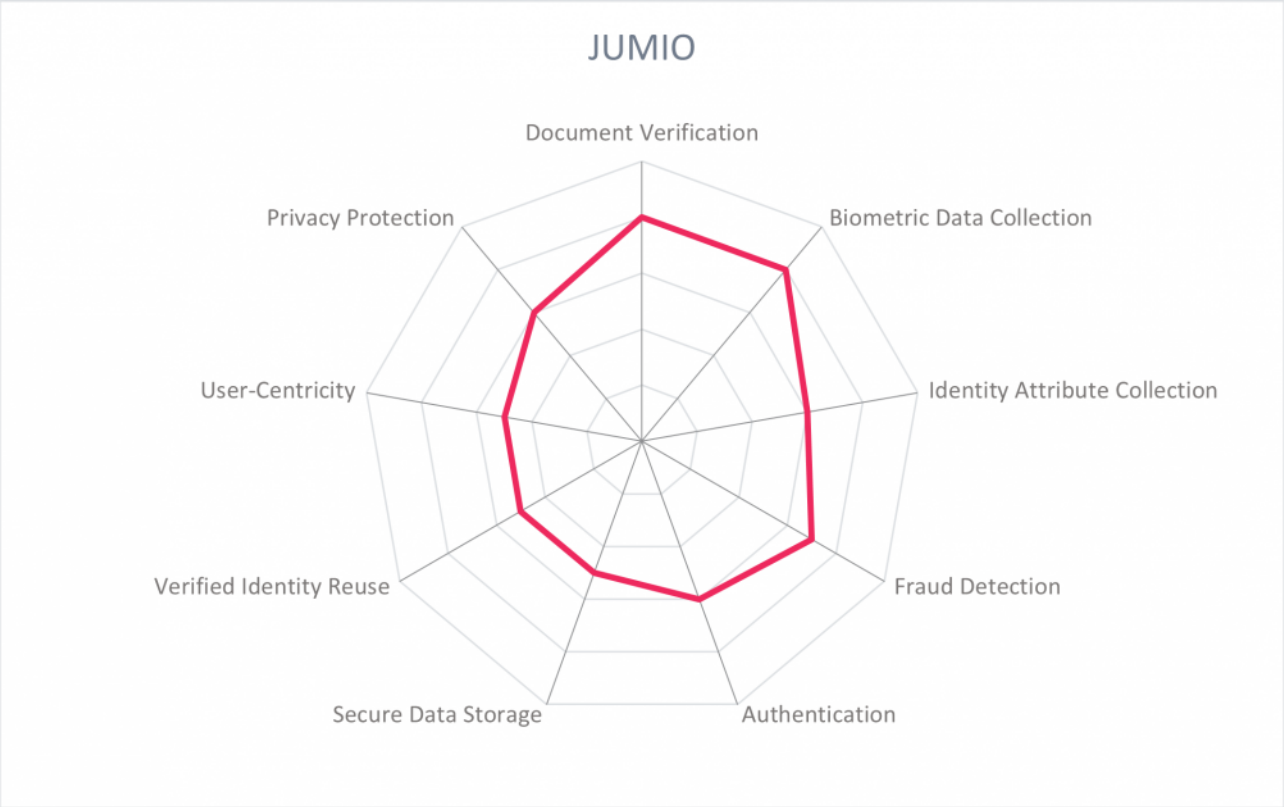
Security	●●●●●
Interoperability	●●●○○
Usability	●●●●●
Deployment	●●●●●
Market Standing	●●●●●

Strengths

- Strong presence in the identity verification market
- Global coverage
- Does support video identification processes, clearly meeting LoA3 requirements
- Offers real time feedback to users on how to successfully complete a verification
- PCI DSS compliant, ISO 27001 certified
- Compiled the largest identity dataset after Interpol for fraud checks

Challenges

- Does not have a reusable product but has projects in the pipeline
- Does not integrate with standard authentication sources like SAML, OpenID Connect
- Could work for more user-centricity in identity collection and storage


JUMIO
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.9 KYC-Chain

KYC-Chain was founded in 2015 as a compliance dashboard and customer on-boarding portal for KYC and identity verification, designed to create efficiencies for financial institutions and regulated entities. KYC-Chain founded the SelfKey Foundation to manage an open-source digital identity wallet to enable identity owners to reuse their verified identities in different KYC processes. Its open-source decentralized wallet is for both individuals and corporations, and its blockchain network enables KYC-Chain's KYC/AML compliance solution. KYC-Chain works to serve global customers, with coverage of 4000 document types from over 240 countries and territories.

The Self-Key wallet is a 'plug & play' option for KYC-Chain, though it can optionally receive data from other wallets. A user downloads the SelfKey wallet as a desktop or mobile app. The user views the marketplace of services, including opening a bank account with partner banks, incorporating a company, and receiving notary services. For each desired service, the user is able to see what the KYC requirements are and can onboard the appropriate identity and other documentation into the wallet. At the point of registering for a marketplace service, the Self-Key wallet sends information directly to the relying party and can automate the process such as auto-filling the registration forms. The KYC-Chain backend for customer enables the customer to monitor applicants to a KYC process, the results of authenticity checks and verifications against authoritative sources and checks against AML sanctions lists. In case of crypto assets, wallet screenings can monitor the full financial history of that wallet. Corporate wallets can be used to enable KYB checks. The relying party's compliance officer makes any approval or denial decisions.

KYC-Chain can be implemented as a stand-alone SaaS, and SelfKey transacts on the Ethereum public blockchain. APIs are provided for company registration per jurisdiction checks. SelfKey uses identity fragmentation to enable selective attribute sharing. A hash of the transaction identifiers is stored on the blockchain. The signing mechanism works via a Javascript Object Signing and Encryption (JOSE) Javascript web token (JWT) as an authentication methodology. Currently, SelfKey is implementing an open-source SSI toolkit designed for full interoperability and compliance with the W3C DID and credential standards.

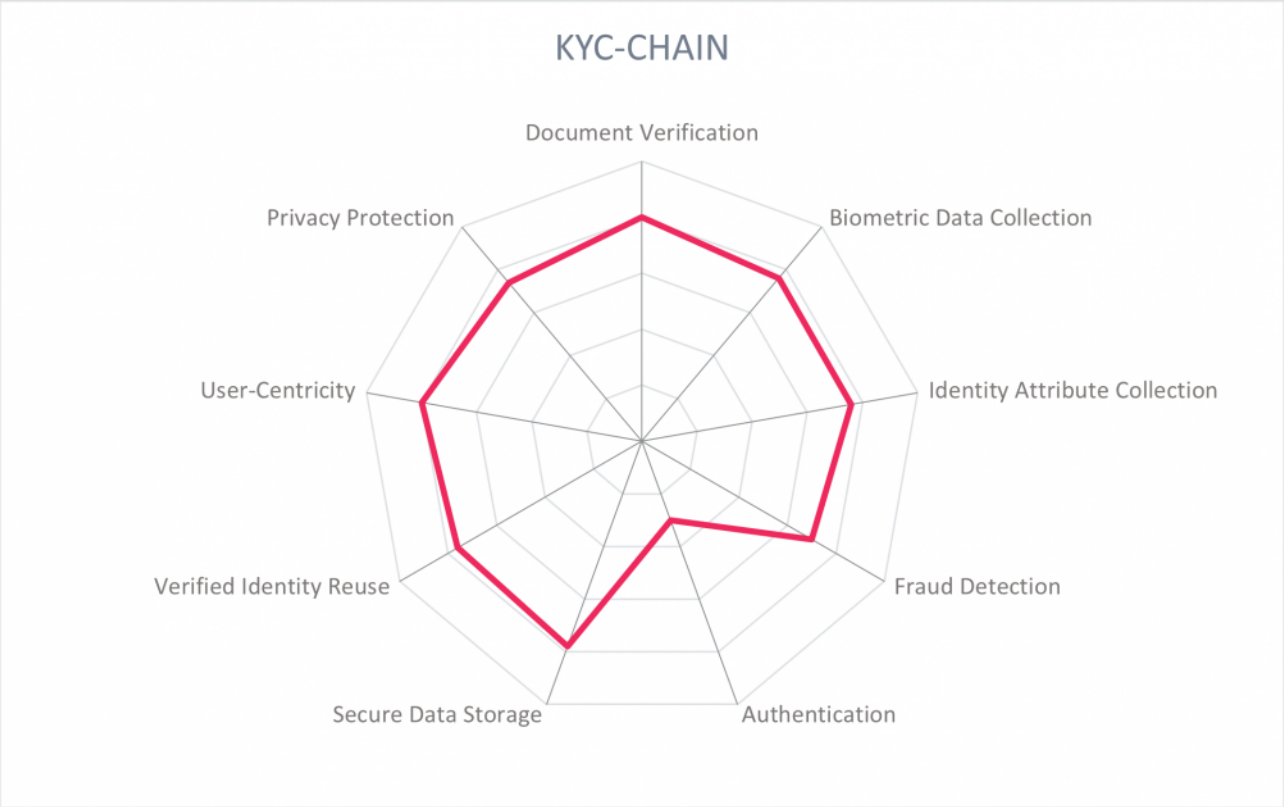
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Market Standing	● ● ● ○ ○

Strengths

- Device recovery is possible
- Wallet and onboarding process possible for individuals and corporations
- Provisions for FAFT travel rule and crypto assets
- Promising applications for self-serve KYC processes
- User app available on iOS and Android

Challenges

- Authentication is currently available using an Ethereum private key, with authentication through W3C protocols on the roadmap.
- Will eventually face scalability issues, recommended to consider sidechain or other decentralized ledgers
- Lacking a strong go-to-market strategy


KYC-CHAIN
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.10 Microsoft

Microsoft, founded in 1975 and based in Redmond, USA, is a familiar figure in hardware and software, digital services, and cloud infrastructure businesses. In spring 2021, it releases its Azure Active Directory Verifiable Credentials product to enable peer-to-peer, B2C, and B2B verified credential issue, storage, and exchange for several reusable use cases. Through its contributions to open-source Decentralized Identifier (DID) and Verifiable Credential (VC) technologies, and efforts to drive interoperability standards in collaboration with DIF and W3C, Microsoft attempts to enable reusable verified identity for use in directory services for remote onboarding, authentication, and user-centric management of identity attributes. Microsoft is a key player in this market and serves customers globally.

