KuppingerCole ANALYSTS

Reusable Verified Identity

Anne Bailey

January 4, 2023

LEADERSHIP COMPASS 2023

This Leadership Compass provides an overview of up-to-date insights on the leaders in innovation, product features, and market reach for Reusable Verified Identity. These vendors enable a digital identity that has been verified to represent a real-world entity to be reused by the issuing organization/identity provider (IdP) or by organization independent of the issuing organization.

Contents

Figures

Tables

Introduction / Executive Summary

In this Leadership Compass, we evaluate solutions that can serve as a foundation for customers who need to utilize verified identity in processes and store it for future use – be it within the issuing organization's (identity provider, or IdP) own ecosystem in the form of authentication, or outside the issuing organization's ecosystem with service providers completely independent of the issuer.

The key capability of this market segment is reusability, meaning that a verified digital identity can be used in multiple contexts. This ranges from using the verified identity multiple times at the same organization to using the verified identity issued by one organization with another, completely independent organization. Reusability builds off the concept of a verified identity, which is a digital identity that has been verified to describe a real-world identity in digital form. Identity verification is therefore a fundamental part of establishing reusability.

However, most identity verification solutions do not address the critical lack of trust when interacting between organizations that prevents, for example, one bank from accepting the KYC and vetting of a customer from another. Reusable identity challenges the previously held tenant that digital trust cannot be shared from one party to another by providing identities that are verified at a sufficient level of assurance which are portable and interoperable.

There are many vendors that provide reusable identity to some degree. While the vendors that participated in this report all have well-functioning solutions that yield some level of reusability, those that scored most highly are ones that also bring a wide breadth of applicability; some solutions are streamlined to function with pre-existing enterprise systems, some offer promising ways to discover and accept the reusable identities of other organizations, some provide a variety of reusable identities such as through eID, bankID, and identity verification, and others are strong providers of digital citizen identities that bring expertise and scalability to the market.

Other vendors that are included in this Leadership Compass may have fully-formed reusable identities, but be limited in geography, be limited to reusability within a single organization or small ecosystem rather than provide widespread reusability across many organizations, or be in an early growth phase with promising potential. These solutions may place lower on the leadership charts seen in chapters 2 and 3 but will still show strong capabilities ratings in each solution's descriptions in chapter 5.

This Leadership Compass gives an overview of the market, required capabilities of a well-rounded solution, and detailed information on the participating vendors.

Key Findings

- This report covers reusable verified identity solutions, or vendors that enable a verified identity to be reused.
- Reuse often takes the form of authentication or identity portability to onboard with organizations separate from the issuer/IdP.

- Storage location is a differentiator between vendors in this market, typically split between federation and API hubs, cloud storage, and user-held wallet storage.
- Storage model is a differentiator between vendors, typically split between decentralized and centralized models, with some options for hybrid models.
- Organizations must weigh the pros and cons of the different storage locations and models, and make a decision based on their unique use case and needs.
- Overall Leaders in alphabetical order are: 1Kosmos, IDEMIA, Microsoft, Ping Identity, Signicat, and Thales
- Product Leaders in alphabetical order are: 1Kosmos, IDEMIA, Microsoft, Ping Identity, Signicat, Thales
- Innovation Leaders in alphabetical order are: 1Kosmos, Airside Mobile, IDEMIA, Microsoft, Ping Identity, Signicat, Thales, Yes.com

Market Segment

The term “Reusable Verified Identity” adds reusability to a verified identity.

- A verified identity refers to digital identities that have been verified to describe a real-world identity in digital form, and that the verification remains valid throughout the identity lifecycle.
- Reuse means that the verified identity can be used in multiple contexts. This ranges from being used by the issuing organization multiple times – like using a verified attribute like facial biometrics as an authentication factor – to enabling the verified identity to be reused by organizations independent of the issuing organization – like an employer accepting a verified education credential for a new hire.

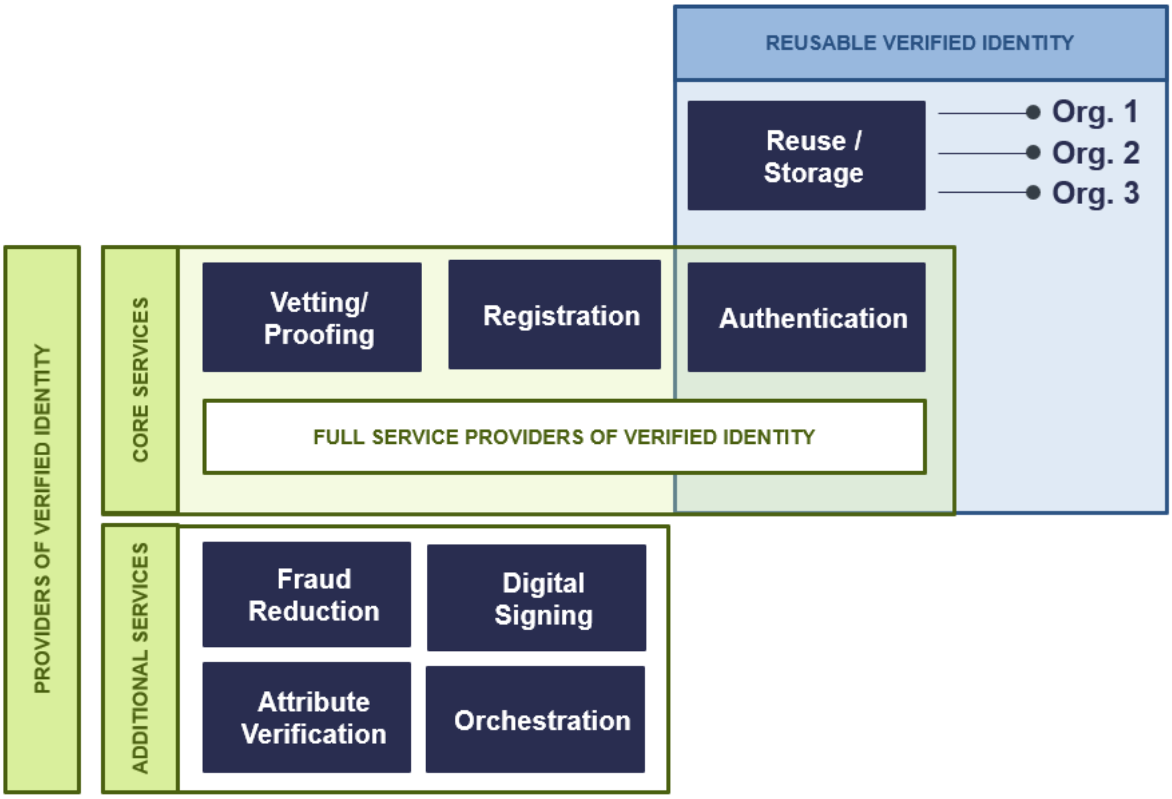


Figure 1: Reusable Verified Identity Builds off the Capabilities of Other Market Segments

The figure above differentiates between the Providers of Verified Identity market segment and the Reusable Verified Identity market segment. Reusable verified identities typically benefit from the capabilities of verified identity providers but enable the storage and reuse of those identities already verified with many different organizations.

Therefore, reuse of verified identities changes the focus from mitigating a single organization's risk to unlocking ecosystem cooperation and reducing repetition while maintaining preventative security. Reusable verified identities are unique in that once issued they can be reused between organizations and across borders with a wide variety of services. Critical factors to their success are the breadth of services the reusable verified identity allows access to, the amount of effort in adding support for a reusable verified identity to a service, and its interoperability with often-used standards.

Thus, this Leadership Compass analyzes vendors that enable a verified identity to be reused outside of the context in which it was issued (with other organizations, or when the user assumes another role) while maintaining high levels of assurance with minimal reverification or validation effort.

Delivery Models

The delivery of reusable verified identity is typically determined by the storage of the identity information. There are many technical possibilities each with pros and cons. The decision for which delivery and storage model to take is best made by the implementing organization.

Storage of identity information can be thought of along two different axes: location and model. The storage location is most often split between federation and API hubs, cloud storage, and user-held wallet storage. The storage model refers to who is in control of the stored identity information and is typically split between decentralized (user-held) and centralized (organization-held) models, with some options for hybrid models.

Required Capabilities

Reusable Verified Identity vendors must provide a majority of the following capabilities.

- Identity Verification: Ability to verify the real-world identity, inclusive of biometric methods, document verification, data aggregation, PKI/certificates, etc.
- Ease of Reverification: The verified identity should maintain its validity over time, supported by an easy, cost-effective reverification upon reuse. This reverification could be facilitated with an identity hub, federation with a verified ID provider (eID), with biometric and liveness checks, with the exchange of Verifiable Credentials, or with PKI.
- ID Storage: The storage of reusable verifiable identities must enable reuse while providing adequate security and privacy. Decentralized and centralized storage options are included.
- Authentication: Apply the verified identity to authentication and/or as a second factor, step-up, dynamic, etc. Authentication methods could include federation, biometric,

PIN, device signals QR/Push Notifications, OTP, and others. Interoperability with authentication sources (including eID schemes, federated partners, FIDO, Windows Hello, etc.) and support of standards (OIDC, SAML) is critical.
- Workforce Applicability: The solution's applicability to workforce IAM use cases, serving employees, partners, suppliers, contractors, freelancers, etc.
- CIAM Applicability: The solution's applicability to consumer IAM use cases, serving individuals and customers to access a service provider's resources and services. Should have self-service functions and the ability to synchronize accounts between devices.
- Scalability: How well the solution can scale to support enterprise-wide identity onboarding and authentication.
- Privacy Protection: Specific attention to end-user privacy in the solution design, information collection, storage, and transactions. This includes 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.

The inclusion criteria for this Leadership Compass are:

- An emphasis on providing a digital verified identity for onboarding and later use
- A baseline level of support for the capabilities listed above, including use of partner technology (e.g., own technology for biometric onboarding, partner technology for document scan and validation)
- Support for cloud, hybrid, or on-premises deployments

The exclusion criteria for this report are:

- Point solutions that only provide identity verification, or elements of identity verification (e.g., only behavioral biometrics without the capacity to generate a digital identity attribute) will not be considered
- Vendors that serve only one country's citizens (e.g., product only usable within the Netherlands by residents of the Netherlands)
- Vendors without active deployments with customers will not be considered

However, there are no further exclusion criteria such as revenue or number of customers. We cover vendors from all regions, from start-ups to large companies.

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership

- Innovation Leadership
- Market Leadership

Overall Leadership

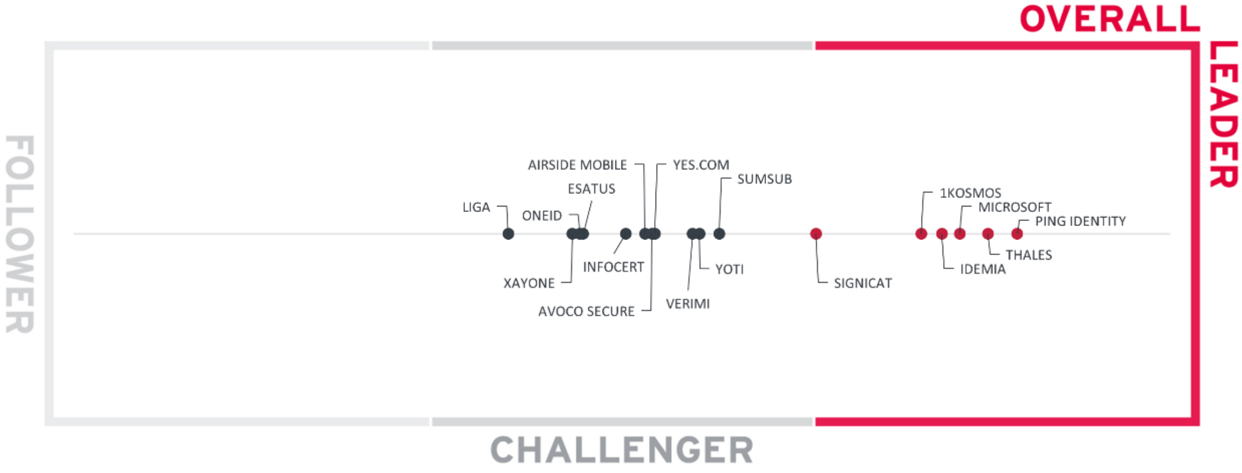


Figure 2: Overall Leadership Rating for the Reusable Verified Identity Market Segment

The Overall Leadership rating is a combined view of the three leadership categories, i.e., Product Leadership, Innovation Leadership, and Market Leadership. This consolidated view provides an overall impression of our rating of the vendor's offerings in the particular market segment. Notably, some vendors will perform better in different aspects. For example, some vendors have a strong market presence but display lower ratings in innovation, while other vendors may show their strength in Product Leadership and Innovation Leadership but have a relatively low market share or lack a global presence. Therefore, we strongly recommend looking at all leadership categories, the individual analysis of the vendors, and their products to gain a comprehensive understanding of the players in the market segment.

In the Overall Leadership rating chart, we see roughly two densely packed groups of competitors. There are six vendors in the Leader section displayed in red. These include known players in the identity issuance space such as Thales, and IDEMIA, and enterprise identity vendors Ping Identity, Microsoft, Signicat, and 1Kosmos.

Eleven vendors are placed in the Challengers section. These include well-rounded products, such as Sumsub, Verimi, Yes.com, Avoco Secure, Airside Mobile, Yoti, OneID, XAYONE, esatus, Infocert, and Liga. Even though these vendors deliver quality products, they typically have a more focused regional reach and capabilities.

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the product features by the company's products will be necessary.

Overall Leaders are (in alphabetical order):

- 1Kosmos
- IDEMIA

- Microsoft
- Ping Identity
- Signicat
- Thales

Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.

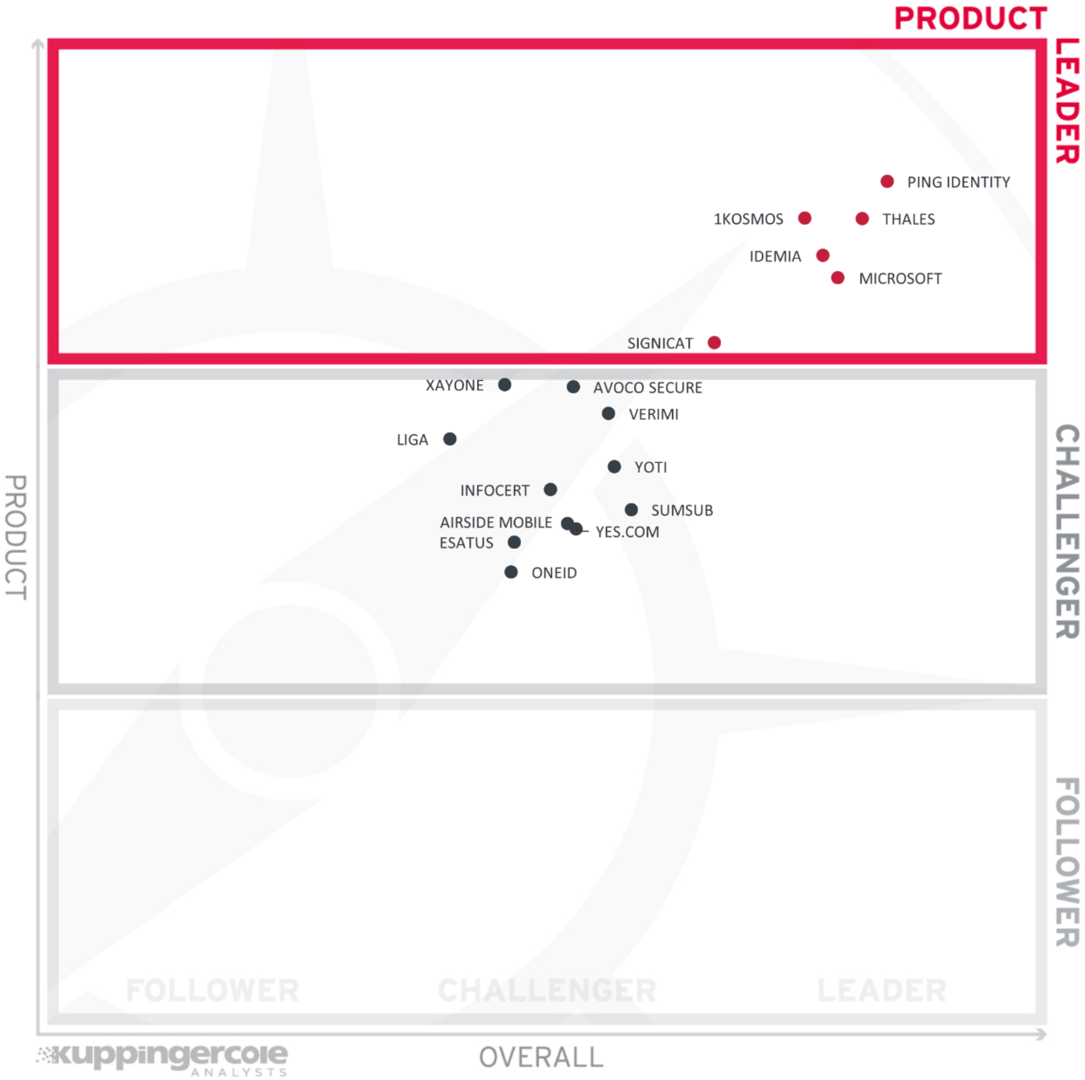


Figure 3: Product Leadership in the Reusable Verified Identity Market Segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

A cluster comprised of Ping, 1Kosmos, Thales, IDEMIA, and Microsoft lead the pack. Ping and Microsoft offer products that provide organizations with a means to use their existing identity management infrastructure for reusable credentials. Thales, 1Kosmos, and IDEMIA take a strategic focus on identity verification for its reuse during later stages of the identity lifecycle. Signicat brings together existing eIDs, other verified identities, and digital signatures for a suite of reusable identity products.

Challengers include a collection of competitors that use different methods to achieve reusability. Liga and Avoco Secure leverage already verified identity attributes to facilitate validated digital identity use and reuse. XAYONE and Verimi use document and biometric verification to generate a verified reusable identity as well as using validated information shared by the user's bank. Airside Mobile onboards credentials to user wallets for reuse within a defined ecosystem.

Sumsub facilitates KYC information across shared customer bases of agreeing organizations. Yes.com leverages the open banking ecosystem in Germany for user-friendly access to verified identity, as does OneID and Yoti in the UK. Infocert is powering a decentralized solution for user-centric identities and wallets, and esatus uses a decentralized architecture to enable workforce identity access management.