Microsoft enables an organization to issue verifiable credentials from its identity provider, compatible with OpenID Connect. In a remote onboarding use case, an organization using Azure AD specifies which ID proofing service they will use, and which identity attributes should be verified. The result of the ID proofing flow is the issuance of a Verifiable Credential to the user, employee, or partner. Using the open-source Verifiable Credentials SDK from Microsoft, the VC issuer service is federated with the organization's IdP using OpenID Connect, allowing the organization to populate VCs with relevant identity claims and issue them to both internal and external parties. Before a VC can be issued, the VC issuer federates to the organization's IdP to authenticate the user, establish a per-organization identifier, and process the identity attributes to be included in the VC. The enterprise manages access rights from the Azure AD-integrated Verifiable Credential service. The organization has the ability to define the identity attributes required for an interaction – such as authentication – and integration with services such as Experian and Jumio allow for organizations to generate VCs that are level 3 LoA compliant.

Onboarding an employee with VCs eliminates provisioning a username/password but allows employee to reuse the VC for verification of identity attributes in other flows, via the Microsoft Authenticator app. DIDs are anchored in ION, an open, public, permissionless Layer 2 Decentralized Identifier network. Identity data is stored encrypted on the user's device and is only disclosed for verification by others when the user chooses to do so.

Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●
Market Standing	●●●●●

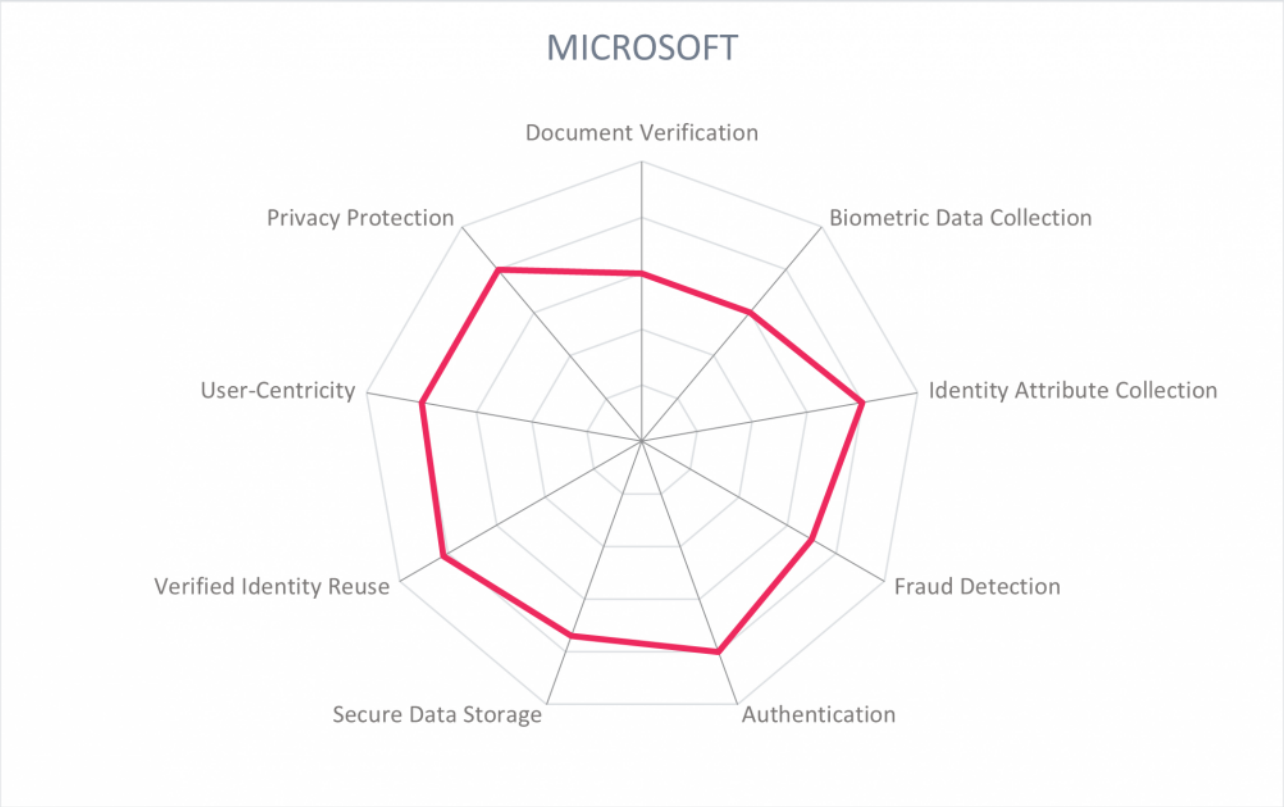
Microsoft

Strengths

- A strong market player with path to attaining critical mass of users
- Close collaboration with DIF and W3C to establish standards
- Open-sourced the Verifiable Credential SDK for open access to and innovation in secure digital identity exchange
- Participates in DIDComm emerging standard for mutual authentication between peers
- Recovery of data possible with mnemonic phrase
- Emphasis on ability to resolve Verifiable Credentials from other issuers
- Revocation of credentials is possible

Challenges

- In public preview, still gaining traction
- Demonstration of strong interoperability and usability must be seen beyond its public preview
- Focus is on OpenID Connect, future support for other standard authentication sources is recommended
- Proposes an ambitious and disruptive approach to onboarding, shifting from signup/sign in to present and verify


MICROSOFT
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.11 Octopus

Octopus was founded in 2017 is based in London, UK. It provides a self-sovereign solution allowing organizations and individuals to authorize, authenticate, and verify reusable identities in real time. Octopus's current customer base is focused on the UK and Western Europe.

Peer-to-peer sharing of verified documents and individual identity attributes is possible. Individual users, known as identity owners, access Octopus via responsive mobile site or a mobile app. They create a personal identity hub, first securing passwords and backup keys then building multiple Personas® allowing the sharing of identity for different types of relationships, for example personal, medical, and professional. Identity Artefacts® are generated by an authorized identity provider, either by self-scanning an ID document or through an existing authentication scheme. Once created, the Artefact® tracks all entities that it has been shared with on a field level, with the possibility to revoke. Organizations can biometrically verify users, leverage 3rd party attestations, or use a collective conferred trust score. The document and biometric checks are powered by Hive ID. Octopus' proprietary AI intelligent agents provide user behavior insight and threat detection. Identity Assurance Level 3 can be achieved.

The solution offers offline, out-of-band, and international authentication. Enterprise usage of Octopus is supported with 3rd party APIs with the benefit of pushing customer data to the edge, and query without decrypting it for strong privacy protection and without leaking metadata. VaultChain® graph platform secures identity privacy by distributing cryptographically-proven, hashed Artefacts® across millions of anonymous encrypted vaults. A new data vault is created for each new relationship. Following SSI principles, users can choose where their data is stored, with options ranging from Dropbox to IPFS to the Octopus Cloud.

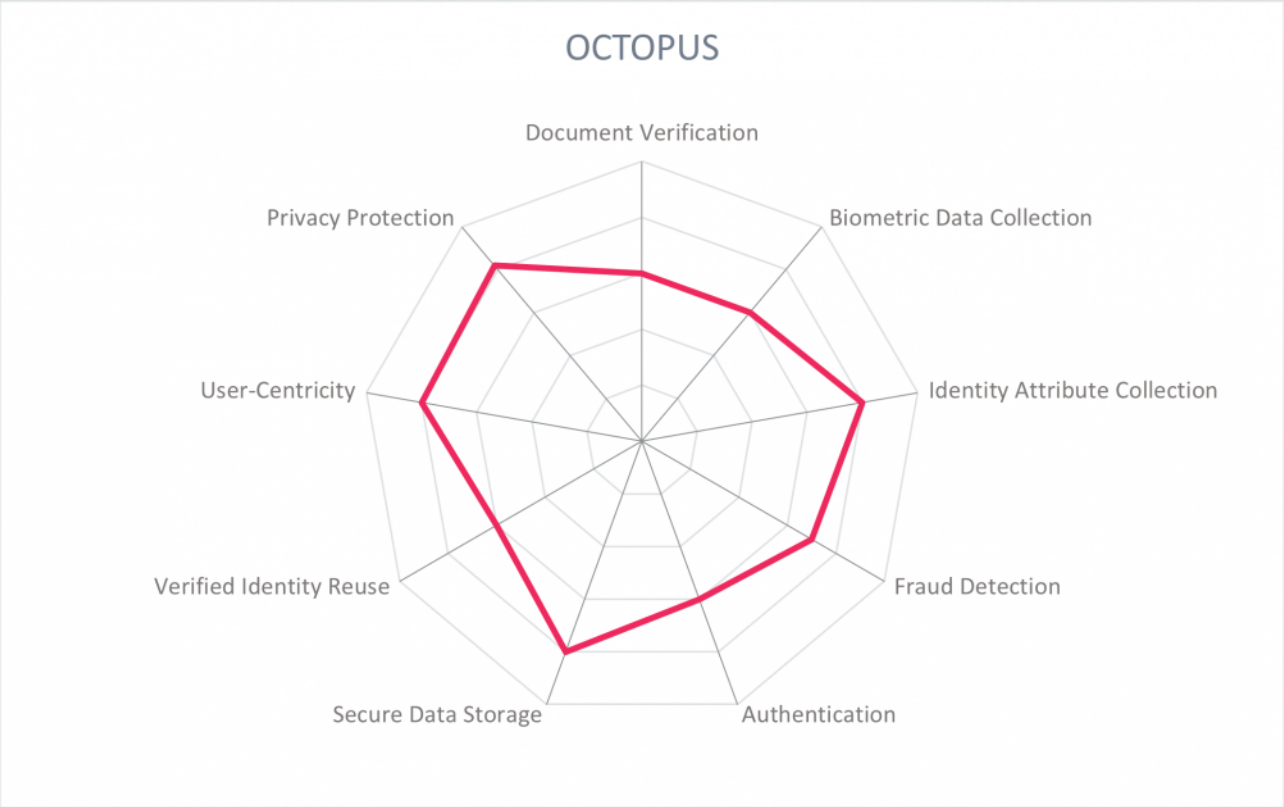
Security	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○
Market Standing	●●●○○

Strengths

- Operates with decentralized ID standards like DID
- Uses DAG with potential for higher scalability that blockchain solutions
- APIs and SDKs are available
- Makes steps towards a privacy and user-centric life management platform
- Selective attribute sharing is supported with zero knowledge proofs
- App can be white labelled
- Strong go-to-market model with retail and financial services partners bringing them to users

Challenges

- Does not use the Verifiable Credentials emerging standard for identity attribute sharing
- App is not yet functional on all devices
- New start-up with limited reach and resources
- Solution requires the user to have a smart phone
- Faces the challenge of gathering a critical mass of users


OCTOPUS
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.12 Onfido

Founded in 2012, Onfido is based in London UK. It provides hybrid and fully automated identification solutions, supported by its proprietary AI to detect fraud signals. Onfido can process over 4,600 identity documents types from over 195 countries and is a strong player in the identity verification market.

Onfido's Identity Verification typically supports customer onboarding processes. At the onset of an onboarding process, a user is prompted to scan an identity document with their mobile device. Five categories of Machine Learning algorithms are deployed for fraud detection for document OCR, document liveness, image quality enhancement, a generalized fraud model, and liveness detection, achieved passively through selfie biometric verification, or actively through video biometric verification yielding a risk score for each. Sign up forms are auto filled from the ID document. Biometric data is collected with a selfie or selfie video for facial matching, liveness detection, texture analysis, etc. Options for biometric authentication exist, linking the biometric authenticator to a verified identity for additional security. Identity Assurance Level 3 can be achieved for high value transactions and upgrading a digital identity for KYC. Verified identities are at this point single use only, with plans on the roadmap to add portable and reusable capabilities.

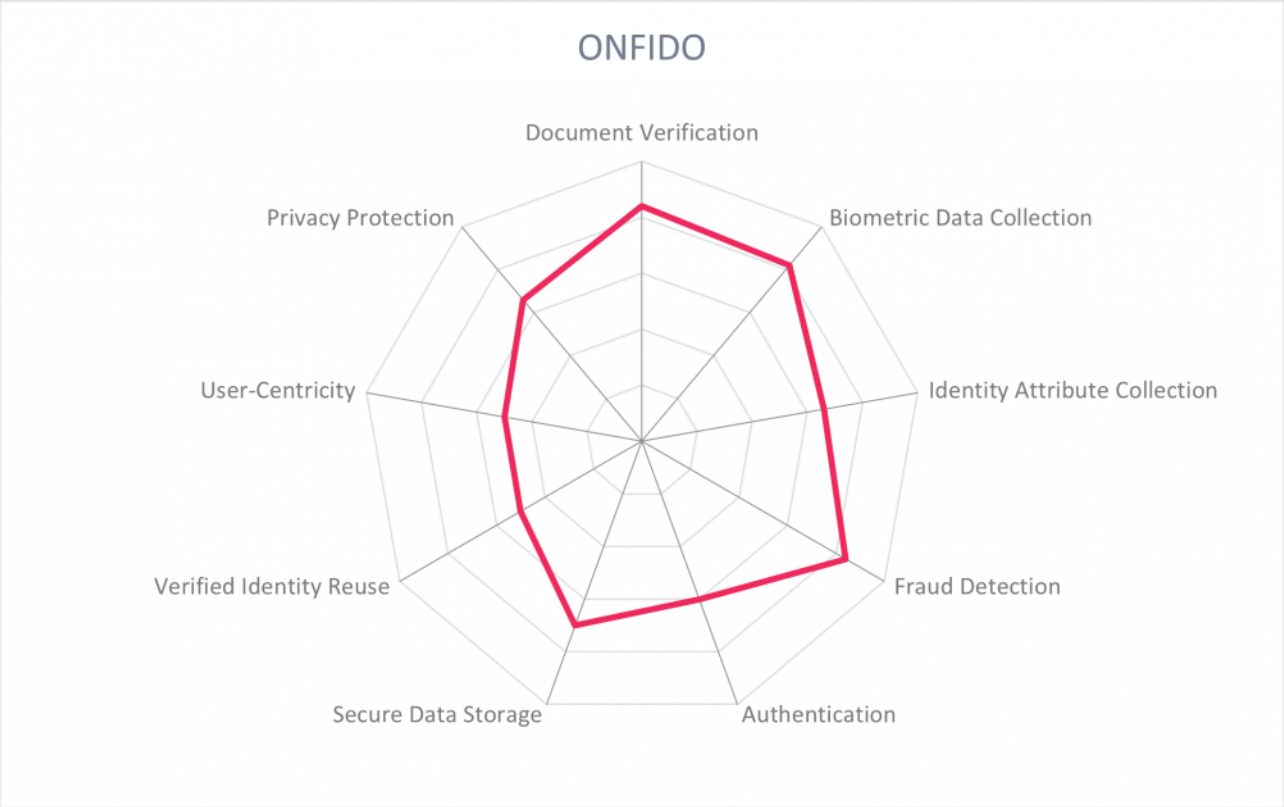
Onfido is a cloud service, exposed with REST APIs for backend integrations. SDKs are available for web, tablet, and mobile, both iOS and Android. Enterprises can determine whether their data is processed and immediately deleted, or stored by Onfido in AWS for future ML training. Onfido has worked with the UK's ICO to establish governance practices and compliant handling of training data.

Strengths

- Certified ISO 27001 and SOC 2 Type II compliant
- Accessibility SDKs and considerations for users with disabilities
- Strong go-to-market model using a partner ecosystem to introduce them to a specified geography or market
- Worked with the ICO in its Regulatory Sandbox on compliant handling of training data
- Cross-checks documents against proprietary compromised document database
- Onfido technology is integrated in many other identity verification solutions

Challenges

- Has a conservative approach to verified identity reuse, with experimentation planned in 2021
- Integrations with standard authentication sources like OpenID Connect or SAML will improve this solution


ONFIDO
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.13 Oxyliom Solutions

Oxyliom Solutions was founded in 2012 and is headquartered in Luxembourg with offices in Casablanca and Dubai. Its product, the GAiA trust Platform, supports onboarding, authentication and lifecycle management. Its digital trust services include key management, electronic signatures, and document signing. Oxyliom Solutions has implemented 8,800 document templates from 245 countries in 88 languages, and serves the African and EMEA regions.

The GAiA Trust Platform is used to support onboarding, often for financial services. Onboarding may be facilitated with face-to-face identity verification and video verification. A user may open an account with face-to-face verification to achieve Identity Assurance Level 3, then verify contact methods and generate a private key-based digital identity for later reuse. The private key is stored on the user's mobile device. This process may be reversed, onboarding a user with a low level of assurance first, then upgrade the assurance level later with digital document verification, scanned by the user's mobile device. Video verification may be entirely browser-based, without requiring the user to download an app. Face matching is completed between the photo ID and the individual completing the video verification process (as 1:1 or 1:n), accompanied by spoofing detection and fraud checks. Verification of a Permanent Account Number (PAN) can be done in real time. Biometric capabilities are provided by Oxyliom, using a selfie video to face match the identity document that was onboarded. Reuse is possible with partners within an organization's ecosystem, for example across all branches of a bank and with partner insurance companies. Authentication with verified biometrics is possible.

GAiA is a cloud native, microservices-based platform. APIs are available for all features on the platform, for which Machine Learning is used to support security. Customers can use HSM to secure encrypted access tokens, data, and keys, or use cloud storage. Connectors to various eID programs and federation systems such as France Connect, eID Luxtrust, eHerkenning, and BankID enable verified reuse of these identities in the GAiA Trust Platform. Verified identity for authentication can be upscaled with connectors to other tools to integrate contextual authentication. Connectors exist for Microsoft, Nexus, social logins, SAML, OpenID Connect, FIDO and OAuth2.