Product Leaders (in alphabetical order):

- 1Kosmos
- IDEMIA
- Microsoft
- Ping Identity
- Signicat
- Thales

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

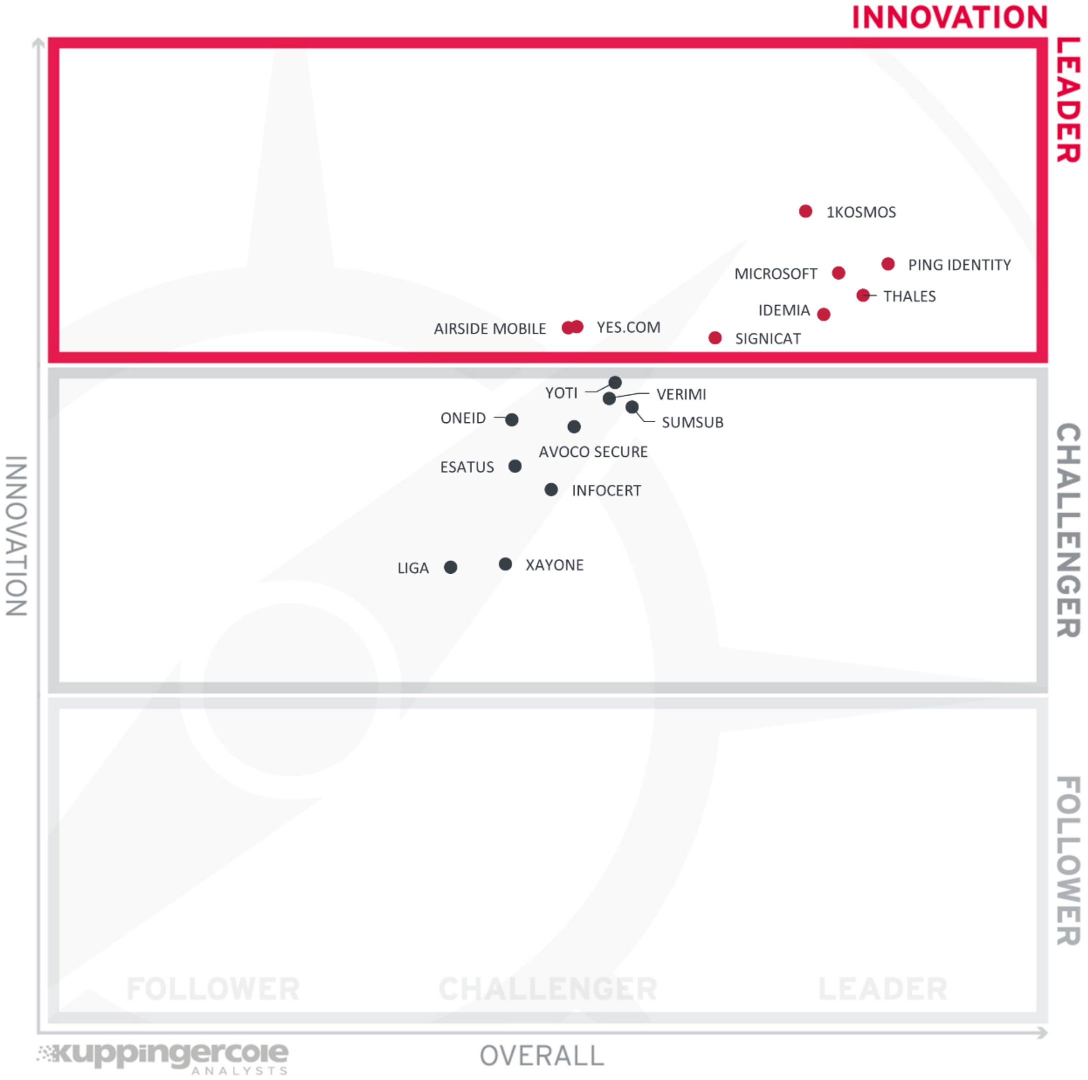


Figure 4: Innovation Leadership in the Reusable Verified Identity Market

There is plenty of opportunity for innovation in this market segment. Binding a real-world identity to a digital credential in the most secure, user-friendly, and privacy-preserving method requires creativity and a willingness to change the status quo. Many different methods are represented in this Leadership Compass, which must be evaluated on a case-by-case basis.

Leading the innovation group is 1Kosmos, a pioneer in using decentralized identity credentials that carry a high level of assurance for both workforce IAM and CIAM use cases.

Ping Identity also takes a decentralized approach while also building out an impressive ecosystem of identity verification partners to meet global regulatory and customer needs. Microsoft strives to enable decentralized identity credentials backed by verified real-world attributes to interoperate with existing infrastructure such as Azure AD with as little friction as possible.

Thales and IDEMIA make strides to enable citizen IDs that interoperate with emerging Mobile Document (mDoc) standards as well as emerging decentralized wallet standards. Airside Mobile and Yes.com keep their solutions lean while making strides for an interoperable and secure means of exchanging verified identity information across organizations and borders. Signicat brings valuable insight into the digital signatures space.

Challengers in the innovation section still have valuable contributions. Verimi, OneID, and Yoti leverage existing ecosystems to advance new use cases for verified identity. Sumsub establishes agreements between organizations to exchange verified information about shared customer bases.

esatus approaches the verified reuse use case differently by targeting the workforce. Liga provides a bridge between certificates and smart cards with validated information while XAYONE meets the needs of the financial sector. Infocert is developing business models for issuer/validator exchange of value.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- Airside Mobile
- IDEMIA
- Microsoft
- Ping Identity
- Signicat
- Thales
- Yes.com

Market Leadership

Lastly, we analyze Market Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

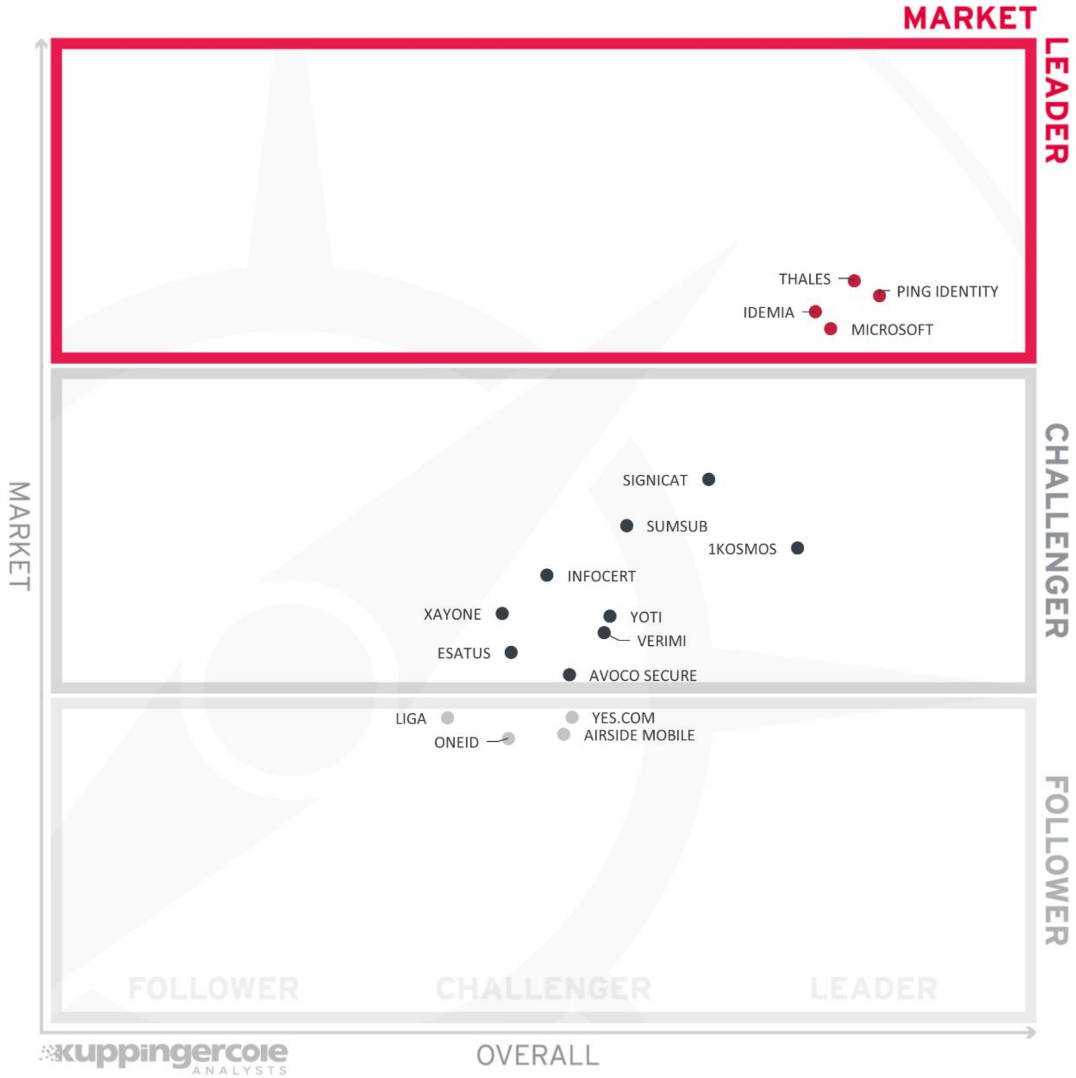


Figure 5: Market Leadership in the Providers of Verified Identity Market Segment

This market segment is developing, and although well-rounded products exist with the means to reach customers globally, most vendors are in early stages of bringing products to enterprise customers. Thales and IDEMIA have a global reach with their citizen identity products. Ping Identity and Microsoft have global customer bases and are bringing their reusable verified identity products to them.

Signicat leads the challengers with a strong market presence in the Nordics and expansion in EMEA. Sumsub has a strong presence in EMEA, APAC, LATAM, and other regions. 1Kosmos is growing its global market share and expanding the regions in which it serves customers.

Infocert has a strong European presence with other products and is gaining visibility with its reusable identity product. XAYONE is based in Europe and serves the African and Middle Eastern markets. Verimi, Yes.com, and esatus are focused on the German/DACH market, Liga and Avoco Secure on EMEA, while Yoti and OneID the U.K. market. Airside is present in North America.

Market Leaders (in alphabetical order):

- IDEMIA
- Microsoft
- Ping Identity
- Thales

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix

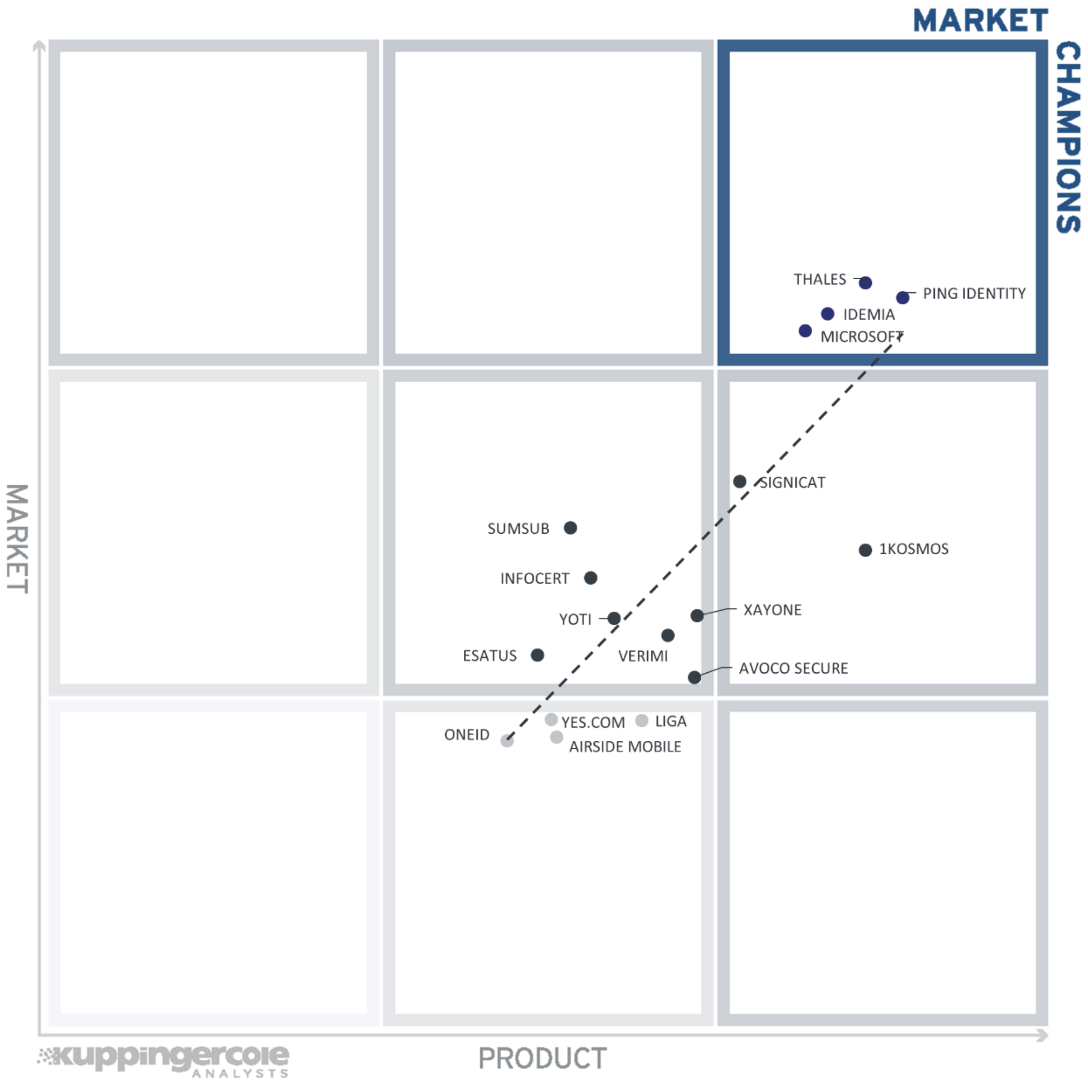


Figure 6: The Market/Product Matrix for the Reusable Verified Identity Market Segment

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

All the vendors below the line have a relative strong product compared to their market share. However, we believe that each has a chance for significant growth. There is a tight clustering of market champions which have the benefit of other well-known products and historic presence in the citizen identity space.

There are also several vendors that have a close correlation between product and market presence. Signicat, Verimi, Yoti, Yes.com, OneID, and Airside are all relatively close to the trend line, indicating their growth and product development are in sync. Other vendors tend to display stronger product performance in relation to their market presence, such as 1Kosmos, XAYONE, Avoco Secure, and Liga. Other vendors have a stronger market presence compared to product functionality, such as Sumsub, Infocert, and esatus.

The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

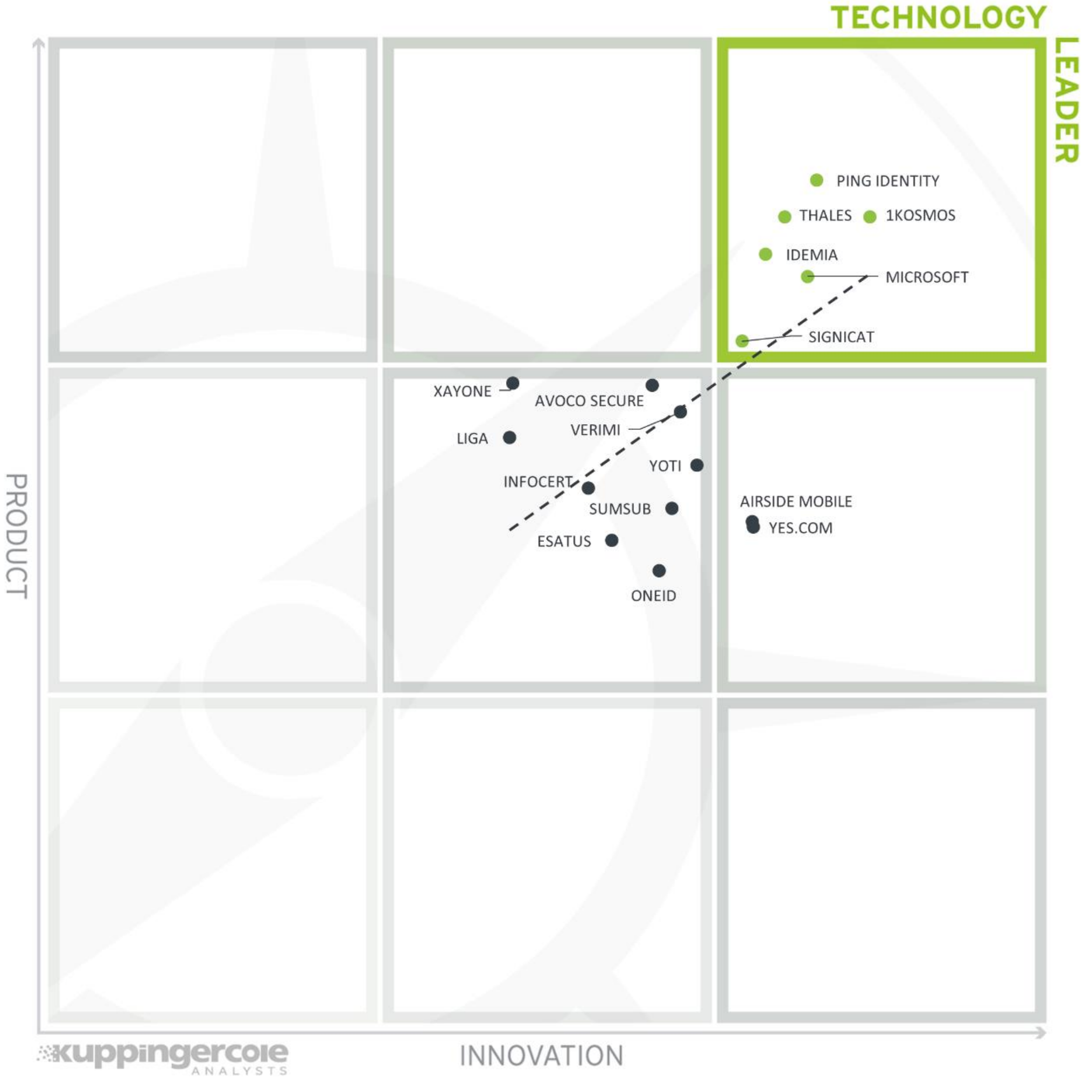


Figure 7: The Product/Innovation Matrix for the Reusable Verified Identity Market Segment

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Vendors are clustered relatively close to the trend line. The technology leaders have wide product functionality, with innovation focusing on interoperability of credentials, wallets, and the portability of existing eIDs and verified identity information. Other vendors showing high innovation include Verimi, Yoti, Airside Mobile, Yes.com, Sumsub, esatus, and OneID.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

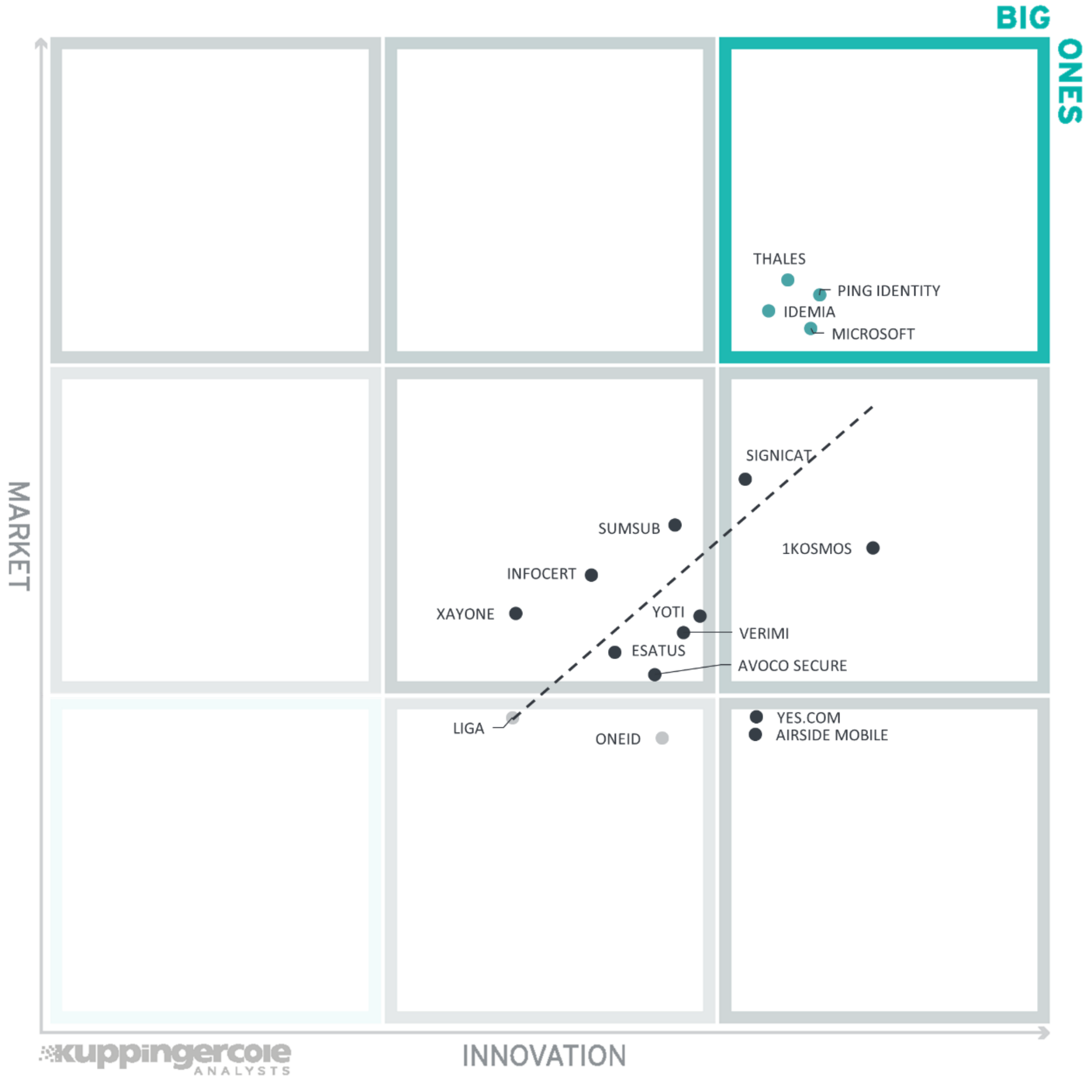


Figure 8: The Innovation/Market Matrix for the Reusable Verified Identity Market Segment