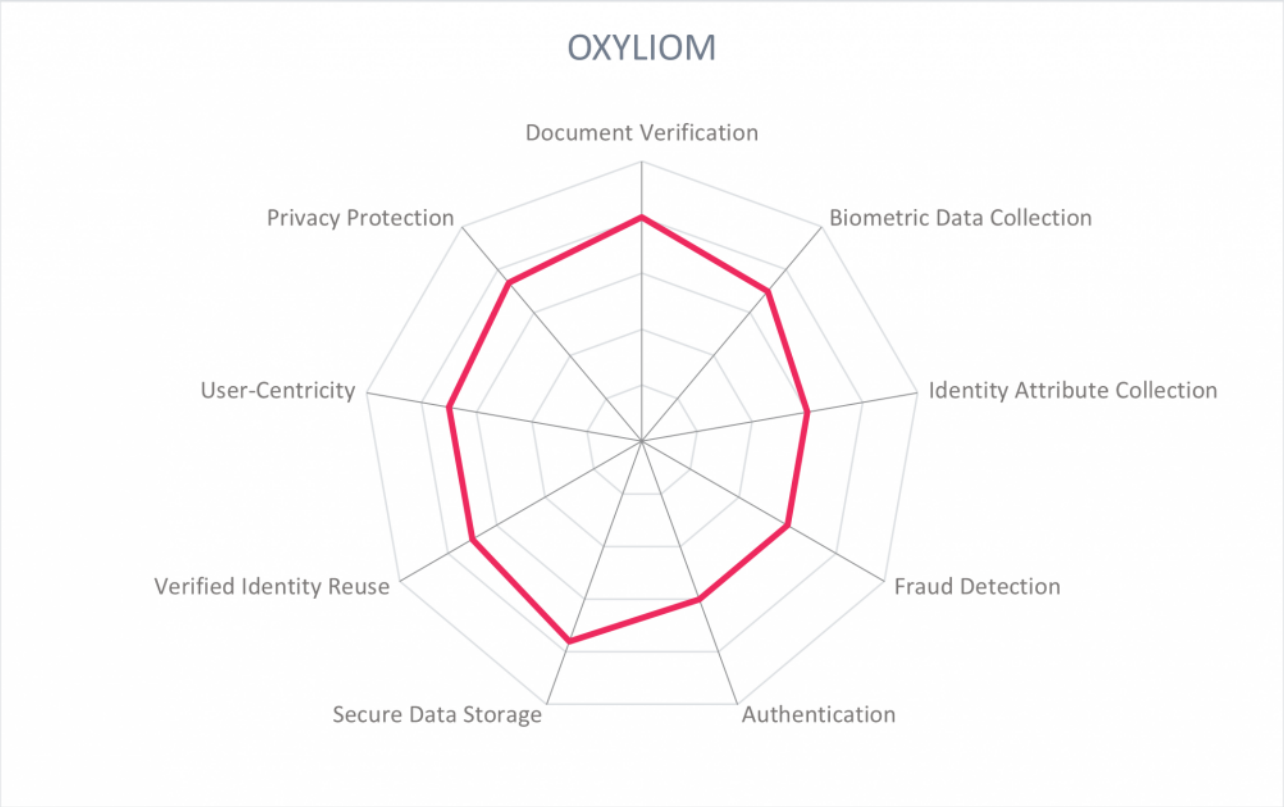
Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●
Market Standing	●●●○○

Strengths

- API-driven approach
- Additional capabilities include document signing and electronic signatures
- Possible to onboard users with eIDs.
- Data is encrypted in transit and at rest
- Connectors to OpenID Connect, SAML, Microsoft, Nexus, and others
- Machine Learning for fraud detection and API security monitoring is built-in

Challenges

- Customer manages storage of user data
- Start-up with a small but growing customer base, support ecosystem, and technology partners


OXYLIOM
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.14 Ping Identity

Ping Identity was founded in 2002 and based in Denver, Colorado. It specializes in solutions for IAM and CIAM, and with the acquisition of ShoCard in 2020 can integrate decentralized identity solutions into their technology stack. With the integration of ShoCard technology, Ping can provide CIAM solutions that enable identity verification as part of the identity management ecosystem. Ping serves clients globally and is one of the main players in the identity market. Identity documents that are accepted include driver's licenses, government ID cards, and processes unknown identity documents with OCR and photo of the user. PingOneVerify enables a user to be verified with liveness detection and scan of an identity document using the Ping or ShoCard mobile device app, during an onboarding process or later in the lifecycle for KYC or as needed by the customer. Biometric info and ID documents are compared, along with other parameters to positively identify the user and issue a Verifiable Credential. Reuse is possible with between Ping customers, for example when a user has already verified their identity with Verifiable Credentials stored on the mobile device. This user can sign up for a new service by scanning a QR code which triggers the ShoCard or PingOneVerify app to select appropriate credentials to share. The user chooses the credentials they wish to use to onboard, and the new service's registration form is auto-populated. In this process, it is not necessary to create a username or password, and authentication is supported by a biometric factor that is associated with the verified identity and/or signing a challenge request sent to the user's phone, integrated with Ping's CIAM platform. The verified identity can be used in step-up authentication. Identity attributes can be shared selectively by exchanging a signed and hashed proof that the attribute is verified.

PingOneVerify is a SaaS service, integrated into Ping's identity platform backend. Account and password recovery are possible. Verified identity attributes are stored salted and hashed on the user's device or in a personal cloud, along with the associated private keys. A blockchain-agnostic sidechain to Ethereum is used to facilitate credential issuance and validation, with plans to move to other public blockchains such as Hedera. While the identity is being verified, the data passes through Ping servers, to third-party services, and returns to the mobile device. The user PII data is then deleted from all Ping as well as third-party servers. For banking transactions, banks maintain the data while the user still controls the private key. The identity data remains with the user stored on their device until they choose to share it.

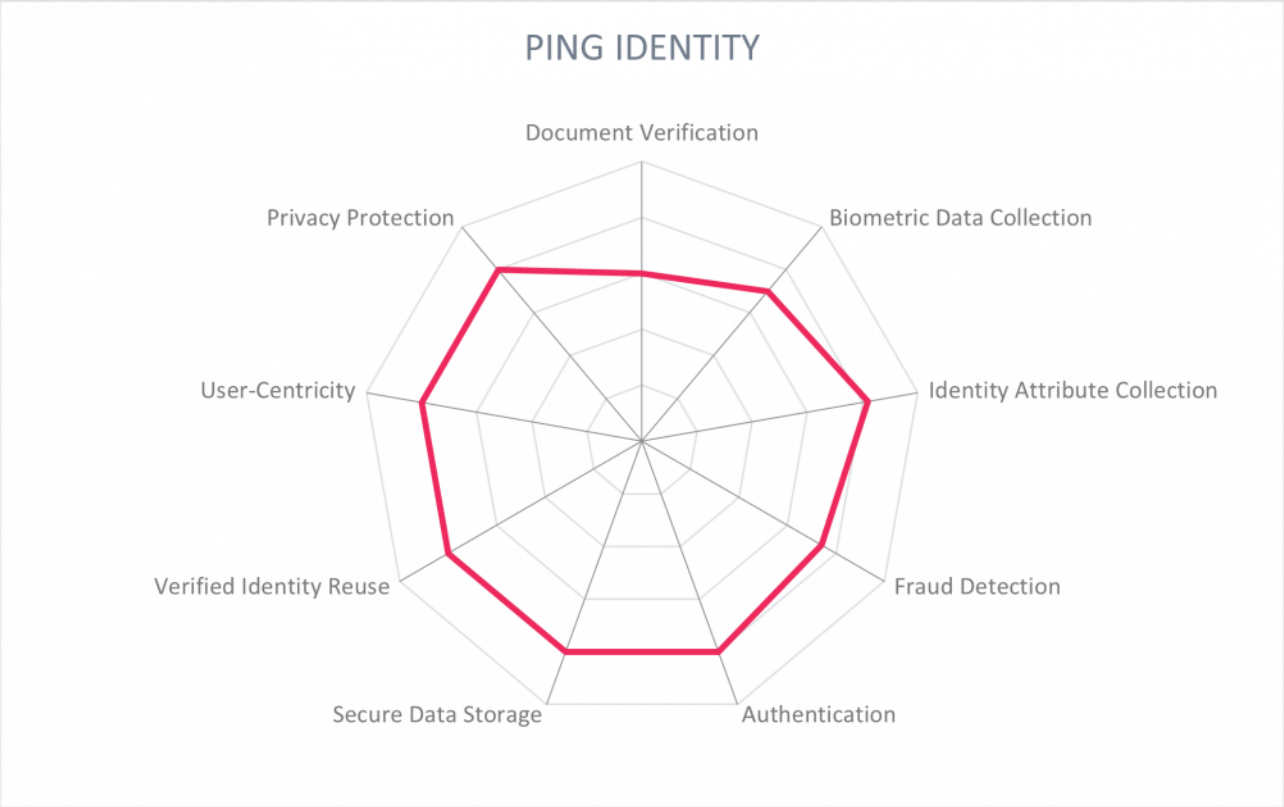
Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●
Market Standing	●●●●●

Strengths

- Able to integrate identity verification into Ping's established platform
- Account and password recovery are possible
- Individual attributes such as date of birth or name are certified
- Ping provides interoperability with its large customer base
- Strong APIs and connectors to other SaaS services
- ISO 27001 and SOC 2 Type II certified

Challenges

- Document analysis is provided with partners
- New product, although promising, just entering the market
- Proposes an ambitious and disruptive approach to onboarding, shifting from signup/sign-in to present and verify


PING IDENTITY
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.15 SecureKey Technologies

SecureKey Technologies (SecureKey) was founded in 2008 and is based in Toronto, Canada. SecureKey is a provider of digital identity and authentication solutions specializing in CIAM onboarding and authentication, enabling the trusted identities provided by banks, telcos, and governments to ease access to other services. SecureKey uses decentralized technology to federate the secure usage of trusted identity with for relying parties. SecureKey's partner ecosystem and market focus is largely Canadian, and is also active in the US, EMEA, and Asia-Pacific.

A user first shares their base identity attributes from their bank profile within the Verified.Me app or browser-based version, generating a DID for each attribute for a reusable, trustable version of this data. When a user wishes to register for a service, the user can select the option to sign-in with SecureKey on the service's website and is presented with a list of banks who are trusted identity and data providers. The user selects their preferred bank, signs in with their bank username and password to authenticate and confirm the accuracy of their profile information. The user can then select a participating organization to interact with and help verify their identity quickly and securely. The intent behind this approach is to provide business integrity benefits as user motivation is high to keep close tabs on their financial transaction accounts. Storage of an ID document anchored to a device. Verified.Me is used for digital KYC processes, and the reputation provided by a bank-trusted identity adds value to other services.

The solution uses a consortium approach with a private, permissioned Hyperledger blockchain implementation. SecureKey only stores integrity proofs, consent, evidence of transmission of encrypted records of data transfer and receipt, in the blockchain. Verified.Me is built with triple-blind capabilities to protect user privacy: neither the trusted identity provider nor the service being accessed know the other parties involved, but receive proof that the identity is verified. Any data that is requested by a relying party is first reviewed and approved by the user.

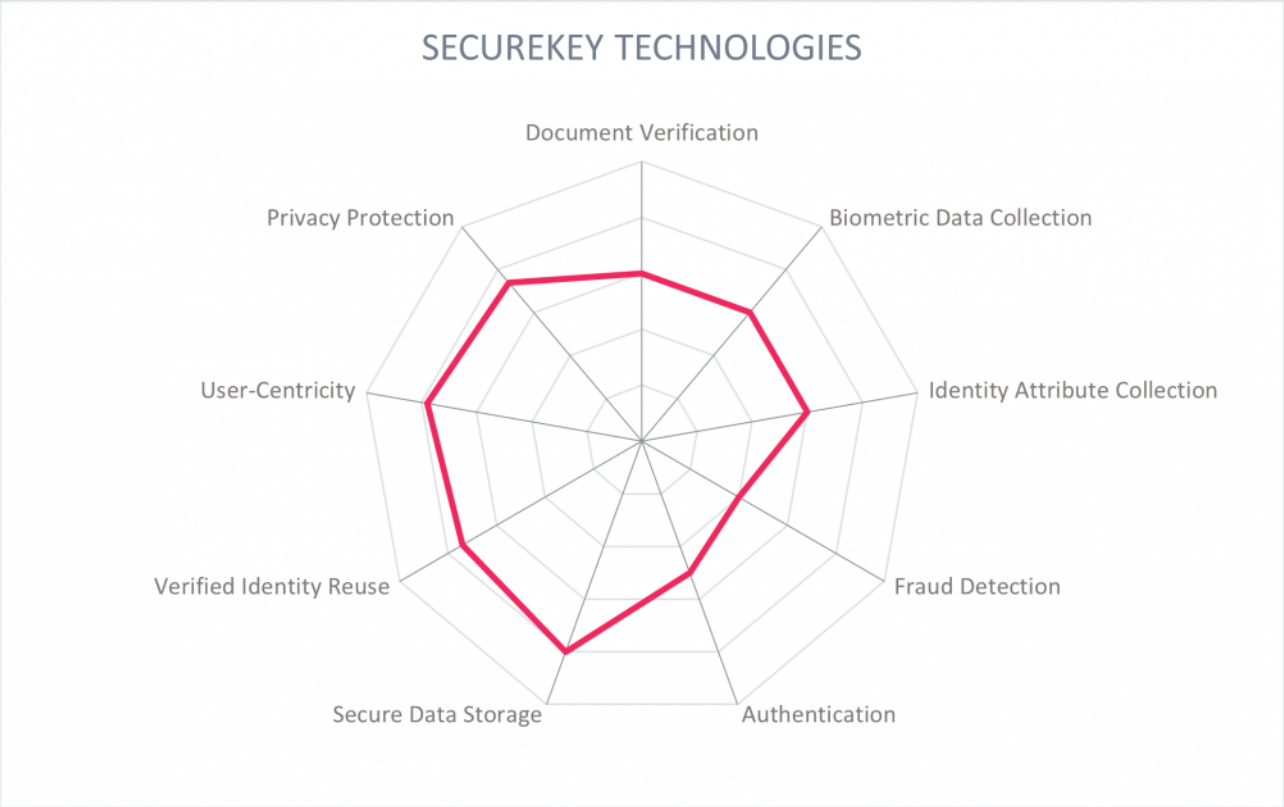
Security	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○
Market Standing	●●●○○

Strengths

- Consortium approach provides secure environment for financial institutions to interact
- Works with W3C, DIF, DIACC, and released its own open-source TrustBloc DID initiative
- Ensures privacy between identity providers and relying parties
- Successfully enables the reuse of an existing digital ID

Challenges

- Consortium approach also restricts the partner ecosystem to those that choose to join the network
- Currently only processes identifiers anchored in Hyperledger Fabric
- Document check and biometric capabilities offered through partners


SECUREKEY TECHNOLOGIES
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.16 Signicat

Signicat is headquartered in Norway and has been delivering identity solutions since 2006. It enables the customer to verify user identities by orchestrating verification steps across many regional partners, packaging identity info and delivering it to the customer. Identity reuse is supported through facilitating the use of digital IDs such as eIDs and BankIDs for access to other online services. Signicat includes over 30 eID integrations, primarily focused on Europe.

The target assurance level determines the method of onboarding, ranging from automated verification, eID onboarding, or video verification from third-party partners. For ID document processing, the ID document is scanned by the end user with a webcam or mobile device, able to analyze the MRZ and using NFC. This intake is combined with biometric analysis of a selfie and photo on ID document. Identification takes place by cross-checking the information from the ID document against authoritative records, then validation occurs by conducting a risk analysis for politically exposed persons, high risk geographies, etc. Signicat's Assure API normalizes attributes from the varying identity providers. The user can authenticate using eID or by using Signicat's MobileID, compliant with PSD2/SCA. Identity Assurance Level 3 can be achieved.

Signicat does not hold any customer data, but it is stored based on customer requirements. Customers are able to choose which third-party services are used to bolster document verification and video identification. Signicat's APIs can be web-based or built into a customer application. Signicat complies with PSD2 SCA requirements.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Market Standing	● ● ● ● ○

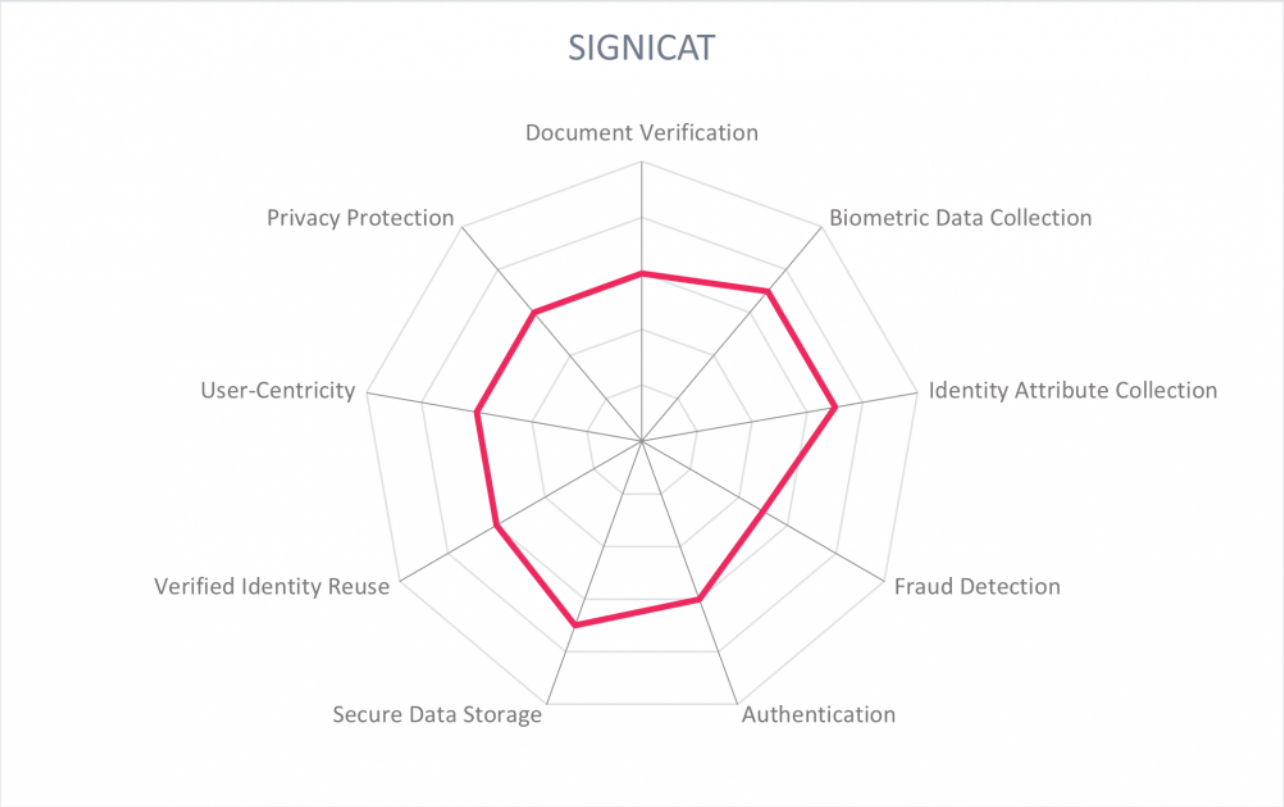
SIGNICAT

Strengths

- API-forward architecture
- Provides access to all eIDs with SAML and OpenID Connect
- Flexibility of third-party partners enable different assurance level schemas to be fulfilled
- Supports use of over 30 eIDs, including BankIDs for identity reuse
- Digital signing capabilities

Challenges

- Most document and video verification services provided by third parties
- No OCR capability
- Verification is done per transaction, does not yet have an option to reuse verified data.