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

The Big Ones referring to those vendors that have both market share and top innovation are in alphabetical order: IDEMIA, Microsoft, Ping Identity, and Thales. Vendors such as Verimi, Yoti, Avoco Secure, OneID, Yes.com, and Airside Mobile can focus on improving their market positions to take advantage of their innovative products.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Reusable Verified Identities. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
1Kosmos	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Airside Mobile	Strong Positive	Positive	Positive	Positive	Positive
Avoco Secure	Strong Positive	Positive	Strong Positive	Strong Positive	Strong Positive
esatus	Strong Positive	Positive	Positive	Positive	Positive
IDEMIA	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Infocert	Positive	Positive	Positive	Positive	Positive
Liga	Strong Positive	Positive	Positive	Positive	Positive
Microsoft	Strong Positive	Positive	Strong Positive	Strong Positive	Strong Positive
OneID	Strong Positive	Positive	Positive	Neutral	Positive
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Signicat	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Sumsub	Strong Positive	Positive	Positive	Positive	Positive
Thales	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Verimi	Strong Positive	Positive	Positive	Strong Positive	Positive
XAYONE	Strong Positive	Positive	Positive	Strong Positive	Strong Positive
Yes.com	Strong Positive	Positive	Positive	Positive	Positive
Yoti	Strong Positive	Positive	Positive	Positive	Strong Positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product. For simplicity, the vendor and not the product is named.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
1Kosmos	Strong Positive	Positive	Positive	Neutral
Airside Mobile	Strong Positive	Weak	Weak	Neutral
Avoco Secure	Positive	Weak	Neutral	Neutral
esatus	Positive	Neutral	Neutral	Neutral
IDEMIA	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Infocert	Positive	Neutral	Positive	Positive
Liga	Neutral	Weak	Neutral	Neutral
Microsoft	Strong Positive	Positive	Strong Positive	Strong Positive
OneID	Strong Positive	Weak	Weak	Weak
Ping Identity	Strong Positive	Positive	Strong Positive	Strong Positive
Signicat	Strong Positive	Positive	Positive	Positive
Sumsub	Strong Positive	Positive	Positive	Positive
Thales	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Verimi	Positive	Neutral	Neutral	Neutral
XAYONE	Neutral	Neutral	Positive	Neutral
Yes.com	Strong Positive	Neutral	Weak	Neutral
Yoti	Positive	Neutral	Weak	Neutral

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the Leadership Compass on Reusable Verified Identity, we look at the following eight categories:

- Identity Verification: Ability to verify the real-world identity, inclusive of biometric methods, document verification, data aggregation, PKI/certificates, etc.
- Ease of Reverification: The verified identity should maintain its validity over time, supported by an easy, cost-effective reverification upon reuse. This reverification could be facilitated with an identity hub, federation with a verified ID provider (eID), with biometric and liveness checks, with the exchange of Verifiable Credentials, or with PKI.
- ID Storage: The storage of reusable verifiable identities must enable reuse while providing adequate security and privacy. Decentralized and centralized storage options are included.
- Authentication: Apply the verified identity to authentication and/or as a second factor, step-up, dynamic, etc. Authentication methods could include federation, biometric, PIN, device signals QR/Push Notifications, OTP, and others. Interoperability with authentication sources (including eID schemes, federated partners, FIDO, Windows Hello, etc.) and support of standards (OIDC, SAML) is critical.
- Workforce Applicability: The solution's applicability to workforce IAM use cases, serving employees, partners, suppliers, contractors, freelancers, etc.
- CIAM Applicability: The solution's applicability to consumer IAM use cases, serving individuals and customers to access a service provider's resources and services. Should have self-service functions and the ability to synchronize accounts between devices.
- Scalability: How well the solution can scale to support enterprise-wide identity onboarding and authentication.
- Privacy Protection: Specific attention to end-user privacy in the solution design, information collection, storage, and transactions. This includes 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.

1Kosmos – BlockID Platform

1Kosmos was founded in 2018 and is headquartered in New Jersey, USA. Its BlockID Platform provides full-service identity verification, including verification of documents and biometrics, onboarding, credential issuance, credential storage, and authentication. The platform supports three products: BlockID Verify which verifies user identity and issues Verifiable Credentials, and BlockID Workforce and BlockID Customer which enable an entirely digital onboarding and authentication experience for both IAM workforce and CIAM use cases.

The BlockID Platform provides several modules that revolve around user-managed identity. First the identity is enrolled, using various methods of identity verification based on customer requirements. Next is authentication, generating an authentication factor that is bound to the verified identity for a passwordless experiences. The BlockID Platform can also deploy traditional MFA methods if needed. The third module consists of Verifiable Credentials, providing the ability to issue, verify, and share credentials with selective disclosure. And the fourth module is storage, providing secure user-centric storage of credentials and biometric templates, protected with a user's private key and supported by a private distributed ledger. These modules are supported by standards, adhering to the NIST 800-63-3 IAL standards and eIDAS to enroll identities; FIDO, SAML, OAuth, OIDC, and NIST AAL for authentication; and W3C Verifiable Credentials and DIDs for credential issuance and storage.

These modules build on each other to deliver a reusable, verified identity. The initial verification of a user to a customer-determined level of assurance, combined with decentralized, PKI-secured storage of the Verifiable Credentials in a user-held identity wallet enable the user to reuse the credentials to enroll with service providers that they have not previously interacted with, or to authenticate upon repeated return to those service providers. The captured data is in complete control of the user and is not accessible by 1Kosmos or their customer. Privacy controls are passed to the user and are not the responsibility of 1Kosmos or their customer. The BlockID reusable identity can be used with any consumer-facing organization that is a 1Kosmos customer, with set organizations in a workforce context, and with a growing number of public institutions and government agencies.

BlockID Verify creates a verified digital identity for use in various onboarding, authentication, and workforce or consumer transactions. To initiate a remote 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 a wallet app to their mobile device. A wallet app is provided by 1Kosmos, may be white-labeled, or an SDK may be used. Additionally, an app-less workflow is available where users verify documents through a combination of web and a mobile device camera, resulting in a digital web wallet. Based on customer-defined requirements and workflows, the user is guided through document and biometric verification, while additional checks against authoritative sources, credit bureaus, and global watchlists occur in the background. For document verification, the front and back of the physical document is scanned with the user's mobile device and optionally read the embedded chip via NFC and checked against authoritative sources. Non-physical identity attributes can also be verified and onboarded, including telco account numbers, SSN, email address, phone number, and banking credentials. The document is verified to be held by the user it describes by onboarding facial biometrics, conducting a liveness check, and comparing against the picture captured during document scanning for a match. Proprietary AI classifies the document and checks for various types of fraud. Once the verification is completed, 1Kosmos issues a W3C Verifiable Credential to the user, stored in their mobile or web ID wallet. This verification is certified by Kantara for NIST 800-63-3 Identity Assurance Level 2 and Authenticator Assurance Level 2. BlockID is also FIDO2 and NIST certified.

BlockID Workforce and BlockID Customer build off the verified identity established by BlockID Verify. These products allow employees, contractors, other externals who need workforce access, or customers to onboard a verified identity, register, and use it for identity-based passwordless authentication or traditional MFA methods. Authentication methods include facial biometrics, TouchID/FaceID, QR code scan, FIDO authenticators, push notification, time-based OTP, email and SMS codes.

BlockID Verify operates on a private permissioned distributed ledger. The user’s identity and biometric data is stored encrypted on their device’s secure enclave, managed by their 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 distributed ledger. 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. The credential wallet app is available as a BlockID-branded app, a white-labeled app, or as an SDK. The platform and products are compatible with iOS and Android, supported by SDKs and an API Gateway for identity providers, brokers, privileged access and single sign-on service providers, and other IAM/CIAM providers.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

1KOSMOS

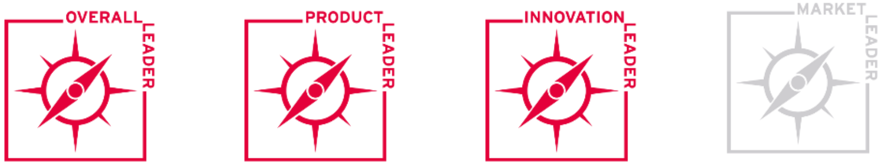
Strengths

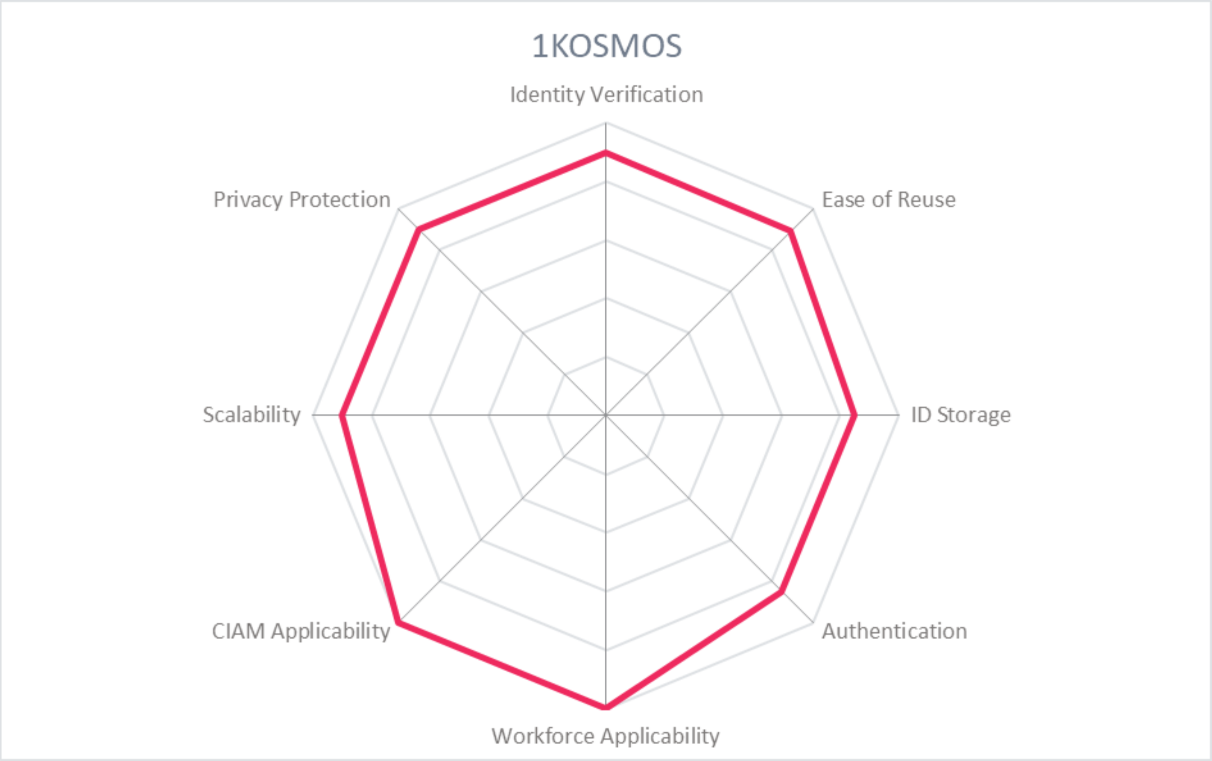
- Biometric authentication factors include face, voice, and fingerprint, and are independent from device biometric capability
- Has backend integration with trusted governmental institutions to verify ID documents
- Provides strong enterprise workforce authentication to achieve critical mass of users
- Process for user data recovery is in place
- Support for both mobile (app-based) and web (app-less) based verification workflows
- Uses standardized Verified Credentials and Decentralized Identifiers for credential storage and sharing
- Supports AD, LDAP, JWT, OAuth, OIDC, and SAML
- Kantara NIST 800-63-3 IAL2/AAL2 certified, FIDO2 certified
- iBETA Biometric Certified
- ISO27001
- Offline authentication is available with OTP
- Scalability is bolstered with container-based microservices

Challenges

- Support for eIDAS is on the roadmap
- Most use cases require the user to have a smart mobile device with camera functionalities
- Is a small vendor with some restrictions on regional document coverage
- Blockchain storage and scalability is a novel topic
- No support yet for behavioral biometrics

Leader in




1KOSMOS
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Airside – Digital Identity App

Airside was founded in 2009 and is based in Herndon, Virginia, US. Its product – the Airside Digital Identity App – provides a reusable verified digital ID to individuals, comprised of their driver's license, passport, COVID vaccination record and/or other identifying attributes, for use in travel, security, finance, real estate, and workplace authentication and access. The solution allows users to enroll and store verified digital credentials within a user-controlled app-based digital wallet, then consent to share only the required data with the relying parties for remote or in-person exchanges.

Reusability is enabled with a mobile app that verifies, onboards, and stores identity information. The data is encrypted at rest on the user's mobile app and during transit; enrolled data is never stored in a centralized database. Once the digital ID is created, the experience is integrated across multiple waypoints. The digital ID is specific to each customer and follows the ISO 18013-5 for Mobile Driver's License (mDL) and verifies identities at NIST 800-63-3 with IAL2. This method can be used to replace physical transfers of data, such as physically handing over a passport for inspection. In some use cases, reusability is extended with workplace access use cases, enabling users to enroll document and biometric information for future site access, using previously verified biometric information as an authentication factor. This could be extended for use in step-up or risk-adaptive authentication use cases. Reusability is limited at this time to the customer's own ecosystem – for example, a user can onboard with one customer's mobile identity app for use with that customer but is not able to use that onboarded identity with a different verifier, customer, or ecosystem.

Users download the Airside mobile app, verify their driver's license or passport, and onboard a facial biometric template to match with the photo identification. In a travel use case, the users can link to their existing travel advantage customer account, such as their airline membership number or TSA Pre-Check Known Traveler Number (KTN). This creates a verified attribute that is stored in their mobile wallet app and digitally signed by Airside and third-party verifiers or issuers with their private keys. The digital credential can be presented at waypoints in US airports, such as a TSA checkpoint or an e-gate to board a flight and verified with a real-time selfie by the onsite verifier's hardware device. When the user is ready to present their identity at a TSA checkpoint, the user generates a QR code in the app to establish a connection with the verifier device via the issuer's public key. The user receives notice of what information is being requested, consents to share it, takes a selfie with the verifier hardware device, and is verified.

Identity verification for onboarding is currently conducted with the DMV or with the cryptographic information on the embedded chip of a biometric passport with the support of Thales and Acuant. Document verification has coverage for all ICAO passports with embedded chips, and the capacity to verify identity documents from over 200 countries. Airside uses an API-forward model, with REST APIs being used for the relying party/verifier to create conditions on how to use personal information and as a conduit for users to share information with content encryption keys.

Airside offers its solution as a cloud service. All data is stored on the secure enclave of the user's mobile device. Airside follows the Kantara Initiative for consent receipt and presents users with a summary of additional information including the date, expiration date, terms, processers, recipients, and purpose of the transaction. Users can revoke consent, with an activity log maintained of actions.

Airside

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

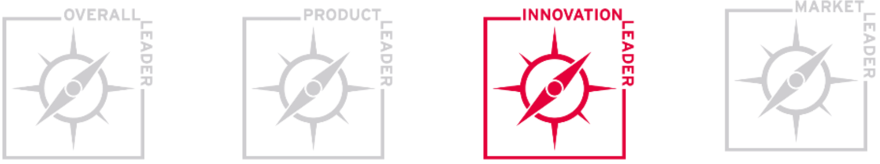
Strengths

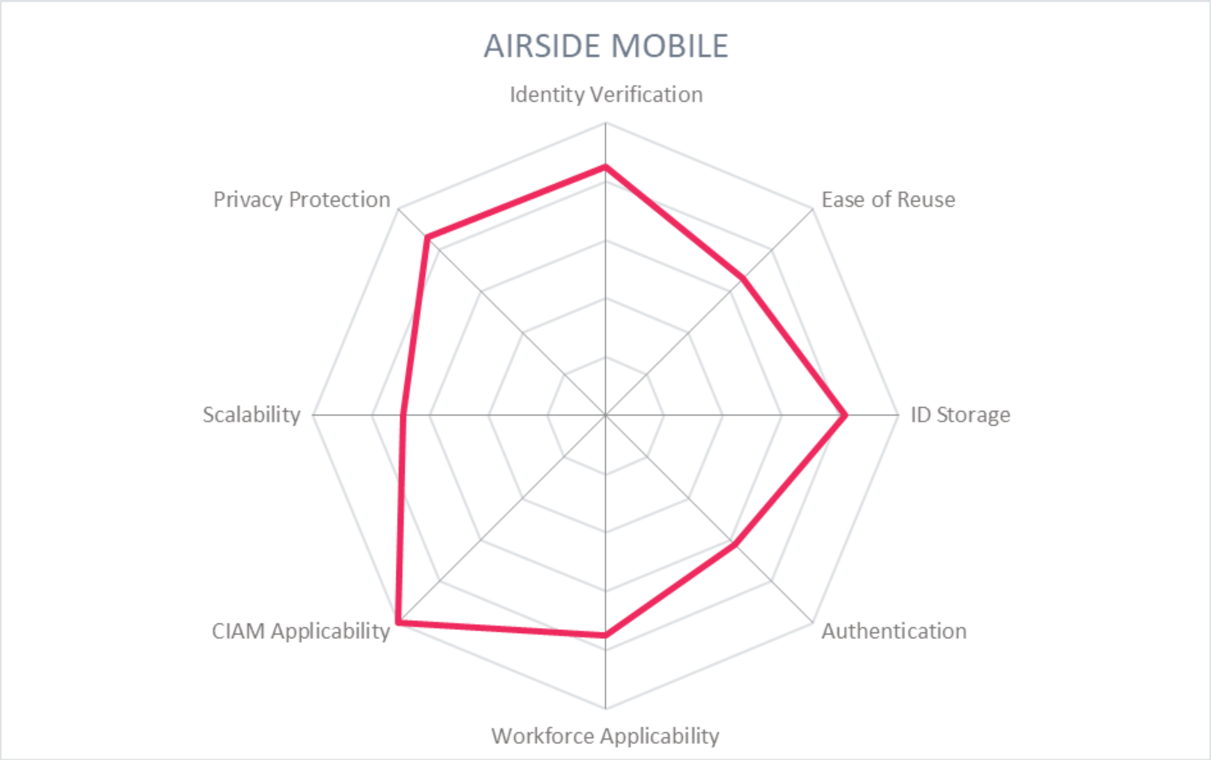
- Follows Kantara Initiative for consent receipt
- Certified Kantara NIST SP 800-63-3 (Technical), Component Service at IAL2
- Adheres to ISO 18013-5 for mDL
- OAuth2 and WebAuthN are supported with OIDC flow being added
- SOC2 Type II certification
- Reuse supported with a user-held wallet for one-time identity enrollment
- Reuse is supported with verified biometric information as an authentication factor
- Strong case for reuse by the credential issuer's ecosystem
- Storage of credentials is user-centric

Challenges

- Credential is stored as a unit (passport) instead of derived separate attributes (name, passport number)
- Product could benefit from offering step-up or risk-adaptive authentication
- Only run in AWS environments
- A growing company with limited global presence
- Primary travel use case is limited by hardware verification devices
- Reuse could be expanded to independent verifiers and customers

Leader in




AIRSIDE MOBILE
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

AvocoSecure – Avoco API

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 Avoco API to deliver verified identity services, packaged as an Identity Network Layer: Trust-T. Avoco is agnostic to where an identity resides, be it wallet-based or sourced from identity attribute providers. Its regional focus is on the United Kingdom but has compatibility with some Western European countries and plans of expansion.