SIGNICAT
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.17 Thales

Thales DIS (Digital Identity & Security) division, previously called Gemalto, is based in Paris, France, and supports governments with their digital ID schemes with a wide portfolio of mobile ID solutions for citizens to provide a digital online identity. Authentication, identity attribute sharing, ID federation services, and digital signature use cases are supported.

Thales provides reusable digital mobile identities to governments with PKI software, enabling citizens to verify their identities in real time and sign into government and private services web portals using various methods, including biometrics. Thales offers identification scenarios to onboard to a mobile ID. Depending on the ecosystem in place, a citizen's identification can be done remotely, based on non-electronic documents data capture and face recognition with liveness checks, through NFC reading of electronic documents, and facial recognition/biometric onboarding with a match on server process. Face-to-face identification is also possible. In the backend, a modular digital identity services management platform pilots the digital ID and can come up with self-service portals so citizens can manage their own identity, credentials, ID attributes, and consents. Since 2019, the company has added a Digital ID Wallet to its digital ID portfolio. This mobile ID enables users to store their identity credentials and attributes in a secure wallet app, which connects directly to government directory services for real time information, identity verification, and reliable attribute sharing. This wallet is a reusable identification solution for both in person and remote usage which can aggregate multiple digitized ID documents into a secure ID vault. The citizen can use them to prove their identity, share selective ID attributes with third parties and securely access online service including tax actions, banking, and government services.

Identity data is encrypted with end-to-end protocols on the user's device. Additional multi-layered security is provided with RASP, obfuscation, device binding, and WBC. Interactions with other identification app holders is facilitated through a secure communication protocol, with data shared only after consent is provided and with users in control of the data they share. Data can be shared via Bluetooth, Wi-Fi-aware, or NFC and is compliant with ISO 18013-5 standard to offer interoperability.

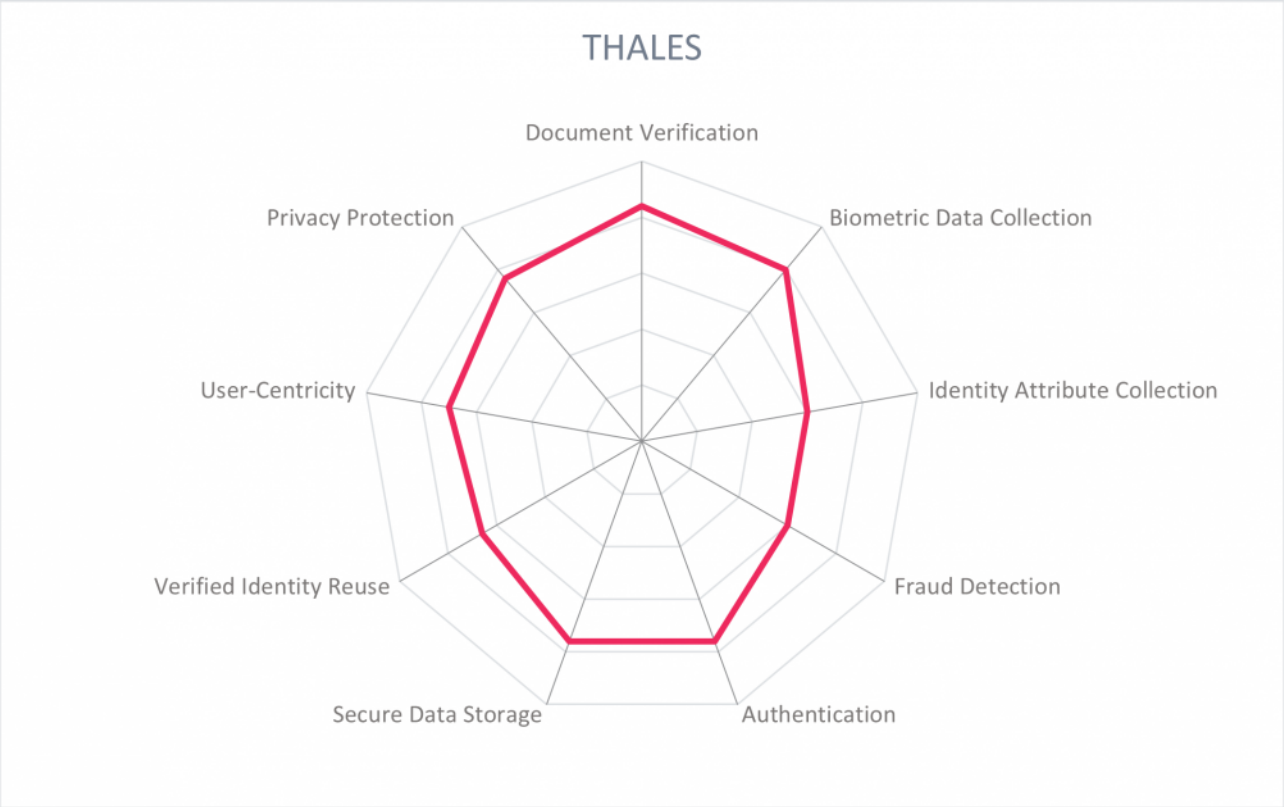
THALES

Strengths

- Strong case for verification, integrating use of physical IDs with reusable digital attributes
- Supports high assurance PKI use cases, strong representation in the banking and government sectors
- Identity verification and attribute sharing is possible offline
- Device synchronization is possible

Challenges

- Product is focused on security, leaving room for improvement on user-centricity
- Can add more fraud detection capabilities


THALES
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.18 Verimi

Verimi was founded in 2017 by a collection of 10 cross-industry shareholders to build a neutral, independent identity platform. Identities are derived from identity documents and existing user accounts. Verimi is designed to serve two types of customers: users/citizens, and B2B or B2C enterprise partners. The major use cases that Verimi fulfills are identification, authentication, digital signatures, and payment. Verimi's regional focus is on the DACH region and Western Europe, and supports verification for ID cards, passports, and drivers licenses for over 150 countries.

Verimi assigns a digital identity to the user at registration, including basic name and contact information as well as a Universally Unique Identifier (UUID) for use within Verimi. All ID attributes are attached within the user's Verimi wallet which can be bound to the Verimi App with strong authentication. Each user is assigned a pseudonymous external unique identifier (eUID) for each partner, so user tracking across partners is not possible by default. The UUID, public keys for authentication and encryption, App-ID, and e-mail address make up the user's Verimi ID. User eIDs can be onboarded from government sources, telecommunications providers, banks, etc. An API layer sits between users and enterprise partners which is certified according to OpenID Connect. The user logs into Verimi for management of identity documents and attributes and a full list of where Verimi can be used. Enterprise partners can customize the verification methods that fulfill their required assurance levels, including video call, NFC reading of eID, federated BankID, Qualified Electronic Signature (QES) self-identification, and biometric/AI identification. Verimi's IDP is approved by the German Ministry of the Interior for providing Identity-Services to the trust level "substantial" according to eIDAs.

The user can access their digital wallet from their desktop, smartphone, or other smart device. User data is protected by user-specific keys, which are stored in a trusted cloud with data encrypted at rest. Sensitive information is redacted in the user interface, and must be authenticated with a second factor within the Verimi App to view. The 2F authentication via the app is provided by a cryptographic signature key and a 6-digit personal number (PIN) or biometric factors. Users provide consent before any data is shared, and can access a full list of which identity attributes have been shared with which entities as stored within Verimi. A user can delete their account, related data, encryption keys, and transactions at any time. To help ensure data minimization is maintained, a Verimi Data Protection Officer works with the enterprise customer to determine which identity attributes are required to provide a service.

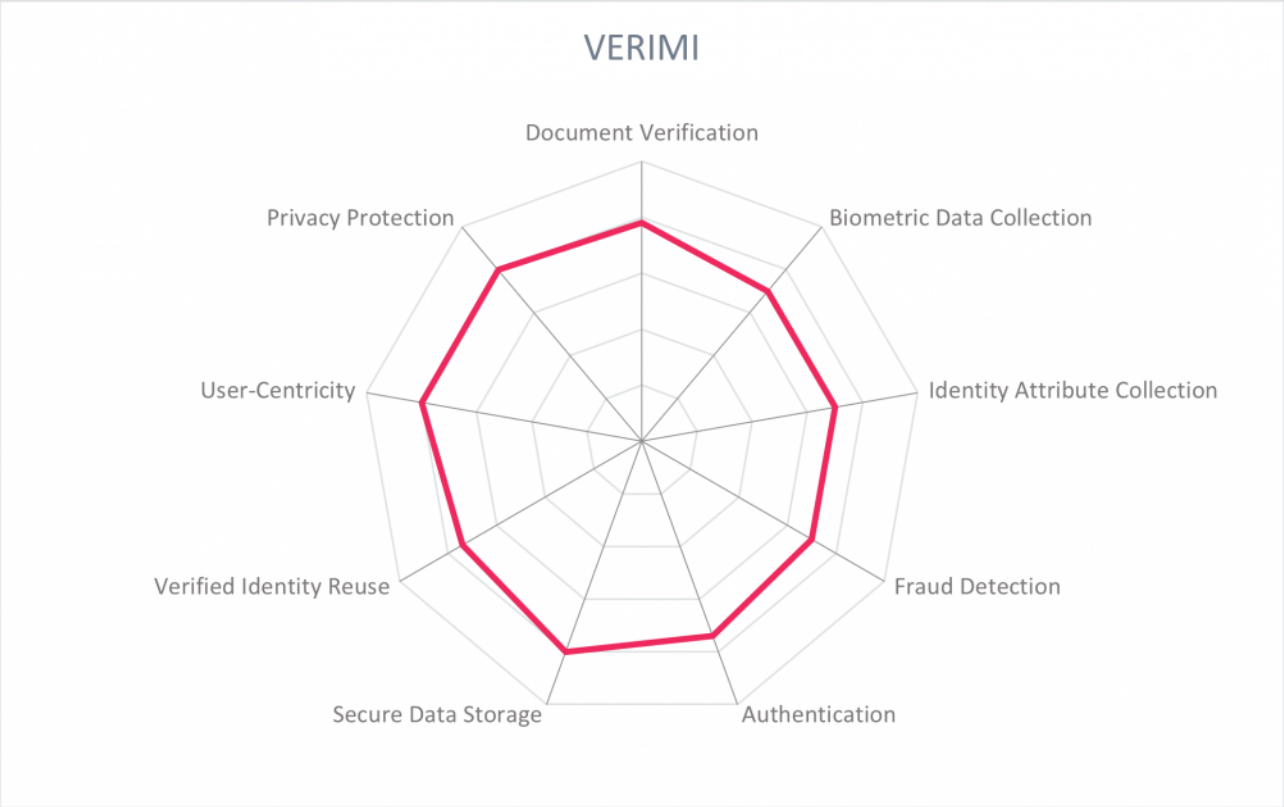
Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○
Market Standing	●●●○○