Reusability is enabled by using existing verified identity data, and when necessary, completing document verification and biometric matching to bind that data to an individual, or additional identity attributes can be gathered and verified on-the-fly. Avoco is a flexible, non-wallet option that still enables users to reuse verified identity information with a variety of organizations and ecosystems. Customers are able to access verified identity data from a variety of authoritative sources from a single identity network layer and can use Avoco to uplift the identity assurance level of data from other proprietary wallets. Users have the benefit of reusing already verified information without having to store and manage it themselves.

Avoco uses its identity network layer, situated between sources of data and relying parties to enable identity collection from trustworthy sources for verification, authentication, consent management, and account management. 25 different verified attributes can be pulled and shared with relying party customers. Levels of trust and industry standards like the UK GPGs can be attached to any given attribute and can be applied dynamically using java scripts on a per-transaction basis. A relying party customer, for example a bank or a retailer, selects which trusted identity providers – connected via Avoco's API to the Trus-T identity network layer – to use for onboarding and authentication. The user is then prompted to onboard with the selected identity providers, typically a bank ID. The relying party is provided with proof to verify the provenance and assurance level of the identity data, and whether the attestation was tampered with.

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 network layer is rule-based for dynamic response, able to customize requirements such as selectively calling the necessary identity attributes for that customer's transaction. User also have the ability to set rules, for example selectively disclosing information, obfuscating it, or using differential privacy. Connections to decentralized ledgers for storing the user's assurance level for future use is also possible.

Flexible deployment options include on-premises, cloud, or managed service. The identity network layer is hardened against several vulnerabilities such as SQL Injection. No data is stored with Avoco but stored based on the customer's requirements. A partnership with Thales supports with identity verification and PSD2 hosting. 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.

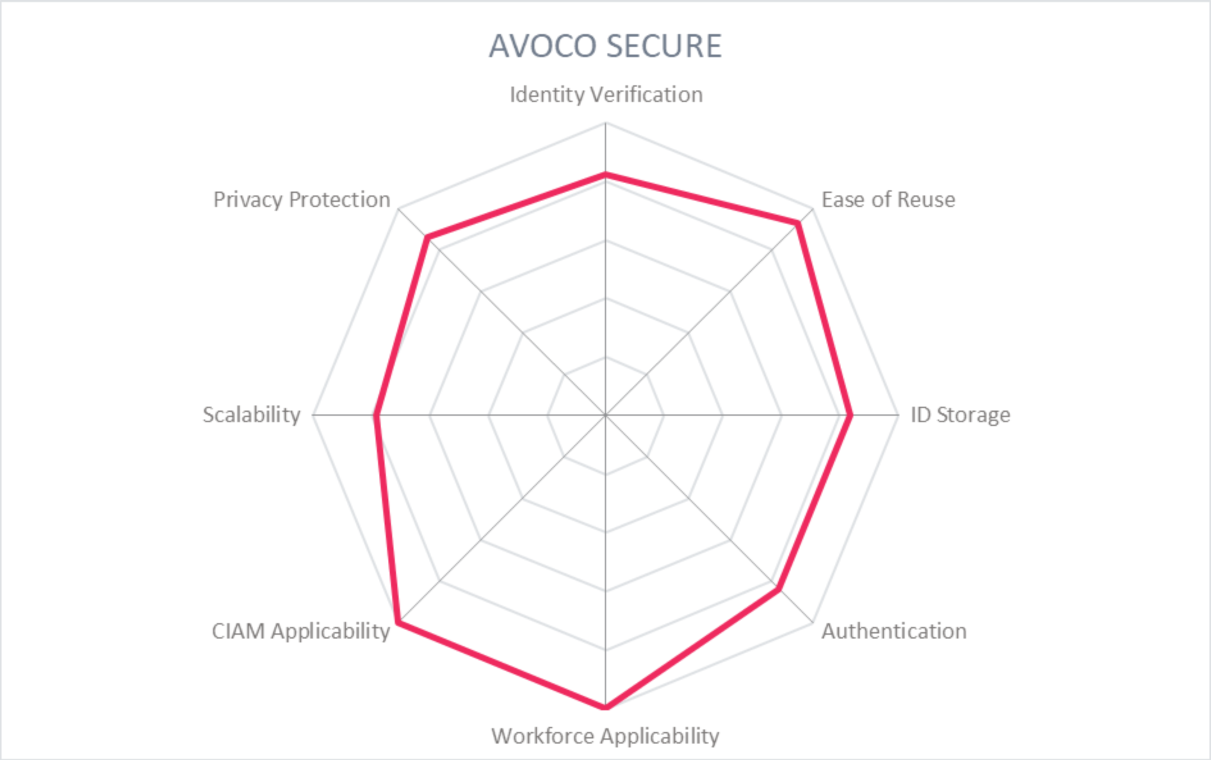
Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

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
- Users as well as relying parties can set rules for information disclosure

Challenges

- A focused solution for the UK with limited support for Western Europe, with wider expansion as a long-term goal
- No app SDK, app solutions are via an app provider integrated with Avoco API
- Small but innovative startup with potential


AVOCO SECURE
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

esatus – SOWL

Founded 1999 in Langen, Germany, esatus provides an enterprise self-sovereign identity suite specializing in authentication and authorization. Its product, SOWL, has an architecture that enables an organization to be their own IdP for the workforce. SOWL 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.

Reusability is achieved by verifying and/or issuing individuals, including members of the workforce, credentials, held by the user for authentication and authorization. Verifiable Credentials from any issuer, be it private or public, can be used. The solution uses principles of self-sovereign identity (SSI), enabling the end user to hold their credentials 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 credentials with attributes such as organization, group, department, static location, and others. These credentials are supported by W3Cs DID standard and Hyperledger Indy AnonCreds, with the private key and credential stored in the user’s wallet and the public key of the issuing organization made publicly available on the ledger for continual verification. Credentials issued by the organization can be managed in the organization’s backend system with a revocation option.

Once the employee has been issued their credential(s), it can be used for authentication and authorization to the employer’s systems or in any other system of a third-party that is interoperable with the selected standards. In an authentication scenario, a user would scan a QR code and be requested to share specific attributes from one or more 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. These credentials can also be used in cross-organizational consortium or collaboration projects, enabling employees from multiple organizations to access shared resources.

SOWL offers a fact-based identity management process, removing provisioning, request and approval processes. SOWL 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 SOWL to interact with other decentralized identity providers and ecosystems. No personal data is stored on the distributed ledger. Although SOWL does not directly provide identity verification, it is an important architectural step to bring verified reusable identities for use in the workplace and other use cases. Although SOWL 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	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

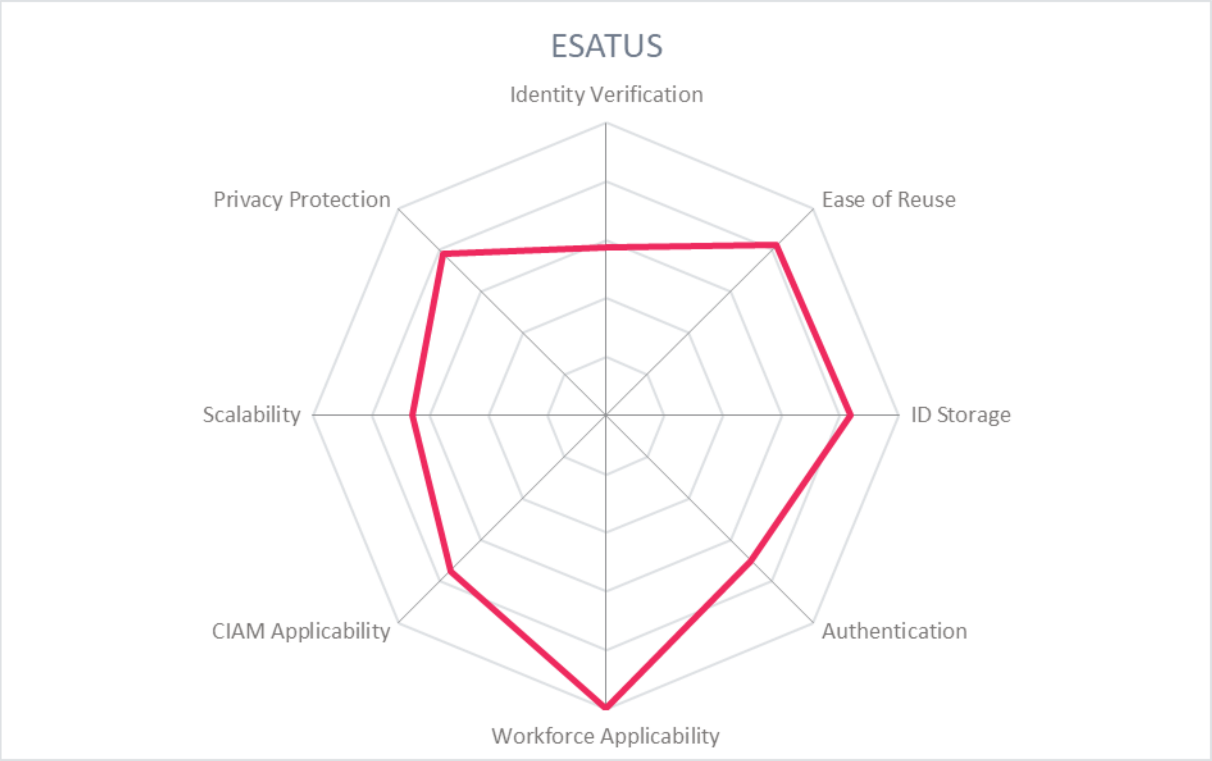
esatus

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
- Does not specifically address KYC and high LoA use cases
- Wallet compatibility is limited to Hyperledger Aries implementations


ESATUS
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

IDEMIA – Digital ID

IDEMIA is the product of a history of mergers and acquisitions with over 70 years of experience in identity. It exists in its current form since 2017, and is headquartered in Paris, France. IDEMIA works with governments and businesses to provide secure identity services, including issuing citizen identity documents, smart cards, biometric terminals, SIM cards, and identity verification. The Digital ID ecosystem serves governments with several nation-wide deployments including USA (with Oklahoma, Delaware, Arizona, Mississippi, with others to come), Colombia, Chile, France, and Morocco. It also serves commercial enterprises and particular use case groups like law enforcement and the US Transportation Security Agency (TSA), and covers identity proofing and verification, digital wallets and integrations, orchestration layers, and more.

Reuse is supported by making a digital identity available for sharing and verification in either a centralized system or derived from the systems-based approach for access via a mobile ID wallet. IDEMIA is active in providing citizen IDs that can be used in public contexts, and is expanding this with joint standardization with ICAO, ISO, ESSIF, NIST, opening reuse of citizen IDs to many more industries and use cases. IDEMIA offers varying licensing models influenced by per-transaction pricing, level of assurance and frequency of reverification.

The Digital ID suite covers many offerings and modules, one of them being the Identity Proofing and Verification which leverages top NIST ranked in-house and partner technology for document and biometric verification along with confirmation against authoritative systems of records. The user first scans their identity document with a mobile device, where various fraud checks are made for known forgeries, screenshots, holograms, fonts, image manipulation, and more. IDEMIA provides worldwide coverage for multiple types of identity documents, including passports, driving licenses, residence permits, etc., and has the use of OCR and NFC. The data from the document is extracted and checked against the appropriate system of record, including national registries, credit bureaus, telecom, banks, watchlists, sanctions lists, and PEP lists. The user takes a selfie, conducts a liveness (also known as “presentation attack detection”) test by following a prompt to nod their head. If necessary, synchronous video verification and other manual methods can be added to the user flow.

IDEMIA’s biometric face matching algorithms are regularly tested by NIST FVRT, with high performance and low-undetected demographic variance. For Digital ID usages, biometric facial recognition is only used in a 1:1 manner. The verification products are able to achieve NIST 800-63-3 assurance level 2 and eIDAS High. User data is stored either in the user’s mobile device, or in an authoritative system of record, and any data used during an identity verification session is deleted in the IDEMIA backend after the transaction. Attribute verification is done through checks against national registries, verifying Verifiable Credentials, and aggregating data from authoritative sources such as credit bureaus, telecom, banks, watchlists, sanctions lists, and PEP lists.

A digital identity that has been onboarded can be stored in a user mobile wallet. This can be provided by IDEMIA, integrated with web or native SDKs with customer applications, or utilize commercial wallets including OEM device manufacturers. In person and online identity verification and identity data exchange can be facilitated. To share identity information with a relying party in-person, the user opens their wallet app and selects “share ID” and a QR code is presented for the relying party to scan. The relying party uses IDEMIA’s Verify App (or SDK for custom integration) to scan the QR code and establish a secure communication channel. The user views and approves the identity attributes to be shared with the relying party, which are sent to the relying party using BLE upon approval.

The Verify App validates the incoming data, selfie, and other collected information needed during the transaction. To share data and verify the user remotely, the user scans a QR code on the relying party’s website to initiate the verification. The user receives a request on their mobile wallet to approve the selected identity attributes to share. The user journey is based on the level of security required by the relying party and could include a selfie and liveness detection or other aspects. The user journey can also be adjusted to suit authentication use cases.

IDEMIA’s products are available on premises and as SaaS. Support for Verifiable Credentials is being built out, as well as support for other decentralized wallets. IDEMIA’s identity verification solution and experience in the identity issuance and verification space make it a strong option for a full-service provider of verified identity.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

IDEMIA

Strengths

- ISO 27001 compliant
- iBeta PAD certified for level 1 and 2
- Regularly test for bias and demographic variance in algorithms
- In-house technology for both document verification and biometric verification
- Multiple options for authenticators, supports risk-adaptive authentication
- Enables user-controlled identity on user devices
- Supports NFC for embedded chip reading
- Supports synchronous video verification
- OAuth, SAML, OIDC are all supported
- Uses in-house facial recognition algorithms tested by NIST FVRT

Challenges

- Could expand risk-adaptive authentication to include network profiling and behavioral biometrics
- Fraud reduction offering requires customization, could be strengthened with use of a risk analysis engine
- Could support SIEM connectors

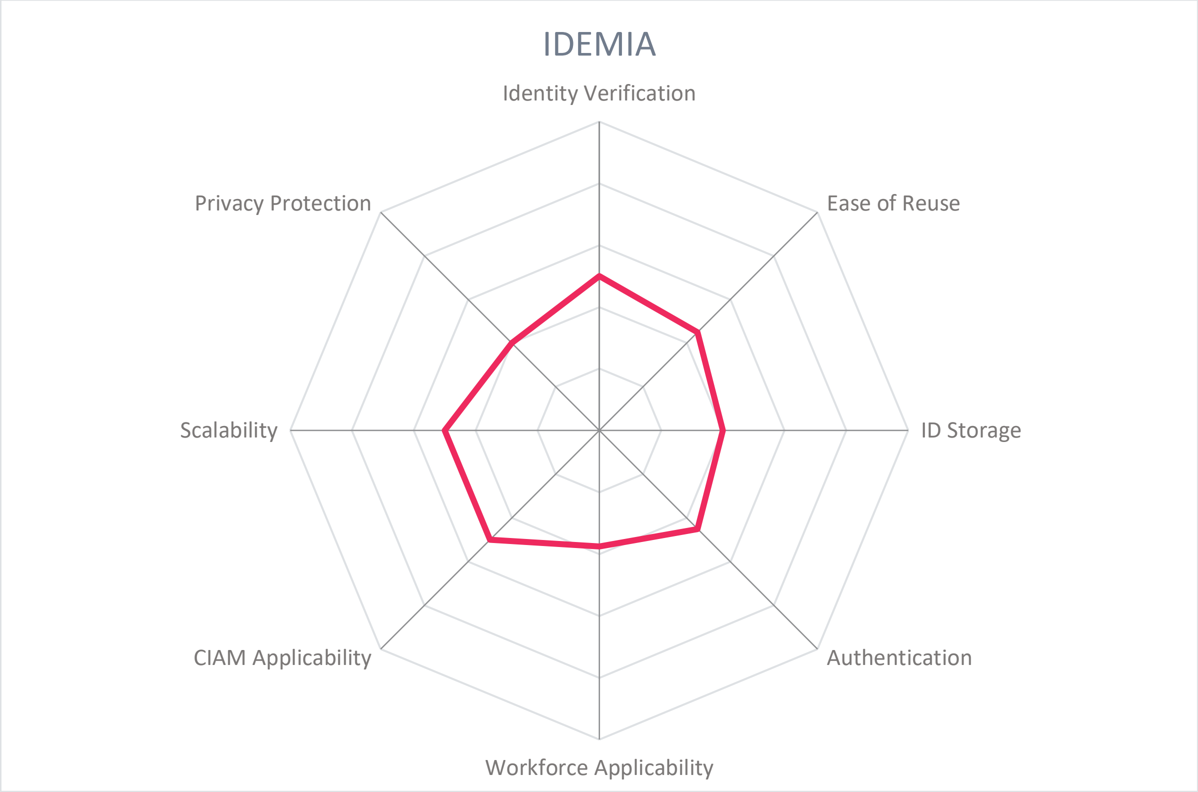
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


IDEMIA
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

InfoCert – Dizme

InfoCert was founded in 2008 and is based in Rome, Italy. InfoCert is the initiator of the Dizme Foundation with several contributors to bring the Dizme product to market. It is a decentralized identity platform that provides enrollment, credential management, authentication, wallet functionality, and APIs and/or widgets for issuers and verifiers. InfoCert assists customers to transform their existing information into a decentralized format through becoming an issuer, or to benefit from verified reusable identity by becoming a verifier for consumer and workforce IAM use cases.

Dizme enables reusability for users to gain access to physical locations, digital signing, and authentication by presenting a verified identity credential. The user-held wallet is central to the solution and can be leveraged via an SDK (free license), as a white-labeled app, or customers can choose to use a proprietary wallet. The wallet establishes a connection with the Dizme stack to issue a credential. Because many issuers and verifiers can issue or verify credentials from the same wallet, users are able to use their onboarded credentials in numerous ecosystems.

Identity information that is being onboarded can be verified and can achieve eIDAS level Substantial. A user begins by onboarding and verifying their email, phone number, and conducting a selfie with active liveness detection. Passive liveness can be optionally added in the SDK version, with attack detection features and biometric authentication. Next, the user conducts identity verification for government-issued identity documents and facial matching. Identity verification is carried out with InfoCert's proprietary technology for Italian documents and uses partners for global coverage. To advance to a "Trusted Assure" level, InfoCert verifies the user's eID, an existing digital signature, or authenticate against a bank and account information. An option for an in-person verification also exists. The wallet can establish a web endpoint that implements OpenID Connect to create a triangle between the wallet holder and the relying party without requiring an issuer API to be implemented. Encrypted messages between parties is enabled.

Verified and onboarded identities can be segregated into separate digital assets controlled by the users, including citizen, consumer, student, employee, corporate account and Legal Entity Identifiers (LEIs). Licensing options exist for organizations wishing to issue credentials and/or verify credentials. The platform facilitates issuer-verifier transactions – where an issuer earns for every verification performed on a credential it issued – while protecting the credential owner's privacy. This is done through a second layer decentralized network which, during a verification, points only to the decentralized identifier (DID) of the issuer for payment without releasing any information on the credential holder. Preventing the verifier from gaining insight into the issuer would provide additional privacy protection.

Options exist to deploy the Dizme stack on-premises, as a cloud service, or as a managed service. Dizme is based on Hyperledger stack using Indy, Aries, and Ursa. The credential format currently used is Anonymous Credentials (AnonCreds). It currently leverages Sovrin as the decentralized network for transactions but could adapt to any Indy-based network with plans to support EBSI and KERI frameworks in the future. Dizme uses the Trust Over IP (ToIP) framework. The wallet solution is produced with open-source contributions.

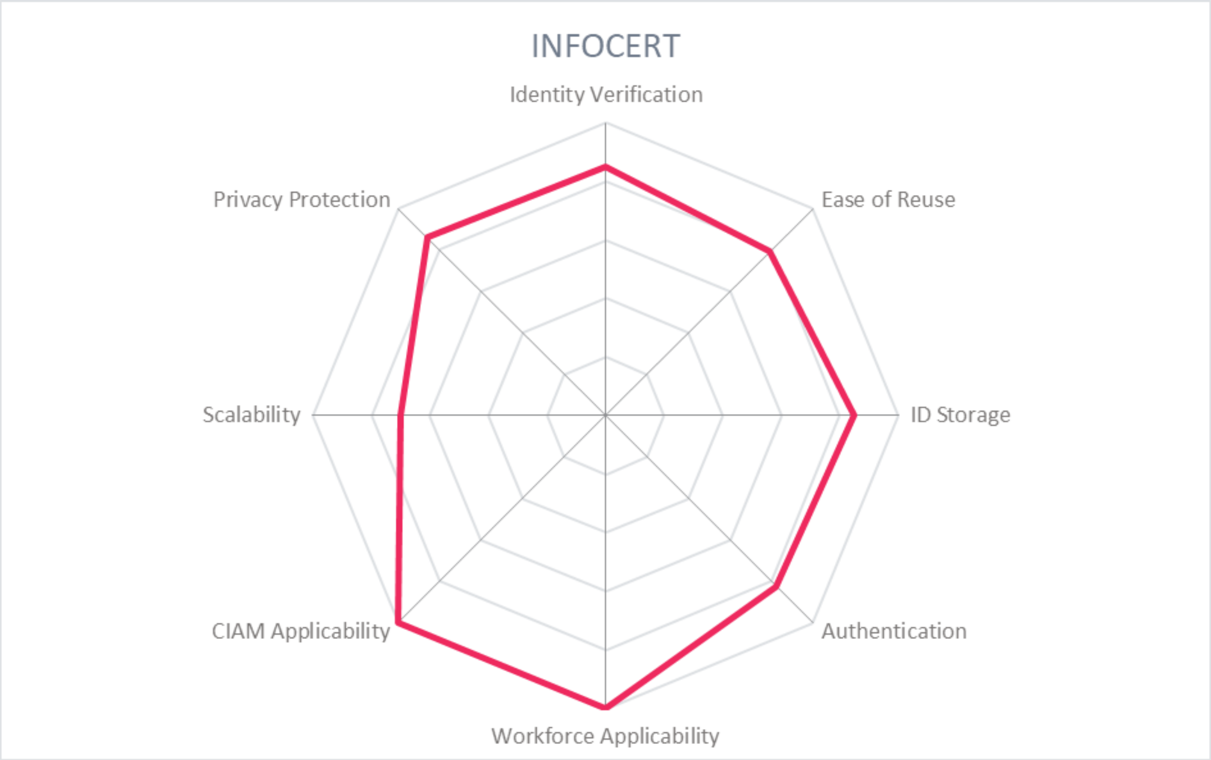
Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Strengths

- An issuer-verifier payment model with privacy-preserving functions
- A Qualified Trust Service Provider (QTSP)
- Support for contextual identity and multiple personas
- Flexible deployment options
- Allows for credential issuance at various assurance levels
- Compatibility with LEI and AnonCreds
- ISO 27001 certified
- Flexible wallet options

Challenges

- Device synchronization is not yet offered
- Wider support for authentication standards such as OAuth2, SAML, and JWT could be supported
- Connectors to SIEM or a security analytics service could be added
- Blockchain scalability is a novel topic


INFOCERT
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Liga – GlobalID

Founded in 1999, Liga is based in Denmark. Its GlobalID product is a cybersecurity platform to harness trusted identities for enterprise workforce use. To build a connection between a company account and a citizen identity, GlobalID connects identity sources with validation systems, authentication factors, and identity providers (IdPs). With GlobalID, organizations validate the identity of their workforce against data that suits the Level of Assurance required, including passports, eID, and video identification. Authentication tokens are then issued by external or internal Certificate Authorities (CAs) or can get verified against existing systems like Azure MFA.

GlobalID enhances the digital lifecycle through reuse of validated identity data for workforce onboarding, active use, and review of the identity at the organization. Authentication is the main focus of reuse with GlobalID, making use of validated identity information to provide tokens or certificates for use as authentication factors. The licensing structure is a combination of fixed and per-user pricing.

The organization determines the rules and LoA that is required for user groups, with automatic tasks assigned to validate identity attributes, issue a smart card, and so on. Data sources from the company network such as HR, AD, Microsoft Active Directory, Micro Focus eDirectory, SAP, etc. are connected to the GlobalID virtual appliance. Data is synchronized in real time from the chosen system to create a record which will be validated for future use. This identity data synchronized from the identity source is validated against third-party eID providers or other third-party identity verification partners conducting passport and video identification.

After the identity data is confirmed to represent real data, an identity record is created with the help of automatic user onboarding with rule-based logic. This logic is based on each company's own requirements, which will vary per organization. In addition to utilizing the eID and other authoritative sources, manual identity approval can be completed if the organization requires it. Thus, the emphasis is on identity validation, with identity verification occurring only when eID and other authoritative sources of identity data need to be supplemented.

After validation of the identity record is completed, a validated digital identity is issued as a certificate or other token to the individual by the authority. The validated digital identity can be used for use in two-factor authentication. According to the organization’s requirements, secure MFA tokens can be ordered for the user automatically, manually, or based on group membership. Additional authentication factors such as FIDO2 token support, Microsoft Authenticator, and other authenticators are on the roadmap.

To add to the lifecycle management of identities, review of the identity validation history is available for compliance and governance. There is a clear auditable record of identity validations and event logging, as well as the ability to revoke and deactivate identities. Access rights can be given to an auditor with customized functions, such as read-only rights.

GlobalID is implemented as a virtual appliance on-premises or as a cloud system. The product user interface can be expanded and scaled through various Java applications for an administrative UI, a portal UI for differentiated processes or device orders, and a user UI for self-service functions including eID validation, account activation, certificate revocation and password reset. Backend integration is completed via REST API. Administrative access and configuration of the BPM process engine, event-based rule engine, and database objects and structures is provided.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

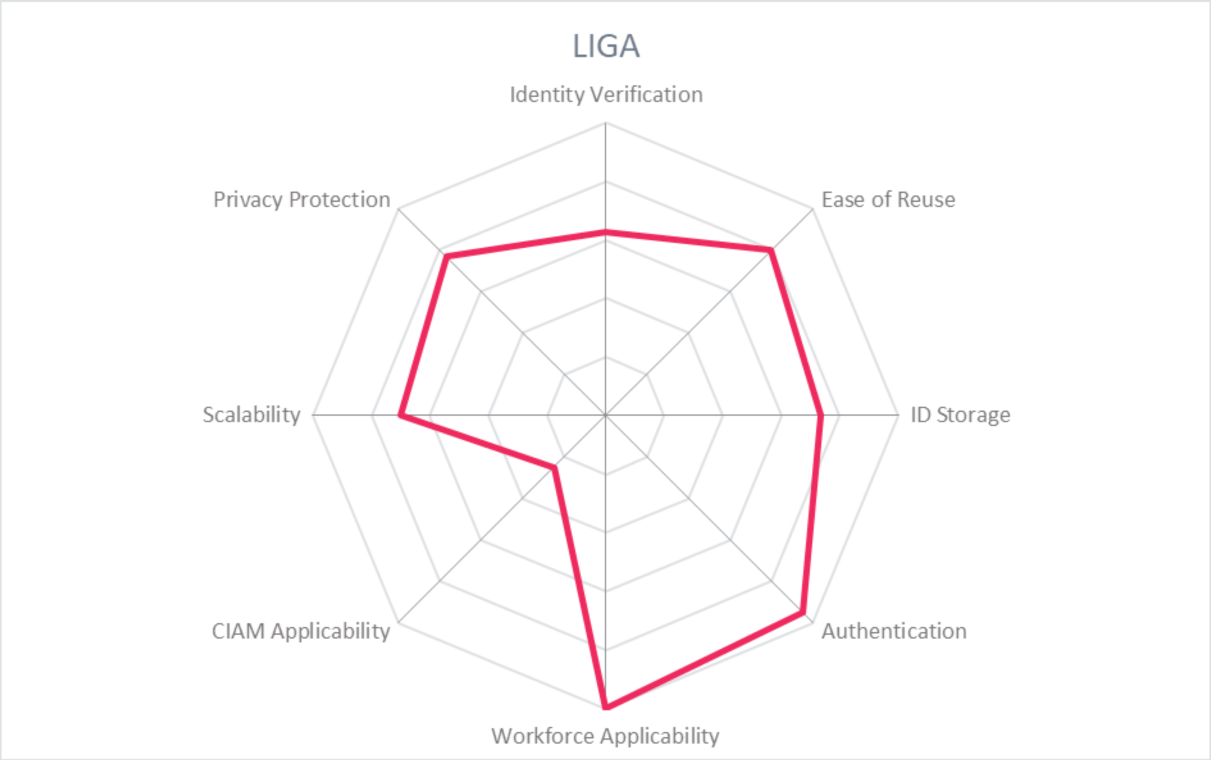
LIGA

Strengths

- Targets industries that prefer use of CAs or hardware authentication tokens
- Supports logging to external SIEM systems
- Supports contextual and risk-adaptive authentication
- Provides a wide range of validated authenticators
- Non-wallet option for verified identity reuse
- Focuses on IAM workforce use cases

Challenges

- Emphasis is on identity validation instead of identity verification through document and biometric verification, may limit geographical reach of solution
- Relatively small vendor with presence currently only in EMEA
- Secure, but non-user-centric storage


LIGA
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Microsoft – Microsoft Entra Verified ID

Microsoft, founded in 1975 and based in Redmond, WA, USA, is a familiar figure in hardware and software, digital services, and cloud infrastructure businesses. In August 2022, Microsoft released Microsoft Entra Verified ID product (based on Verifiable Credentials and Decentralized Identifiers) as generally available after over a year in public preview. Its Entra Verified ID product enables peer-to-peer, B2C, and B2B verified credential issuance, storage, exchange, and verification for consumer and workforce use cases. Through its contributions to open-source DID and Verifiable Credential standards, Microsoft enables reusable verified identity for use in Azure Active 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 and accept Verifiable Credentials (VCs) for users, employees, partners, etc. These VCs can be supported by identity proofing that is conducted by partners for document verification, biometric verification, and liveness detection for the customer’s desired level of assurance. 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.

Reusability is enabled by building up an ecosystem of interoperable, user-held credentials, which are verified to the level of assurance required by the use case. Credentials that are issued by organizations are held in the user’s Microsoft Authenticator app (functioning as the user’s digital wallet), and the user is able to use them with other unconnected organizations that use the Microsoft Entra suite or with providers that have built interoperability with Entra Verified ID such as Ping Identity. Reuse of the credentials is also supported by the Verified ID Network, which is a list of all organizations that issue Entra Verified ID credentials and is visible and available to all issues and verifiers. Organizations can use the Verified ID Network to search for and accept credentials issued by other organizations, allowing for easy reuse of issued credentials by the business for onboarding and authentication purposes. Entra Verified ID is currently included with any Azure Active Directory subscription.

To issue a VC, the organization federates to the organization’s IdP to authenticate the user, establishes a per-organization identifier, and processes the identity attributes to be included in the VC which can include government-issued documents, facial and/or fingerprint biometrics, liveness, or other attributes. The result of the ID proofing flow is the issuance of a Verifiable Credential to the user, employee, or partner for reuse with the issuing organization or with external organizations. In a remote onboarding use case, an organization using any IdP hires a remote employee who is sent a link to the Employee Portal for onboarding. The employee verifies their identity with a combination of document scan, biometric, and liveness detection and requests their employee ID card. The employee scans a QR code creating a secure connection to their Microsoft Authenticator app, and the employee credential is sent and stored in the user’s device.

The enterprise manages access rights from the Azure AD-integrated Verifiable Credential service, and employees can request access to resources with their employment credential. The organization has the ability to define the identity attributes required for specific interactions, such as authentication to a particular resource. 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, with the Microsoft Authenticator app also functioning as a digital wallet.

The product is a SaaS service able to be deployed on all major cloud platforms. DIDs are anchored in ION, an open, public, permissionless Layer 2 Decentralized Identifier network, as well as web servers and did:web. 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	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

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 interoperability groups
- Supports multiple DID methods
- Recovery of data possible with mnemonic phrase
- Emphasis on ability to resolve Verifiable Credentials from other issuers
- Revocation of credentials is possible
- Certifications including ISO 27001, PCI-DSS v 3.2, SOC 2, HIPPAA, WCAG 2.0
- Provides QuickStart to enable companies to easily discover issuers and verify credentials

Challenges

- Demonstration of strong interoperability and usability must be seen beyond its public preview
- Does not support contextual and risk-adaptive authentication
- Policy-based authentication approach using verified identity attributes could be supported
- Support for OAuth2 and SAML could be provided

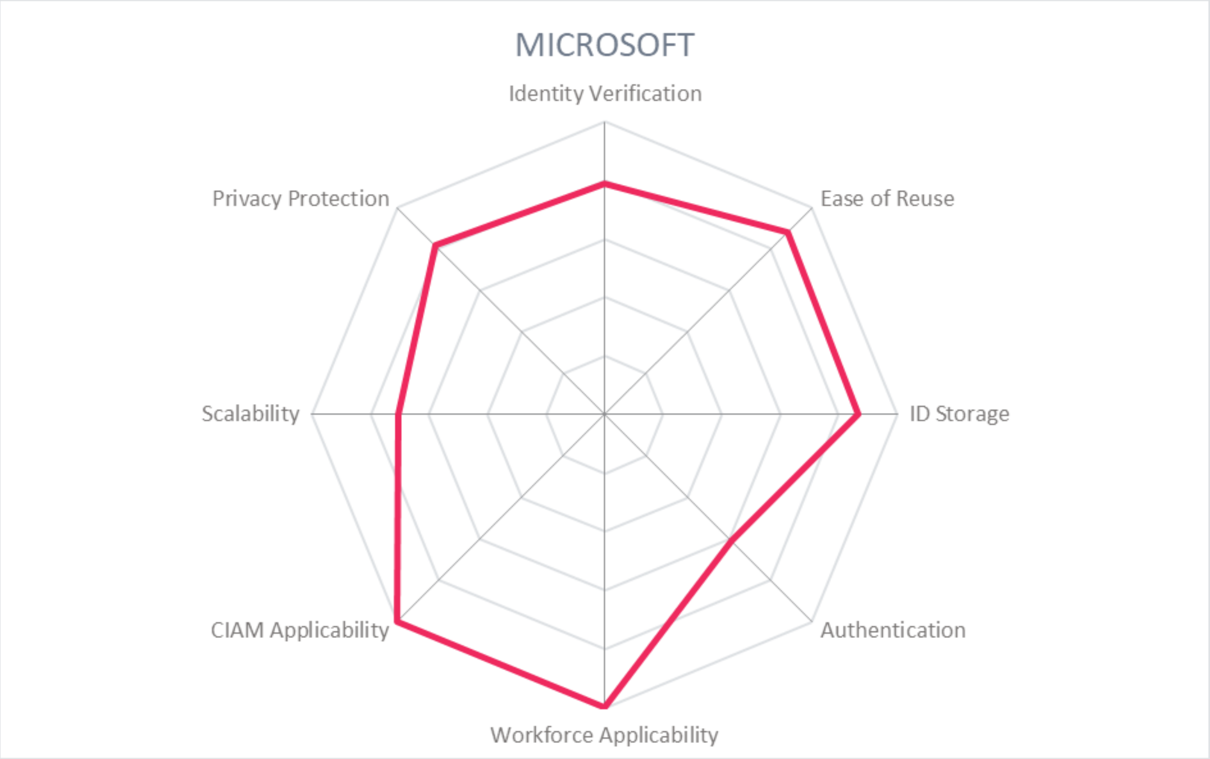
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


MICROSOFT
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

OneID – OneID

Founded in 2019, OneID is a UK-based ‘identity fintech’ vendor (OneID is a trading name of Digital Identity Net U.K. Ltd.). Its product OneID is a bank-enabled digital identity, facilitating onboarding and authentication using verified bank processes and profiles. It is specifically focused on serving the UK as an identity scheme (similar to the Nordic BankID schemes), leveraging the already high usage of online banking, accessible to 40 million individuals, to provide verified identities in other consumer IAM use cases.

OneID uses the identity information held by UK banks to verify and authenticate users to relying party services. The OneID platform works with identity providers (IdPs), being banks located in the UK. These provide verified account information, strong customer authentication (SCA), biometric authentication, fraud monitoring and other security functions that can be input into a relying party’s KYC and AML processes. The platform also connects relying parties that require verified identities during onboarding, authentication, or uplift during high-value transactions. This network of relying parties includes DocuSign, Shopify, WooCommerce, and those in the finance, entertainment, retail, e-signing, and sports sectors. Attributes can be additionally verified with UK government services, credit agencies, and other attribute providers. OneID can also verify email addresses and phone numbers during the onboarding journey.

Reusability is facilitated by leveraging the online banking ecosystem in the UK, allowing the user to use identity data that is verified by their online banking provider to enroll or authenticate with an unrelated service provider. By channeling the onboarding, age verification, authentication, or KYC flow through the user’s online banking environment, the user is not required to complete extra identity verification steps such as verifying an ID card or biometric matching (there is no need for an additional OneID account for the user). OneID serves to connect banks acting as IdPs with businesses that need verified identity information with a per transaction payment model with a portion of the benefits going to the IdP for providing verified information. For banks which choose not to serve as an IdP but still want to participate, OneID is certified as an IdP according to the UK Government’s ID framework. Since the online banking environment or banking app is reused and acts as a digital wallet, the user is not required to download an additional digital wallet app.

A typical onboarding flow begins with a user visiting a relying party app or site, and selecting “Register with OneID”. The user is then prompted to select their bank and to consent to sharing particular data attributes with the relying party. Upon consent, the user is routed to their bank login page where they securely authenticate. After successful authentication and confirming details in a bank screen, the user is sent back to the relying party site with the requested information. Registration or order forms are automatically populated with verified data sent from the bank site.

OneID is certified to the UK DCMS identity trust framework as an Identity Service Provider and Orchestration Service Provider, and is also a Scheme Owner. OneID leverages open banking certificates and financial-grade APIs (FAPI) to secure exchange between OneID and the IdP bank. Metadata, including provenance on verification measures behind each attribute can be shared as well (using OpenID Connect Identity Assurance), signed by the IdP bank to ensure validity.