Strengths

- Strongly contributes towards a reusable digital ID with selectively sharable attributes
- Digital wallet can be accessed from desktop, mobile, or other smart device.
- Accepts eIDs from government sources and trusted IdPs
- Device synchronization is possible
- Compliant in all regulated sectors in Germany: BSI TR 03107, eIDAS, AML, TKG, GDPR, and PSD2 compliant
- Follows security and privacy by design principles
- API-forward solution based on OpenID Connect
- Additional value-added services such as QES and direct debit payments

Challenges

- No support for separate personas, but offers support for multiple entries for an attribute like emails and mobile numbers
- Identity transactions require Wi-Fi or internet connection
- Support for identity reuse could be strengthened with P2P exchanges


VERIMI
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.19 WebID

WebID is based in Germany, founded in 2012. It is a digital identity provider of AML compliant IDs. WebID focuses on meeting the needs of regulated and non-regulated industries, particularly in Germany and the DACH region but is available worldwide. WebID initially onboards users with the highest trust level possible with video identification, and supports identity reuse for authentication.

WebID provides identity verification via video calls, fully automated AI/biometric identification, BankID, and eID. Reuse is supported with authentication use cases, supported with TAN on mobile device, with biometric authentication on the roadmap. A user's WebID digital ID is derived from the data on government-issued ID documents, and a video call via browser or using the WebID app with WebID's ID center for an approximately 3-minute call with an ID checker. When the video verification is successfully completed, an OTP is sent to the user's mobile device to conclude the verification. WebID's Global Trust Technology Platform (GTTP) interlinks identity databases from multiple identity providers to make these digital identities available to business customers using a single interface. This enables digital identifications and signing for customers, and integrates with third-party products. Different product lines allow for varying levels of verification: WebID True Ident enables users to reuse their data stored in WebID's database, and re-verify with an OTP to the user's mobile device.

User data is stored on WebID's servers at the allowance of the user who always initiates and provides consent for any data transfer, and has the right to delete their data and account at any time. Customers store data as required for AML compliance. Data is stored by WebID encrypted, protected by multiple firewalls, with a server location in Germany. Data at rest is ensured with file hashes and encryption.

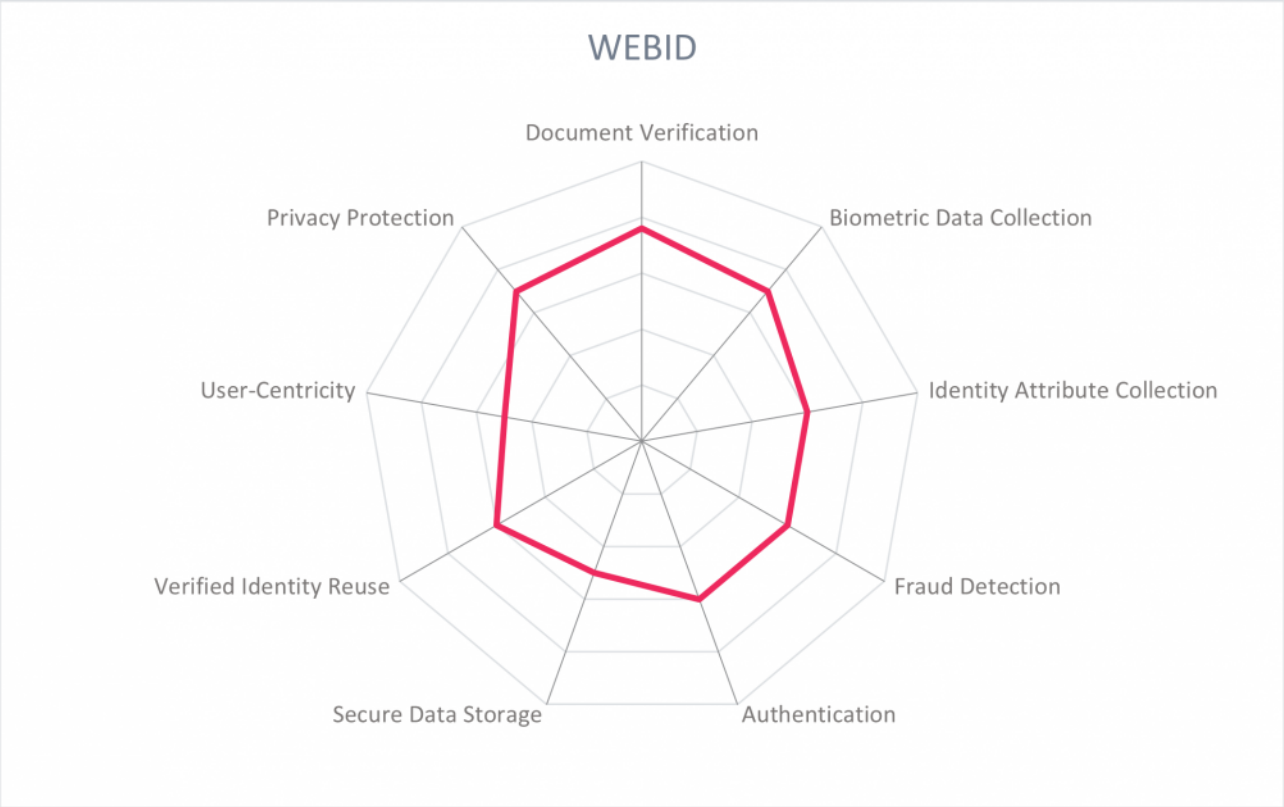
Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ○ ○
Deployment	● ● ● ● ○
Market Standing	● ● ● ● ●

Strengths

- Support for transactions with keyboardless devices, as well as mobile and desktop
- Strong ability to meet AML, KYC and highest trust levels
- Strong solution for video verification
- Data servers in Germany
- Qualified Electronic Signatures (QES) as an additional capability

Challenges

- Strong provision of verified identities, but reuse is limited to authentication use cases and within enterprise ecosystems
- Manual entry of data is typical for identity verification, though can be customized as per customer requirements
- Could increase interoperability with integrations with OpenID Connect, SAML, etc
- User identity is oriented around the enterprise customer, though the user retains ownership of the digital identity


WEBID
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

5.20 Yes

Yes was founded in 2016 and is based in Switzerland. Yes is an Open Banking ecosystem, composed of 1,000 active bank partners and over 4,000 passive bank participants. The geographic focus is on Germany, with entry to other markets on the roadmap.

Yes enables users to onboard with other services using their online banking credentials. The user selects the option to register with Yes and is sent to their preferred online banking portal to login. The user receives a notification requesting consent to transfer information to the relying party. A TAN as a second factor is sent to the user's phone or maintain the same second factor that is configured for the user's online banking account. Registration forms are auto-filled from the online banking profile. If required for higher levels of assurance, the relying party receives the user identity claims with metadata to attest its verification process and trust framework for a fee. A pseudonymous identifier can be provided for user re-login. Yes achieves eIDAS level Substantial.

Yes establishes a marketplace for qualified trusted service providers, enabling relying parties to select the provider based on price and differentiated features. Identity data is exchanged between banks and relying party only, with financial institutions managing data based on regulatory requirements. Yes does not hold user data at any time during the transaction. Users view their transactions in the preferred online banking portal. Payment initiation is on the roadmap.

Security	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●
Market Standing	●●●○○

Strengths

- Built using open standards including OAuth, OpenID Connect, and Cloud Signature Consortium
- Qualified Electronic Signatures (QES) as an additional capability being rolled out
- AML compliant
- API-forward architecture
- Valuable for logging into infrequently accessed sites
- Compelling use case for financial institutions to remain active post-PSD2

Challenges

- Relatively small vendor, with opportunities for growth
- No biometric capability yet
- Identification of eIDs and BankIDs via partners
- No additional verification process on top of BankID


yes®

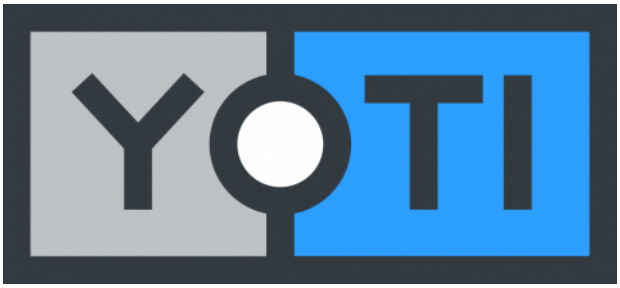
5.21 Yoti

Yoti is a global digital identity platform based in the UK with a suite of products spanning identity verification and KYC, authentication, e-signatures, and age verification. It also has the Yoti app, a reusable decentralized identity wallet launched in 2014 . Yoti is used by clients in the health care sector, government, and large multinationals and focuses on streamlining and securing CIAM and B2B partner onboarding use cases. Yoti serves the UK market with expansion to North America, Canada, India, Australia, New Zealand, and France. ID documents including passports from 195 countries, drivers' licenses, and national identity cards.