It is a cloud-native platform with multi-tenancy. While the robust verification and fraud reduction capabilities are provided by the IdP banks, OneID enables enterprises to leverage the verified identities for consumer onboarding and authentication. OneID partners with DocuSign and other e-signing solutions to enable electronic signature use cases. With capacity to expand regionally (by connecting to other national ID schemes), OneID is a compelling option for those looking to leverage online banking for verified identity.

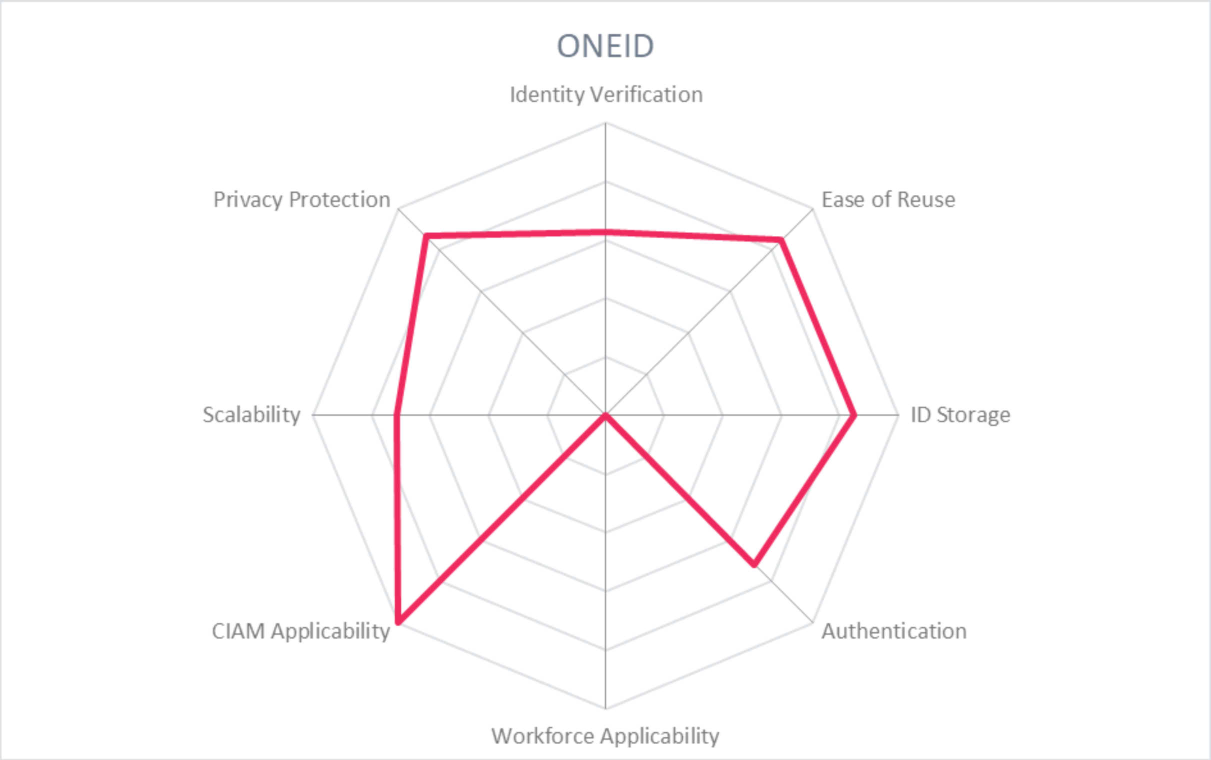
Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Strengths

- Supports DCMS GPG45 Medium and High levels of assurance
- Support for OpenID Connect is provided
- FAPI is used in open banking protocols
- No digitization of physical documents or selfie is required
- Growing ecosystem of relying parties in the UK
- Supporting and involved in the GAIN initiative
- Serves age verification use cases
- B Corp certified
- Contributing to open standards via OIDC IDA

Challenges

- Could offer connectors to SIEM
- Focused on serving the UK market only


ONEID
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Ping Identity – PingOne Verify and DaVinci

Ping Identity was founded in 2002 and based in Denver, Colorado. It specializes in solutions for IAM and CIAM, and its products PingOne Verify and DaVinci orchestration engine allow the organization to conduct identity verification with a variety of document, biometric, and digital attribute evidence. Ping serves clients globally and is a main player in the identity market.

PingOne and the DaVinci connectors provide reusable, verified identity by verifying the user identity, issuing a Verifiable Credential (VC), and storing it in a user-held wallet – either provided by Ping via an SDK, or issuing the VC to a third-party wallet. Interoperability of the credentials is designed initially across Ping and Microsoft Entra customers, allowing users to reuse their Ping-issued VCs with service providers in both of those ecosystems. This will be extended to other wallet and credentialing ecosystems. PingOne customers are also able to verify credentials issued by other PingOne and Microsoft Entra customers.

PingOne Verify is Ping's own verification service that covers document verification, biometric verification, aggregation from additional sources such as credit reporting agencies and telecommunications and checks against international watchlists. These various proofing signals are collected and assessed to achieve the customer's desired level of assurance based on NIST 800-63-3, ISO 29003, and/or eIDAS standards and transform it into a digital credential. With the acquisition of ShoCard in 2020, PingOne Verify can integrate decentralized identity solutions into their technology stack that support W3C, DIF, decentralized ledgers such as Hyperledger Indy, and standards like the ISO 18013-5 mobile driving license. Depending on the customer requirements, the credentials can be used as workforce credentials or for CIAM use cases.

PingOne Verify conducts automated ID inspections by scanning the front and back of a government-issued ID with the user's mobile device, selfie-to-ID photo matching, and liveness detection. Documents that are supported include U.S. and international driver's licenses, ISO-based international passports, and European ID cards. An optional manual inspection of ID documents can support when and if automated decisions cannot be made. A decisioning engine, supported by manual inspection when necessary, determines the authenticity of identity documents and attributes and issues a proofing receipt. The proofing receipt and issued credential are bound to the device, and the related PII data is stored encrypted in the mobile device. 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, except where the issuer is using Ping's optional directory services for verified attribute storage. For example, in banking transactions, the issuing banks typically 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.

The identity proofing flow can be integrated into onboarding processes or later in the lifecycle as needed by the customer. Identity is verified and credentials are issued via a web browser or native mobile SDK (available for iOS or Android) or via compatibility for third party wallets. Further functionality is enabled with the DaVinci orchestration platform, which provides over

100 third party connectors to additional document verification, biometric matching, and fraud reduction vendors.

PingOne Verify is a SaaS service, integrated into Ping's identity platform backend and other services like PingFederate to verify the identity of new registrants or during authentication. The product can however be deployed on premises, as a SaaS service, or as a managed service. The administrative dashboard and webhook data delivery service provides insights into transactions, fraud indicators, reasons for rejected transactions, etc. 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, and all PII data that was passed to PingOne Verify or third-parties is deleted. A blockchain-agnostic sidechain to Hyperledger (private permissioned) or Hedera, Ethereum, GoChain, Stellar, or BTC (public)is used to facilitate credential issuance and validation, with plans to move to additional public blockchains.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Strengths

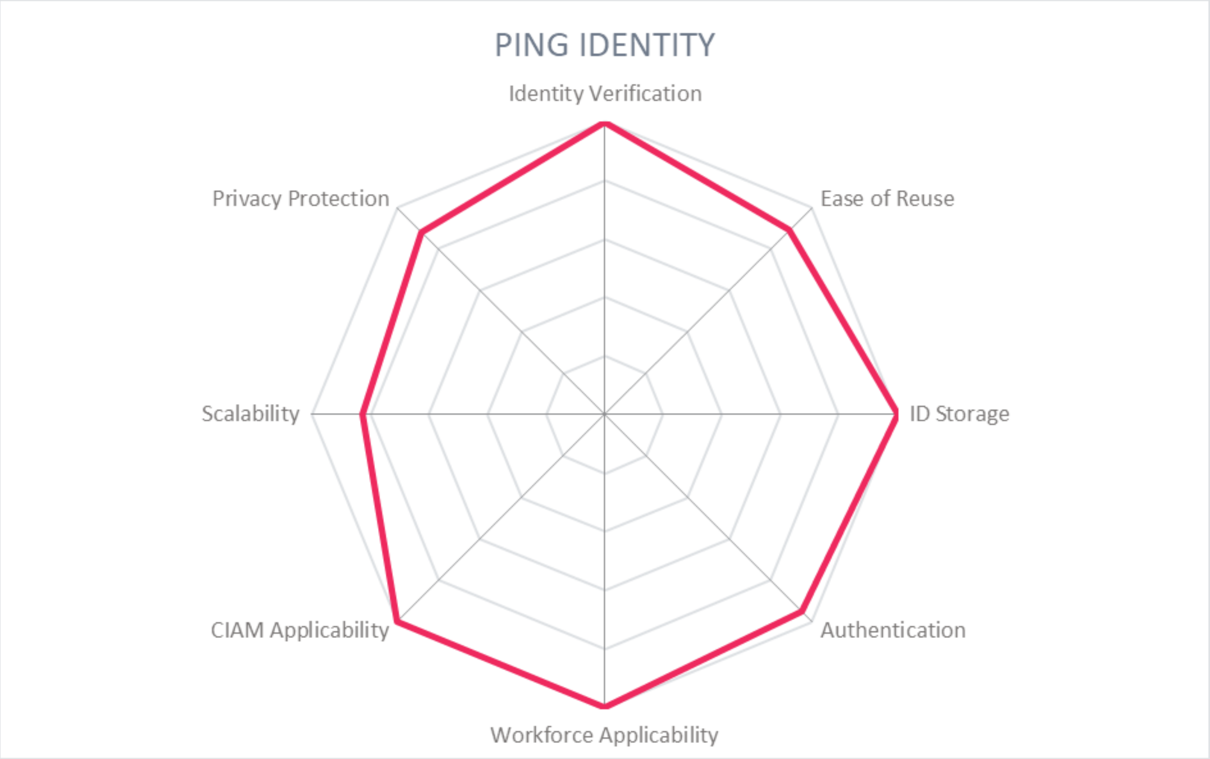
- Able to integrate identity verification into Ping's established platform
- Account and password recovery are possible
- Individual attributes such as date of birth or name are certified
- Ping provides interoperability with its large customer base
- Strong APIs and connectors to other SaaS services
- ISO 27001 and SOC 2 Type II certified
- Supports NIST 800-63-3, ISO 29003, and eIDAS for various levels of assurance
- iBeta Level 1 and 2 PAD certified
- Designing wallet and credential interoperability for a multi-wallet/multi-credential world

Challenges

- Proposes an ambitious and disruptive approach to onboarding, shifting from signup/sign-in to present and verify
- NFC reading of documents is not yet available in PingOne Verify
- Does not yet provide assistance for incident analysis and/or remediation
- Cloud infrastructure only available on Amazon AWS

Leader in

OVERALL LEADER · PRODUCT LEADER · INNOVATION LEADER · MARKET LEADER


PING IDENTITY
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Signicat – Digital Identity Platform

Signicat is headquartered in Norway and has been delivering identity solutions since 2006. The Digital Identity Platform facilitates the use of eIDs for a suite of Sign-up, Sign-in, and Sign-it products, directly supporting reusable models of verified identity. The platform enables the customer to leverage existing eIDs and verify user identities by orchestrating verification steps across many regional partners, packaging identity information and delivering it to the customer. The product suite leverages the verified identities of primarily European eIDs for onboarding, authentication, electronic signatures, seals, and time stamps for a variety of use cases and flows. Recent acquisitions of Electronic IDentification, Dokobit, and Sphonic expand remote identification capabilities, orchestration and fraud reduction, and increases their technology partner ecosystem. Signicat has a primarily European focus, but is expanding their global coverage particularly in the DACH region.

Signicat provides an identity hub for reading electronic IDs, electronic identity verification, and verified attributes. Signicat has over 30 integrations with primarily European eID providers, ranging from country schemas such as Nem ID and itsme to open banking ecosystem solutions such as Verimi and Yes. Signicat's Assure API normalizes attributes from the varying identity providers.

To cover identity documents beyond these connectors, remote identity verification is provided in-house by subsidiary ElectronicID or by partners such as ReadID, Onfido, Facetec and WebID. These use methods such as document scanning, biometric onboarding, liveness detection, and synchronous video verification with a live agent. To support attribute verification and registry lookups, Signicat connects with over 25 regional attribute providers. To conduct onboarding with compliant KYC/CDD checks, the identity is first proofed – ether using the eID connectors or with a remote identity verification flow – with attributes verified through authoritative records checks. Additional checks for politically exposed persons (PEPs), ultimate beneficial owners (UBOs), and sanctions lists support the KYC/CDD checks, with information on varying cross-border definitions provided to customers.

Customers are able to choose which in-house and third-party services are used to achieve the level of assurance required by their use cases. The customer's target assurance level for onboarding and authentication can be customized and determines the strength of verification. NIST Identity Assurance Level 2 and eIDAS high can be achieved with the solution.

By facilitating the use of either pre-existing eIDs that the user holds or verifying user attributes through the open banking ecosystem and third-party identity verification partners, Signicat makes a reusable verified identity ecosystem available to businesses. The verified identity is not only used once, but can be integrated into the onboarding or enrollment process and can provide verified identity attributes as authentication factors. The user can authenticate using a variety of authenticators, including eID or by using Signicat's MobileID, compliant with PSD2/SCA. The electronic signatures product allows the business to make electronic signatures available for a variety of use cases, supporting advanced electronic signatures (AES) and qualified electronic signatures (QES) linked to a verified identity. Signing can be enabled within apps, customer portals, CRM and ERP systems, or web chat interfaces.

The solution can be offered using all major cloud platforms, and supports OpenID Connect, SAML2, and WS federation protocols. With the identity hub model, Signicat does not hold any user eID data. Rather, it provides one API for the customer to access – in a two-way encrypted communication – any of the connected eIDs. Signicat's standardized APIs can be web-based or built into a customer application.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Signicat

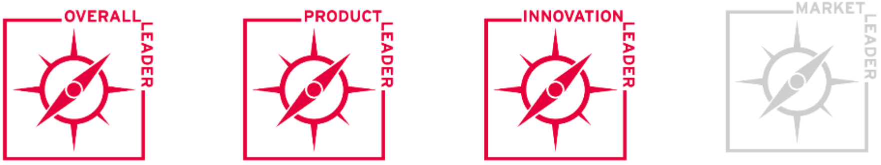
Strengths

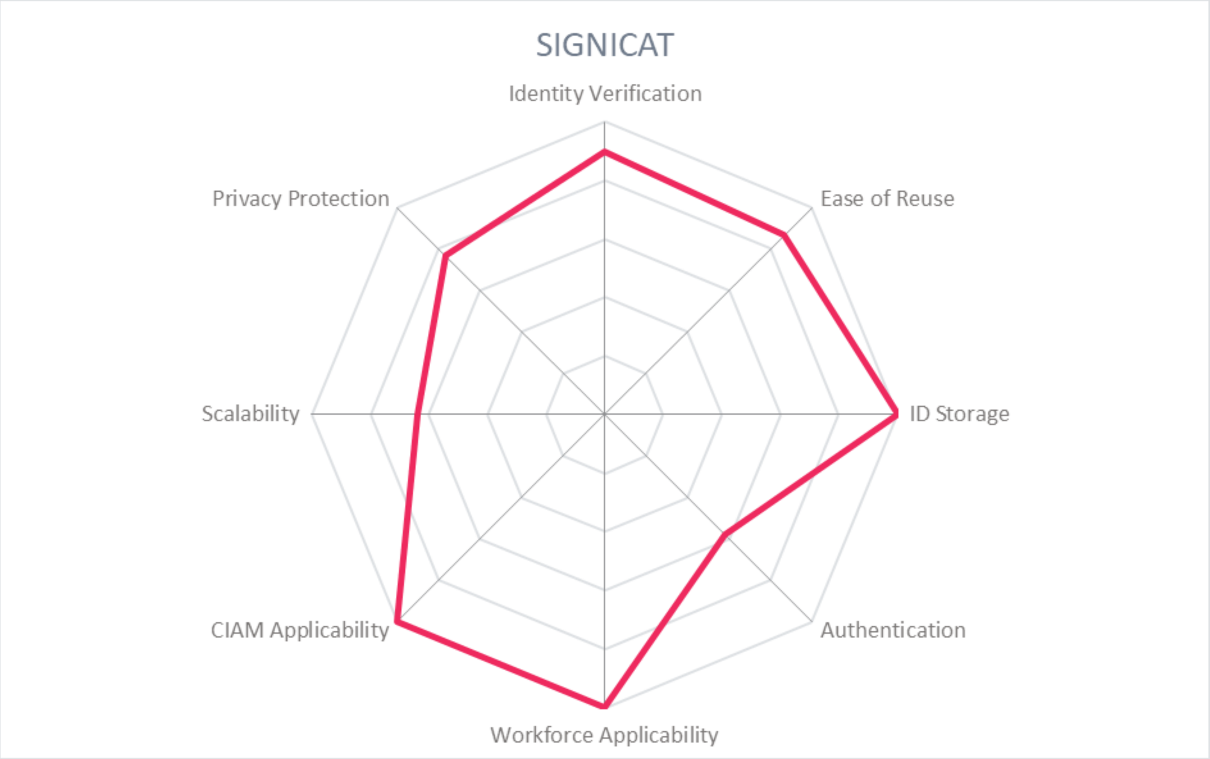
- API-forward architecture
- Provides access to eIDs with SAML, OpenID Connect, and WS federation
- Flexibility of third-party partners enable different assurance level schemas to be fulfilled
- Supports use of over 30 eIDs, including BankIDs for identity reuse
- Digital signing capabilities
- FIPS 197 and 140-2, ISO 27001, 27018, and SOC 2 certified
- Additional services like AES/QES
- Expanding orchestration capabilities

Challenges

- Solution could expand fraud reduction with device intelligence and user behavior analytics
- The solution could offer connectors to SIEM or security analytics services
- Not available on-premises

Leader in




SIGNICAT
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Sumsub – Sumsub ID

Sumsub was founded in 2015 and is based in the UK. Sumsub provides identity verification, transaction monitoring, and business verification. Sumsub covers over 220 countries and territories globally with over 6000 document templates, and focuses on helping clients to scale globally by providing high pass rates in such complex and emerging markets such as SE Asia, Africa, and Latin America. With a particular focus on fintech, marketplaces, cryptocurrency, and payments, Sumsub works with customers that have overlapping audiences to maximize the savings between sharing KYC and verified identity attributes.

Reusability is achieved by establishing direct partnership between Sumsub customers that have a large overlapping user-base, where KYC checks can then be directly shared between them. Potential partners first validate that they have a significant overlap of users. After a partnership has been formed, both partners verify and onboard users as usual with document and liveness checks, supported by fraud and AML checks in the background. When partner A requires a KYC check on a user that has already been verified by partner B, partner A requests a liveness check from the user which is compared against the full identity verification and KYC onboarding completed with partner B. A consortium approach is also possible instead of direct partnerships, which may accelerate the opportunities for reuse. The business model takes a pay-per-valid-user approach.

Verification flows are possible via API or SDK integration. The organization can customize verification flows for the document requirements per country and territory, which document, video and biometric verifications, attributes, and additional steps (such as a questionnaire) are required, and per regional regulatory policies as well. The solution is a combination of in-house verification technology including OCR for document proofing, facial liveness, and face match against duplicates and blacklisted faces. An API call is used to compare against watchlists. Partner solutions to deliver other identity verification functions for an orchestration approach.

An analytics tab is provided in the administrative dashboard to assess conversion rates, time spent at each step, and many other indicators. Application summaries of identity verifications are available in the administrative portal, including insight into why a verification may have failed. The risk level at which to flag a wallet and transaction can be customized. AML screening allows customization of lists to check against. The look and feel of the flow is customizable with whitelabeling options possible. There is 24x7 development and customer support available from Sumsub.

In an example flow where a user interacts with a Sumsub customer (Service Provider A) for the first time, the user signs up for a new service in a browser environment and is asked to complete an identity verification flow. User accepts to share their identity information as per GDPR requirements. The user’s location is determined via the IP address, and the user selects the document type that they will verify. Users are prevented from uploading cropped, blurry, or incorrect documents. Then liveness detection is done by taking a video selfie and moving the head in the instructed manner. When the user interacts with another Sumsub customer that has a partnership with Service Provider A, the user is able to complete the KYC/identity verification process by only submitting a liveness check, which is compared against the full KYC onboarding done by Service Provider A.

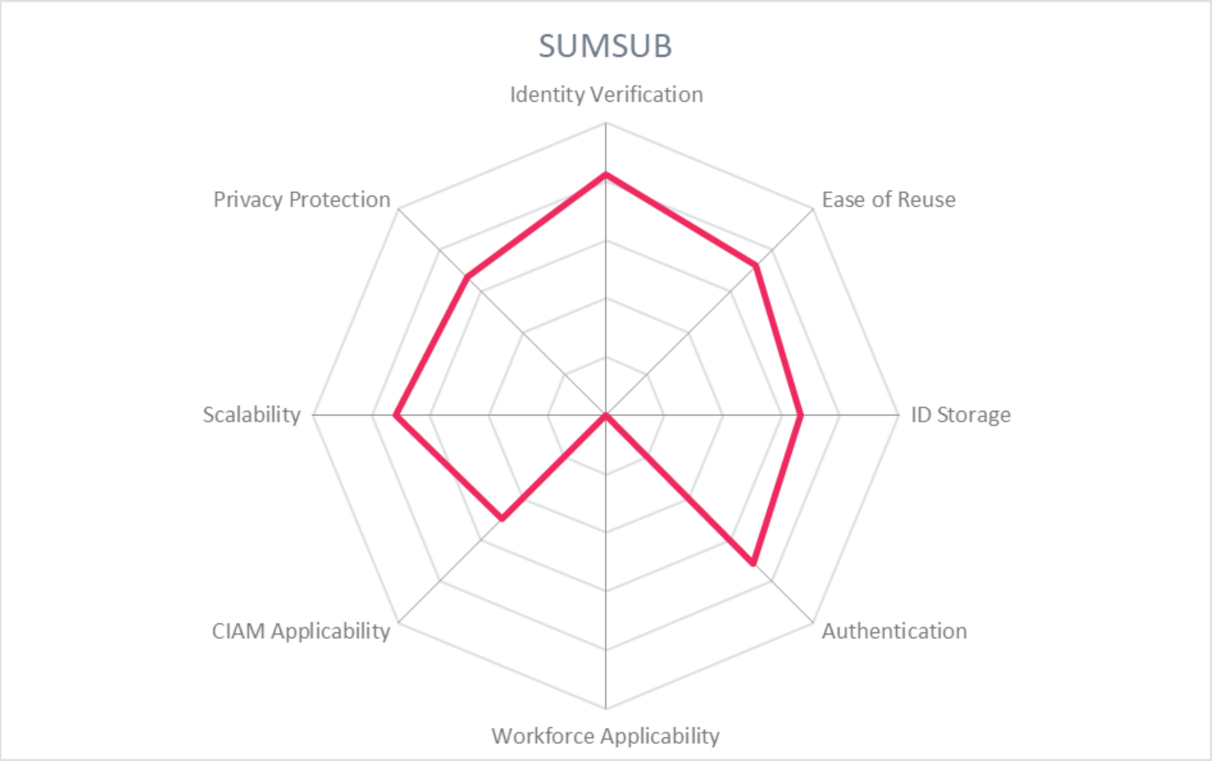
Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Strengths

- Offers customers a pay-per-valid-user licensing model
- SOC II Type 2 certified
- Innovative approach to reusing verified data among shared customer bases
- Strong global presence
- Well-developed integrator partnerships
- Offers AML checks for additional attribute validation
- Supports contextual and risk-adaptive authentication
- In-house OCR for document verification

Challenges

- Reusability requires a direct partnership between two Sumsub customers or a consortium approach
- Available as a cloud service only, through AWS
- Does not yet support importing of eIDs or bankIDs
- Could offer support for 0Auth2 and OpenID Connect


SUMSUB
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Thales – Digital Identity and Security

Thales Digital Identity and Security (DIS) division, formerly called Gemalto, is based in Paris, France, and supports governments with their digital ID schemes and private sector organizations that wish to be a private identity provider (IdP) within a national government-driven initiative. Thales does this with a wide portfolio of mobile and wallet ID solutions for citizens to provide a digital identity for in-person and online interactions, providing both holder wallets and verifier wallets. Thales provides mobile citizen identity solutions and eGovernment services, and identity/document/biometric verification and authentication for financial services and other industries globally. Thales can meet both IAM and CIAM identity verification use cases.

Thales provides verified identities with support for different mobile wallet formats that enable both online and in-person interactions: based on ISO 18013-5 for mobile drivers' licenses and mobile documents, based on the W3C standard for Verifiable Credentials, and for a mix of the two. The wallet can manage multiple digitalized credentials such as identity cards, mobile driver's licenses, digital travel credentials, and m-healthcare credentials with the ability to selectively share only information and attributes which are strictly necessary for the transaction, such as a proof of age, entitlements, etc. Different identification onboarding scenarios are offered to issue an identity credential with support from partners and in-house technology. Depending on the ecosystem in place, a user's identity can be verified 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. The identity data is stored locally on the user's device. The identity verification can be conducted with mobile flows or with a web browser. The user is bound to their device during onboarding.

Once an identity has been verified and a credential issued to the user's wallet, in-person verification is possible by establishing a secure connection between two mobile devices (the digital ID wallet and the ID Verifier app) via QR code, NFC, and data transferred via Bluetooth, WIFI, or NFC. The identity credential is verified either with PKI or by providing a short-life token that checks the government source registry.

Thales supplies an SDK for online-only interactions to manage identification, authentication, signature, and identity attribute sharing flows, as well as an SDK for wallets that support these flows for online and offline interactions. Credentials from the Thales user wallet can be read and verified by the verifier apps of other suppliers that are based on ISO 18013-5 standard. Thales allows for credential issuers to set policy regarding multiple user wallets and self-service, ranging from allowing users to populate their digital wallet with the same credentials on multiple devices to revoking credentials when transported to a different device's wallet. In addition to the user identity wallet, Thales also provides the verifier app for organizations requesting identity credentials and supports peer-to-peer credential sharing as well. Authentication via biometrics, the Thales Digital ID Wallet app, PKI eID cards, and others is possible to customer and government web service portals.

In the backend, a modular digital identity services management platform pilots the digital ID and can provides self-service portals so users can manage their own identity, credentials, identity attributes, and consents. 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 Digital ID services platform can support various digital credential formats, including those based on the mobile doc ISO 18013-5 standard as well as the W3C Verifiable Credential standard to address decentralized identity models.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

THALES

Building a future we can all trust

Strengths

- Strong case for verification, integrating use of physical IDs with reusable digital attributes
- Modular digital credential issuance platform to support multi-wallets, multiple document formats, multiple standards, and multiple issuers
- Supports high assurance PKI use cases, strong representation in the banking and government sectors
- Advanced mobile security and data protection mechanisms
- Identity verification and attribute sharing is possible offline
- Global coverage for document verification
- Identity verification is provided with both in-house and partner technology
- Can provide both the highest levels of assurance for both eIDAS and NIST
- Supports peer-to-peer credential sharing
- Provides user wallet app and verifier app
- Data minimization

Challenges

- Expertise on serving citizen ID needs, with ability to serve other industries
- Could offer connectors to SIEM or security analytics services

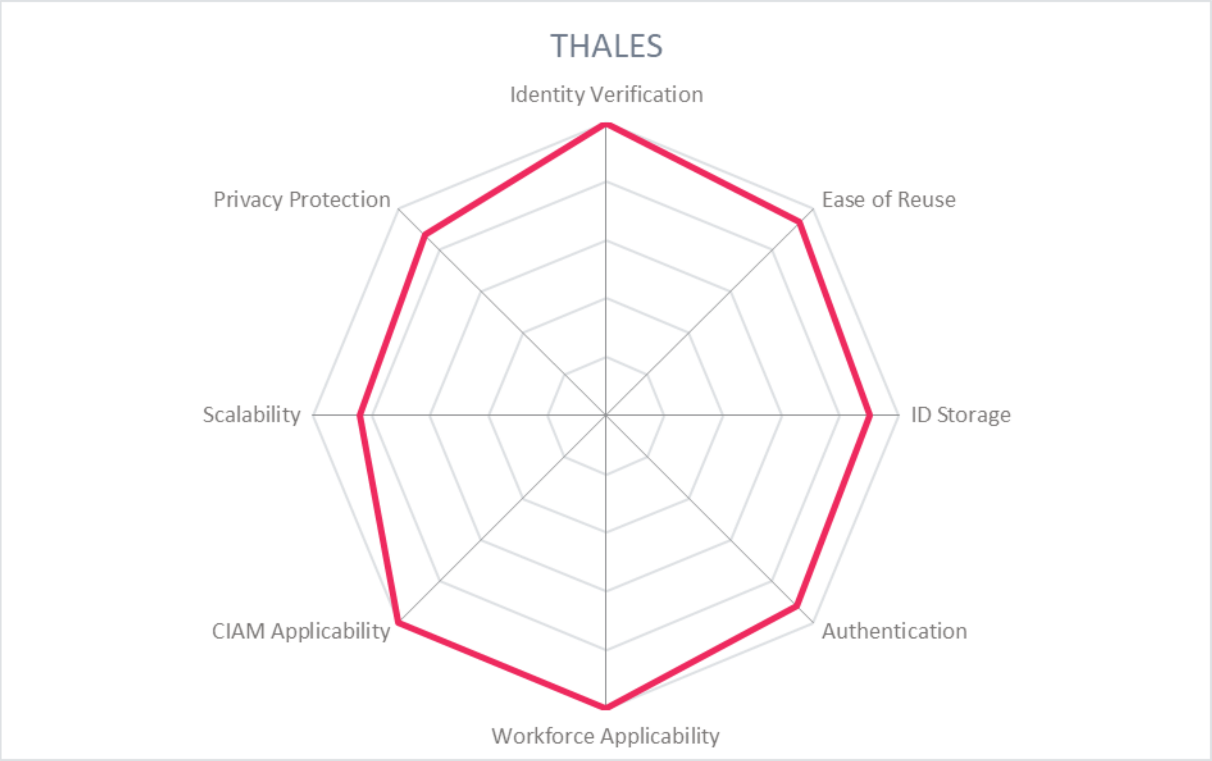
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


THALES
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Verimi – Verimi Ident, Access, Sign, Pay

Verimi was founded in 2017 by a collection of 10 cross-industry shareholders, which has since grown to 21 shareholders primarily based in Germany to build a neutral, independent identity platform. In November 2022, Verimi and identification service Yes merged to further develop the digital identity services and ecosystem in Germany, which in the future will result in a single platform approach. The Verimi product suite includes identification, access, electronic signatures, and payment. Verimi serves two types of customers: users/citizens, and B2B or B2C enterprise partners. Verimi's regional focus is on the DACH region and Western Europe, and supports verification for ID cards, passports, and driver's licenses for over 150 countries.

Identities are derived from identity documents and existing user accounts and stored in a user mobile wallet designed to serve use cases in all sectors. Multiple identity verification methods exist to onboard credentials to the user wallet, including synchronous video verification and automated remote verification supported by partners. 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.

To use the identity service, a user opens and authenticates to the Verimi wallet app. Verified identity attributes – approximately 50 are available, ranging from name to vaccination status – are organized by credential. When onboarding or sharing identity information with a relying party, identity credentials and attributes can be combined. To share identity information, the user accesses the relying party's site or app, authenticates with their Verimi app, and approve the transfer of requested identity attributes as OpenID Connect tokens.

Enterprise partners can customize the verification methods to 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 eIDAS trust level high.

For self-service, the user logs into Verimi for management of identity documents and attributes and a full list of where Verimi can be used. 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.

Reusability of the identity is supported by issuing the identity credentials and attributes directly to the user with a one-time identification process. With the encrypted ID data stored in the cloud, accessible via the user's Verimi wallet app, the user can choose to present those to any party which accepts Verimi credentials for account opening, authentication, or signature use cases. This cloud-based model enables the user to have multiple devices synced. Privacy principles are upheld with no data tracking, profiling, or advertising done by Verimi, and by providing the user with a transaction history.

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	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive

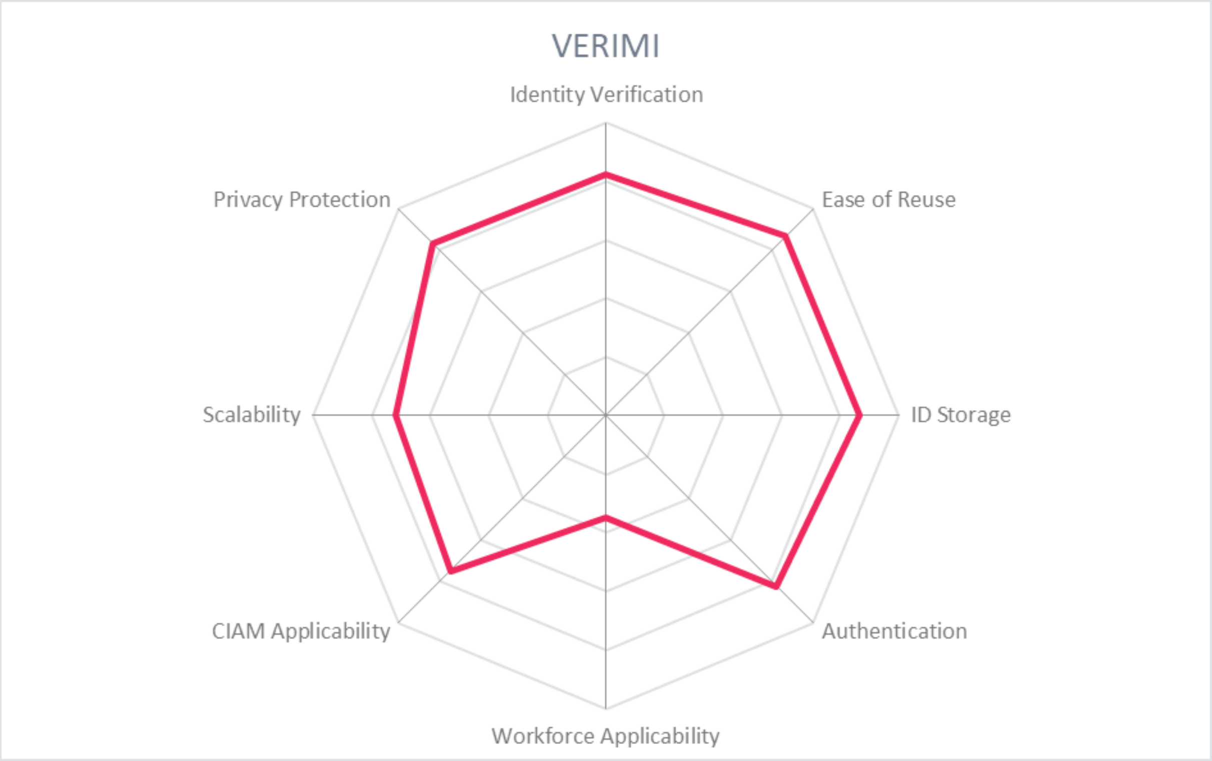
verimi

Strengths

- Strongly contributes towards a reusable digital ID with selectively sharable attributes
- Digital wallet can be accessed from desktop, mobile, or other smart devices.
- Device synchronization of wallet apps is possible
- Accepts eIDs from government sources and trusted IdPs
- 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
- Step-up authentication is available

Challenges

- Separate personas support through opening a second ID wallet
- Support for identity reuse could be strengthened with P2P exchanges
- While verification capabilities reach globally, the solution is currently focused on the DACH region only


VERIMI
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

XAYONE Solutions – GAiA Trust Platform

XAYONE Solutions was founded in 2012 as Oxyliom Solutions. They are headquartered in Luxembourg and have offices in Casablanca and Dubai. The company has developed the GAiA Trust Platform, which provides two solutions: GAiA Advanced Identity Management and GAiA Trust Services Management for securing electronic transactions serving the B2C and B2E markets. There is a particular focus on serving financial services, government, and transportation industries with identity verification and enrollment capabilities.

Reuse is enabled by verifying the user's identity and issuing a PKI-based verified identity attribute to a user-held digital wallet. The private key is stored on the user's mobile device. This verified identity can be shared with partners within an organization's ecosystem, for example across all branches of a bank and with partner insurance companies. For an organization to issue and verify credentials, a license and the mobile app SDK are required. Reuse of verified identity attributes is also possible via authentication, using verified biometrics as an authentication factor. 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.

The GAiA Trust Platform can conduct identity verification to support KYC and verified onboarding of users. Identity verification may be completed with in-person identity verification, hardware-supported verification in specific locations such as in airports, video verification, or by leveraging a user's laptop or mobile device for document and biometric verification. An identification policy orchestrator allows for the flexible design of policies including identity attribute verifications, identity assurance levels, and authentication assurance levels. NIST Identity Assurance Level 3 or eIDAS High can be achieved.

XAYONE offers a remote identity verification app that can scan any ICAO passport and perform hologram verification, facial recognition, NFC reads against chipped documents, and passive liveness and spoofing checks. To onboard users, documents from a library of 11,000 templates in over 100 languages can be scanned and verified. 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. API connectors as well as SAML and OpenID standards are available for most known identity providers (IdPs). The document verification process is provided by in-house technology, including checks of the MRZ, OCR, reading of an embedded chip using NFC, and various validity checks. Face matching is completed between the photo ID and the individual completing the liveness or video verification process, accompanied by spoofing detection and fraud checks against masks and replay attacks. Biometric capabilities are completed in-house, with 1:1 and 1:n matching capabilities. Connections to 3rd-party identity proofing services are not provided.

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. 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.

The platform features user dashboards for self-service consent and privacy management, including the abilities to view/edit/export/delete personal information. Family management can be configured via roles and a delegated admin model. The GAiA Trust Platform offers key management and works with leading HSMs to provide high levels of data security, secure encrypted access tokens, data, keys, and provide consumer privacy. XAYONE adheres to OAuth2 Device Flow for registration and association of consumer IoT device identities with consumer identities.