Yoti's embedded identity verification can be white labelled in customer websites and mobile apps, customizable to the customer's required level of assurance. Document verification uses a combination of AI and trained security personnel and takes 1-3 minutes. The document scan uses OCR, NFC for chip reading, and scans the MRZ. The document scan is a hybrid process with AI, third-party database checks, and supported by qualified document checkers. Yoti allows some user-certified data. Identity data is extracted from an image and used to cross reference the ID documents. Identity verification is completed with liveness detection and face matching, supported by fraud detection via mask attacks. Yoti's document scanning capabilities meet the AML requirements of UK's JMLSG.

Yoti provides a receipt of credentials shared to the individual, and a business receives evidence and a recommendation from Yoti. The user's private key to their data is held and managed by the individual only. Data is not stored on the user's device, but in a private cloud data store, with Yoti's transaction data retention period specified by the customer or deleted immediately after a transaction via API call. Consent is requested from the user for every identity transaction. Yoti's architecture design ensures each piece of user data (i.e., first name, surname, DOB) is stored sharded and separately to prevent fraud and hacks.

Security	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○
Market Standing	●●●○○

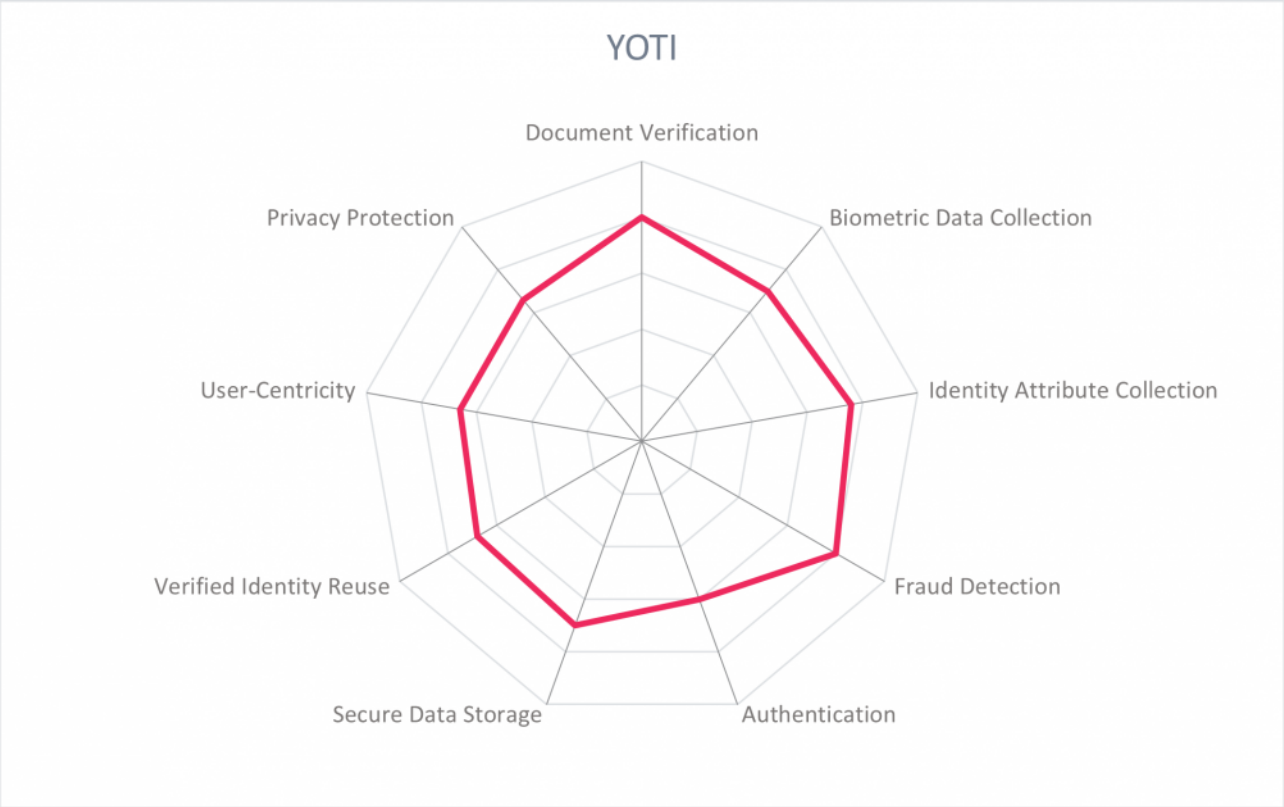


Strengths

- Supports DIDs
- Part of Canadian DIACC and projects to create interoperable trust frameworks across public and private sectors
- ISO 27001 and SOC 2 Type II certified
- Account recovery is possible
- eSignature is an additional capability
- Registered BCorp
- Biometric authentication linked to verified identity

Challenges

- Relatively small vendor must achieve critical mass of users for strong benefits of identity reuse
- Could increase interoperability with integrations with OpenID Connect, SAML, etc
- Age estimation is based on algorithmic prediction


YOTI
Document Verification
Biometric Data Collection
Identity Attribute Collection
Fraud Detection
Authentication
Secure Data Storage
Verified Identity Reuse
User-Centricity
Privacy Protection

6 Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but still offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this report, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

- EnStream uses mobile subscriber data to verify customers and support AML compliance. With a geographic focus on Canada, identity verification, device authentication, and location services can be provided to a customer to increase security during login. This partnership with telcos for verified identity has not yet achieved reusable identity. Watch this vendor if a telecommunications-specific identity verification solution is needed.
- European NetID Foundation was established in 2018 in Germany to provide a European-centric and privacy-forward single sign-on option for consumers. Users have access to a Privacy Center, from which the user can control consent of data usage and password management. Companies can become partners by integrating NetID as a registration/authentication option. NetID is a free offering, with account providers being WEB.DE, GMX, or 7Pass. At this point there is no inclusion of verified identity in this solution. This is a vendor to watch for its contributions to the open-source community and privacy-forward work.
- HiveID is an identity verification solution through identity document scans and biometric data collection. HiveID also provides biometric authentication. This vendor to watch is a technology provider for vendors in this Market Compass, and in coming years may participate more in the reusable aspect of verified identity. Keep an eye on this vendor for advancements in the biometric identification and verification space.
- iDIN is a solution serving citizens of the Netherlands through federation of BankIDs. iDIN consists of several product types that can be used in different use cases: identification, login and age confirmation. Signing will be added in the near future. This is proving itself to be a strong and well-developed approach to reusing BankIDs with a range of service providers. Watch this vendor if you're interested in strong solutions serving the Dutch region.
- IDNow is a remote identity verification solution for KYC use cases. Automated identity verification is possible, as well as video identification, verification via bank transfer, support for German eID cards, and

electronic signatures are offered. Based in Germany, IDNow has global coverage for verification. IDNow did not respond when asked to participate in this report. For a complete view of the remote identity verification market, keep this vendor on the radar.

- IRMA is an open-source decentralized solution out of the Netherlands to onboard a Dutch passport to a mobile phone for service registration and digital signatures. Although the solution is available outside the Netherlands, the identity attributes able to be onboarded are limited to name, address, email, and phone number. This project may see more growth as integrations for decentralized solutions with enterprise authentication sources become more widespread. Watch this vendor to for advancements in the decentralized open-source community.
- Jolocom is an open-source decentralized identity solution with SmartWallet and SDKs for any role in the Self-Sovereign credential exchange ecosystem: for verifiers, issuers, custodial services, and more. With regular releases of new capabilities, this open-source vendor may be the foundation for new verified identity solutions in the coming years. Watch this vendor for advancements in the decentralized open-source community.
- Mitek Systems uses AI/ML to onboard government-issued IDs and the holder's biometric information. Integration into customer apps for KYC uplift is possible. This vendor has compelling digital identity onboarding capabilities and may contribute more to reuse of verified identity in the future. Keep this vendor in mind when looking for AI/ML capabilities in verified identity onboarding use cases.
- Seczetta is an identity proofing solution specifically geared towards enterprise onboarding of employees, external partners, contractors, and devices. Using document scanning and biometric data collection, this information is transferred to the organization onboarding them. The API-based platformed has integrations to Sailpoint, Ping Identity, and other major IAM providers. This vendor is a rising solution for complex multi-party and/or remote onboarding scenarios. Watch this vendor for developments in enterprise-grade identity verification for an array of use cases.
- Vela specializes in providing the architecture to issue, store, and share employment credentials. A decentralized solution, this vendor is a promising player in reusable identity, and may develop stronger identity verification capabilities in the future. Keep an eye on this vendor for applications of sharable workplace credentials.

7 Related Research

Market Compass: Decentralized Identity: Blockchain ID & Self-Sovereign Identity – 80064
Leadership Compass: CIAM Platforms – 80040
Leadership Compass: IDaaS Access Management – 79016
Executive View: Callsign Intelligence Driven Authentication – 80174
Executive View: Oxyliom Solutions GAiA Advanced Identity Management – 80175
Executive View: Ping Identity's PingFederate – 80330
Executive View: Signicat – 72537
Advisory Note: Mobile Biometrics for Authentication and Authorization – 70283

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
- Ease of Delivery
- 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.

Ease of Delivery 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

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.