APIs are available for all features on the platform. The GAiA Trust Platform can be installed on-premises on Linux or Windows or in most Tier 1 IaaS platforms. The platform is offered as SaaS and operates from a single cloud provider in Luxembourg, which may impact scalability despite being a microservices-based solution. Multiple licensing/subscription models are available. Most sales and support are currently in Africa, the Middle East, and the Benelux region of the EU.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

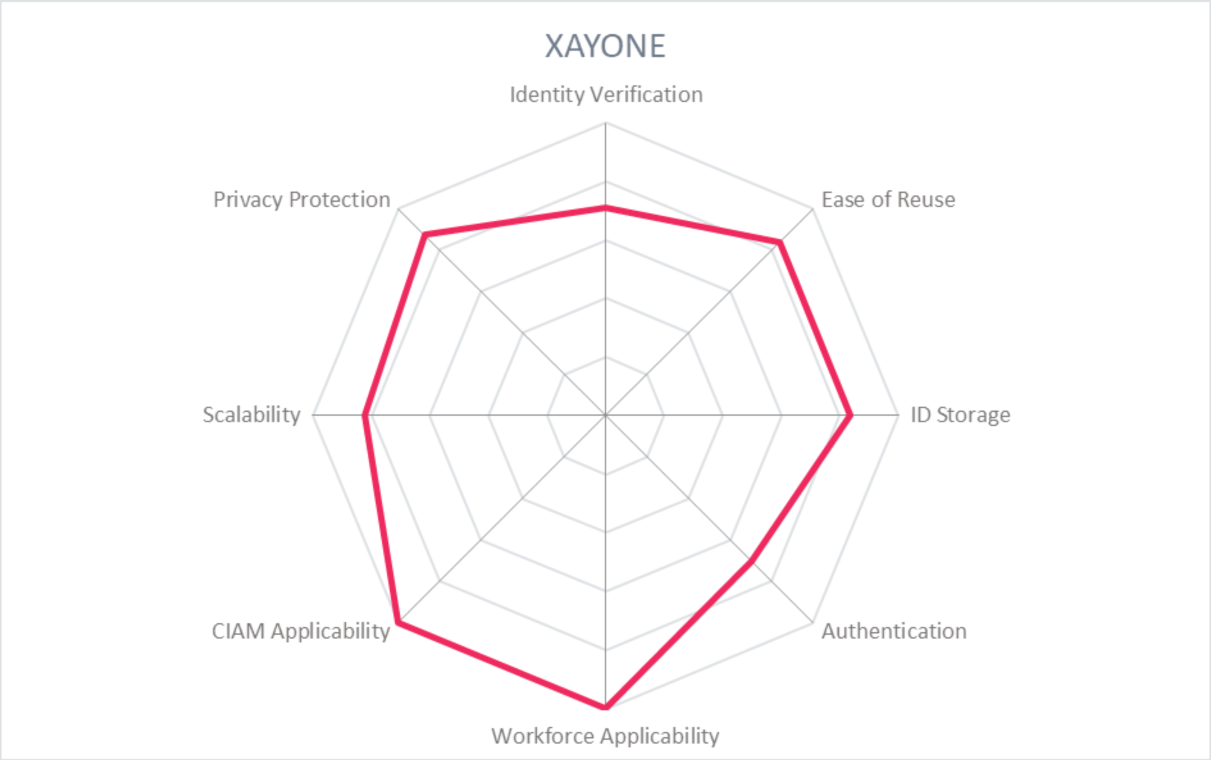
XAone

Strengths

- Document and biometric verification is done in-house
- Strong support for relevant regulations in the financial industry, including AML, eIDAS, GDPR, KYC, and PSD2
- NIST IAL 3 and eIDAS High can be achieved
- PKI-based user-centric storage
- Offers in-person and video call identification options
- Reuse is possible within an organization’s ecosystem
- Authentication using a verified biometric factor is possible
- Offers orchestration and digital signing services

Challenges

- Verified identities in user wallet not yet usable outside of a defined ecosystem
- Passive biometrics are not built in
- Not yet been audited for ISO 27001 or SOC 2 Type 2
- Reuse could be expanded by facilitating credential sharing to organizations independent of the credential issuer


XAYONE
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Yes – Yes Open Banking Ecosystem

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. In November 2022, Yes and ID wallet provider Verimi merged to further develop the digital identity services and ecosystem in Germany, which in the future will result in a single platform approach. The modular solution provides identity services including verification, onboarding, and authentication, electronic signing, securely sharing bank account information, and payments. The geographic focus is on Germany, with entry to other markets on the roadmap.

Yes allows customers to leverage the verified identities held by banks to onboard and authenticate their users as well as enable them to sign with Qualified Electronic Signatures (QES), age verification, and payment. Yes enables a customer to onboard new users with their online banking credentials from the numerous active and passive bank partners. The user selects the option “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 customer or relying party. For two factor authentication, a TAN is sent to the user’s phone, or the same second factor that is configured for the user’s online banking account is maintained which could include biometrics. Registration forms are auto-filled from the online banking profile. A pseudonymous identifier can be provided for user reauthentication, directing the user to their preferred bank automatically. Yes achieves eIDAS level substantial, and KYC screenings for politically exposed persons (PEPs), Ultimate Beneficiary Owners (UBOs), blacklists and sanctions lists are conducted through the verified information provided by the partner banks.

To enable users who do not bank with the 1,000 active bank partners to still onboard or reauthenticate with Yes, Yes works with identity verification partner Crif to do a one-time video verification and bank authentication. Payments can be made directly from the user’s banking app instead of through a third-party payment service. Payments are released after a successful two-factor authentication to the banking app.

If a higher level of assurance is required, the relying party receives the user identity claims with metadata to attest its verification process and trust framework for a fee. User identity and account information can be signed with a QES to certify the authenticity of the data. Other signing use cases allow the user to sign contracts online by selecting “sign with Yes” to be redirected to the user’s bank login page or app where they would authenticate. After completing the second factor, the user would confirm the signature to complete the transaction. The document remains with the relying party, with an API provided for signing.

The Yes Open Banking Ecosystem facilitates reusability of a verified identity by allowing users who have registered with Yes to onboard or authenticate with third-party services using their verified online banking credentials. This ecosystem is supported by over 1,000 active bank partners and can extend to non-active bank partners with the support of identity verification partner Crif. Relying parties must implement OpenID Connect 4 Identity Assurance protocol, which provides technical interoperability of credentials from the many different identity providers (IdPs). No wallet or self-management of credentials is required of the user – since the verified identity attributes are stored in the core banking system of the user’s chosen bank, the user simply selects their bank for onboarding, authenticating, or providing an e-signature with, and are routed to their online banking app to complete the transaction.

The Yes product portfolio is modular and API-based. 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.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

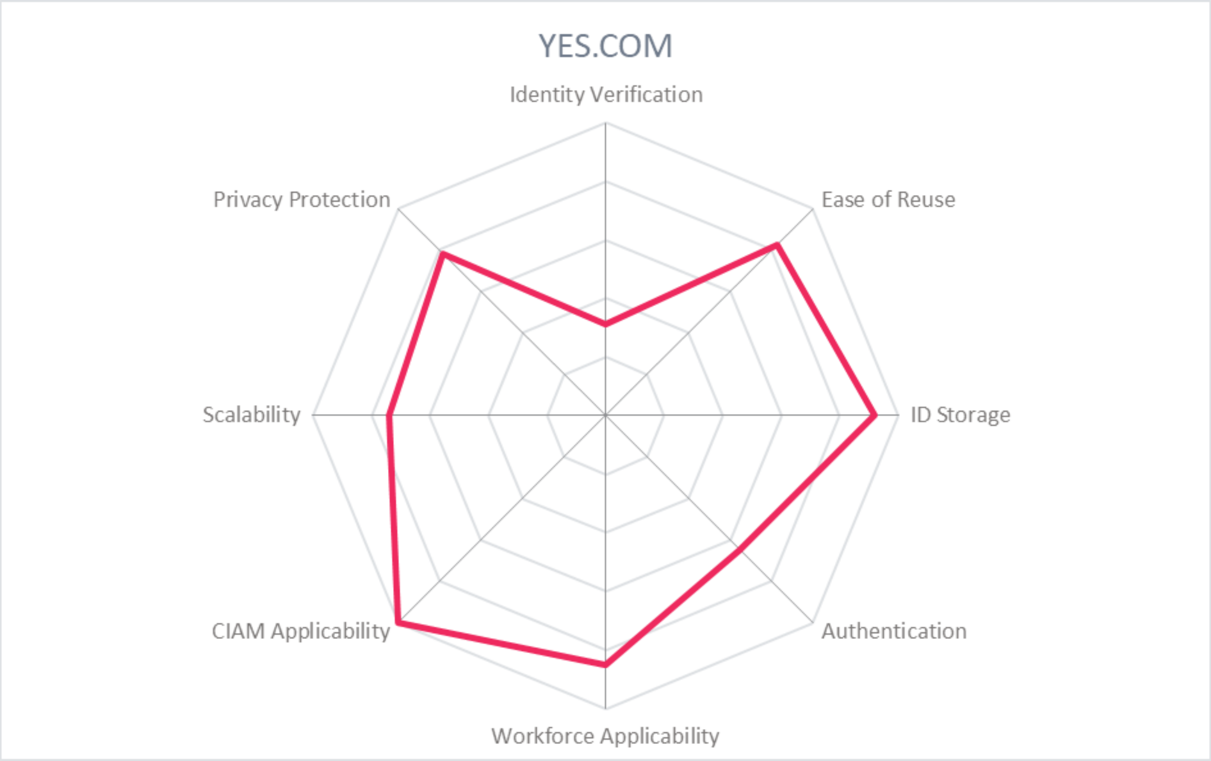
yes®

Strengths

- Built using open standards including OAuth, OpenID Connect, and Cloud Signature Consortium
- Qualified Electronic Signatures (QES) use cases
- Payment capabilities
- AML compliant
- API-forward architecture
- Valuable for logging into infrequently accessed sites
- Compelling use case for financial institutions to remain active post-PSD2
- Collaborating with GAIN initiative for global reach

Challenges

- Relatively small vendor focusing on DACH region, with opportunities for maturity and growth
- Biometric capability provided by banking apps rather than in-house tech
- Identification of eIDs and BankIDs via partners
- Document verification provided by participating banks
- Could add additional fraud reduction measures such as user behavior analytics


YES.COM
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

Yoti – Yoti App & IDV Services

Yoti is a global digital identity platform based in the UK that provides identity verification, age verification, e-signatures, and authentication solutions for customer identity management. To facilitate this, it provides the Yoti app with verification options in the browser such as transaction-based identity verification. 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 EMEA and APAC.

The process typically begins with identity verification, composed of document verification, and biometric facial matching. A partnership with the UK Post Office called Post Office EasyID allows for in-person verification that is interoperable with Yoti. Document verification uses a combination of Machine Learning and trained security personnel, typically taking 1-3 minutes. The document scan uses OCR, NFC for chip reading, and scans the MRZ, meeting the AML requirements of UK's JMLSG. The document scan is a hybrid process with Machine Learning, third-party database checks, and is supported by qualified document checkers. Identity documents – including passports from 195 countries, drivers' licenses, and national identity cards – can be verified. Identity verification continues with liveness detection and face matching, supported by fraud detection via mask attacks. In addition to verifying government-issued identity documents, Yoti allows some user-certified data to be verified such as address or contact information. The identity verification can be orchestrated to meet eIDAS low through high assurance levels, NIST 800-63-3 levels 1 and 2 (as relates to liveness detection), and GPG45 medium and high identity profiles.

Yoti has a proprietary digital identity wallet. The wallet is offered as a no/low code portal or as an SDK integration with additional features such as own credential creation and location restrictions. The wallet is the user's vehicle to a reusable, verified identity, where the one-time identity verification onboards the identity credentials for future use with any verifier that accepts W3C credentials. Yoti stores credentials in a decentralized hybrid model. The credentials are stored in Yoti's protected cloud infrastructure in a sharded and decentralized state, while the user holds their private keys in the secure element of their mobile device. Via the private keys, the user maintains control of their credentials but has the benefit of cloud-based storage for easier recovery of the identity wallet in case of stolen or lost device, or other changes.

Organizations can use the verified identity attributes onboarded by the users to request attributes to complete other transactions for issuing credentials (i.e. employee ID) to the verified individual. Yoti has a ForgeRock integration, available through the ForgeRock marketplace. While import of Verifiable Credentials to the Yoti wallet from other issuers is supported via API, the import of external identities such as eIDs or BankIDs is not yet supported.

Yoti provides a receipt of credentials shared to the individual, and a business receives evidence and a recommendation from Yoti. Principles of data minimization are maintained. 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. All data stored on the Yoti platform is encrypted at rest with AES-256 encryption.

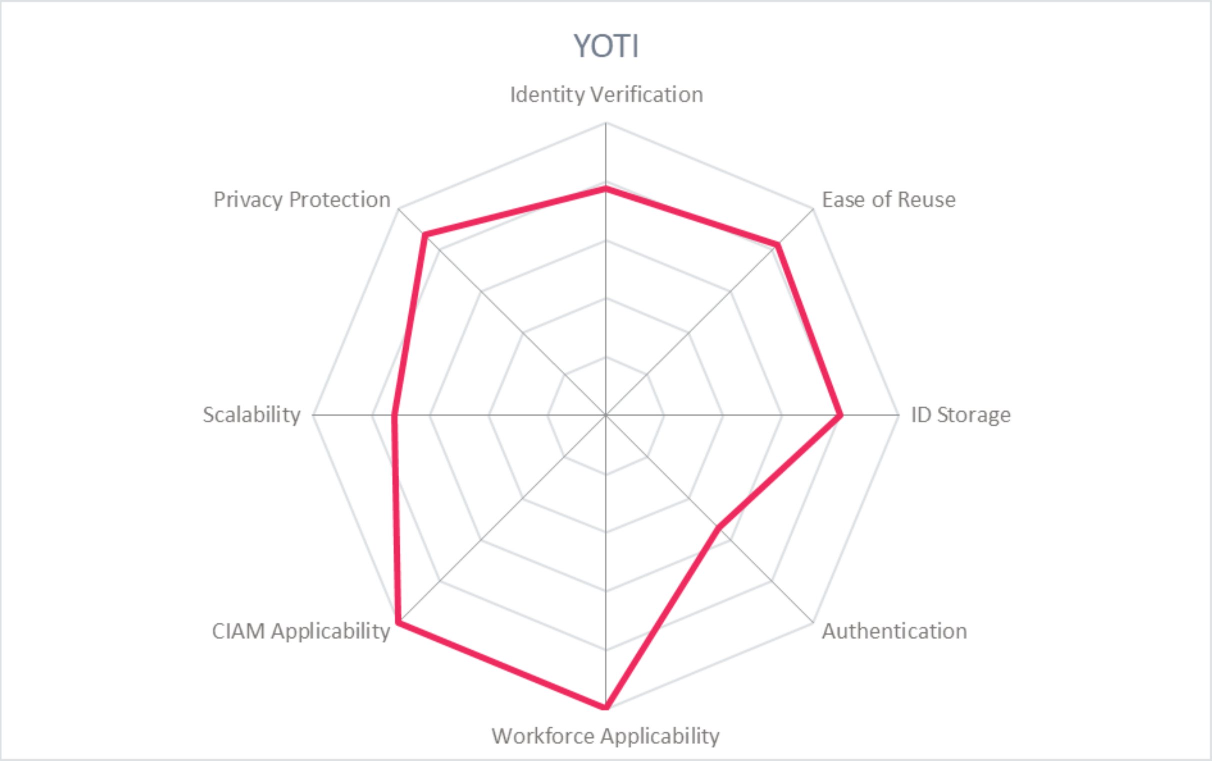
Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

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 and ethical framework in place
- Biometric authentication linked to verified identity
- Data minimization principles
- Online and offline usability

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.
- Exporting credentials to an external wallet is possible but still challenging
- Import of external identities is not supported


YOTI
Identity Verification
Ease of Reuse
ID Storage
Authentication
Workforce Applicability
CIAM Applicability
Scalability
Privacy Protection

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 offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, 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.

- Civic – Based in San Francisco, US, Civic focuses on creating a secure identity ecosystem and blockchain verification services.
  Why worth watching: Civic unites Verifiable Credentials with liveness, uniqueness, ID documents, location, and sanction screening for decentralized functionality.
- Cryptovision – Based in Gelsenkirchen, Germany, Cryptovision is a specialist for cryptography and solutions for secure electronic identities.
  Why worth watching: Cryptovision is an influential vendor parallel to the Providers of Verified Identity space as a proven provider of secure identity solutions for governments, health, automotive, finance, insurance, energy, and IT.
- Evernym – One of the pioneers of decentralized identity and now owned by Avast, Evernym provides a platform to issue and verify verifiable credentials.
  Why worth watching: Evernym has a suite of products to issue, verify, and store reusable digital credentials.
- ID.me – Providing identity verification and authentication products, ID.me allows businesses to consume identity credentials that have been verified, particularly to cut down on fraud.
  Why worth watching: ID.me provides a variety of identity verification methods with a promising pathway to reuse.
- Indicio.tech – Indicio helps organizations adopt open source, decentralized verifiable credential solutions and provides proprietary wallet solutions for holding, and sharing credentials.
  Why worth watching: with several large-scale projects completed, Indicio has proven experience in the market.
- iov42 – iov42’s product is an identity platform to enable businesses and governments to coordinate interactions securely, particularly focusing on supply chain and manufacturing solutions.
  Why worth watching: iov42 targets specialized industries that are not always met by other vendors.
- KnowMeNow – KnowMeNow provides blockchain-enabled KYC for organizations, with a strong bridge to reusability.
  Why worth watching: Targeting the financial industry and KYC requirements, KnowMeNow is an option for reusable KYC.
- Northern Block – An enterprise self-sovereign decentralized identity platform, Northern Block allows enterprises to issue and verify credentials that are stored by the user.
  Why worth watching: Northern Block is an active player in the decentralized identity market.

- Procivis – Based in Zurich, Switzerland, Procivis offers an interesting portfolio of eID, mDL, and SSI products, providing wallets, means of converting credentials into digital formats, and flows to digitalize in-person processes.
  Why worth watching: Procivis is providing actionable verified identity solutions to governments and bureaucratic offices, influencing real habits of people.
- Prove – With a focus on reducing fraud, Prove supports identity verification for authentication, leading towards reuse of verified identity information.
  Why worth watching: using identity verification to support authentication is one promising way to bring reuse to digital identities.
- SecureKey – Based in Toronto, SecureKey is a provider of digital identity and authentication solutions specializing in CIAM onboarding.
  Why worth watching: SecureKey works closely with government and public services for decentralized, reusable identity solutions.
- SecZetta – 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.
  Why worth watching: Seczetta is delivering alternative methods for reusable enterprise-grade identity verification for an array of use cases.
- SelfKey – Selfkey is an open-sourced foundation that offers a decentralized identity platform, wallet solution, and reusable KYC.
  Why worth watching: Selfkey sets itself up as an enabler and gateway to the web3 metaverse.
- Spherity – Spherity provides a collection of identity and credential solutions for humans and products using decentralized architectures.
  Why worth watching: Spherity provides solutions specifically meeting industry compliance requirements.
- SwissSign – A traditional certificate authority, SwissSign offers solutions to manage verified information and create reusable flows.
  Why worth watching: SwissSign is an incumbent player that could influence the reusability for certificates and verified information.
- ValidatedID – ValidatedID provides decentralized identity solutions for enterprise customers and individual users.
  Why worth watching: ValidatedID is a player in the decentralized identity market, working to revolutionize identity management.
- Vela – 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.
  Why worth watching: Vela is working towards developing products to provide sharable workplace credentials.
- Workday – Through an acquisition of decentralized solution Shocard, workday is developing credential solutions for the workforce.
  Why worth watching: Workday is a large software provider for enterprise workforce solutions and may have a significant reach.
- ZealID – ZealID provides a streamlined identity verification for authentication, based on biometrics linked to device.

Why worth watching: ZealID offers a user-friendly method of reusable identity.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors 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.

Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

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

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

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

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

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

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

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

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

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn’t lead to a very low overall rating. This factor considers the vendor’s presence in major markets.

Financial strength even while KuppingerCole doesn’t consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a “good citizen” in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive
Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral
Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren’t met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don’t appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which don’t provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

Leadership Compass: Providers of Verified Identity 2022— 80919

Leadership Compass: Fraud Reduction Intelligence Platforms - 80488

Market Compass: Providers of Verified Identity - 80521

Market Compass: Decentralized Identity - 80064

Buyers Compass: Providers of Verified Identity - 80792

Executive View: 1Kosmos - 79064

Executive View: Signicat - 72537

Leadership Brief: The Business Value of Decentralized Identity – 80531

Leadership Brief: What to Consider when Evaluating Decentralized Identity? – 80451

Leadership Brief: Guide to Implementing Decentralized ID – 81204

Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarksÔ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support 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.