KuppingerCole Report

LEADERSHIP COMPASS

By Anne Bailey
September 06, 2022

Providers of Verified Identity 2022

This Leadership Compass provides an overview up-to-date insights on the leaders in innovation, product features, and market reach for full-services Providers of Verified Identity. These vendors cover the entire identity verification process from beginning through onboarding and authentication.

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

Content

1 Introduction / Executive Summary 4

1.1 Key Findings 4

1.2 Market Segment 5

1.3 Delivery Models 6

1.4 Required Capabilities 9

2 Leadership 11

2.1 Overall Leadership 11

2.2 Product Leadership 12

2.3 Innovation Leadership 14

2.4 Market Leadership 16

3 Correlated View 19

3.1 The Market/Product Matrix 19

3.2 The Product/Innovation Matrix 20

3.3 The Innovation/Market Matrix 22

4 Products and Vendors at a Glance 24

5 Product/Vendor evaluation 27

5.1 1Kosmos 29

5.2 Experian 33

5.3 GBG PLC 36

5.4 HID Global 39

5.5 IDEMIA 43

5.6 iProov 47

5.7 Microsoft 50

5.8 OneID 53

5.9 Onfido 56

5.10 Ping Identity 59

5.11 Signicat 63

5.12 Thales 66

5.13 TrustBuilder 69
5.14 Verimi 73
5.15 Yes 77
6 Vendors to Watch 80
7 Related Research 83
Methodology 84
Content of Figures 90
Copyright 91

1 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, be it in onboarding an unknown customer or verifying that a contractor is who they claim to be. Providers of Verified Identity are vendors that can issue a digital verified identity or enable an external verified identity to be onboarded and used by the enterprise. Full-service providers can also register, onboard, and authenticate using the verified identity.

The term "Verified Identity" stands for 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. Therefore, Providers of Verified Identity are the vendors that can issue such a verified identity or enable an external verified identity to be onboarded by an enterprise.

Identity verification has previously been viewed as a product category of its own but is increasingly being integrated into full-service solutions, enabling identity verification to be conducted remotely, automatically, passively, federated from verified accounts, in a decentralized manner and/or in parallel to other steps of the identity lifecycle.

This is an emerging market space, and the vendors that are assessed in this Leadership Compass display different methods to provide an enterprise with a verified identity. Some rely on federating verified account information, such as from banks. Others leverage the growing eID ecosystem particularly in Europe. Some embrace the emerging Verifiable Credentials model. And others use the document/biometric/liveness verification model which is gaining popularity and accuracy. Each approach must be assessed individually based on enterprise requirements.

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

1.1 Key Findings

- This report compares full-service verified identity providers, or vendors that conduct digital identity verification alongside providing several of the identity lifecycle stages including vetting/proofing, registration, authentication, and additional services such as fraud reduction, electronic signing, attribute verification, and orchestration.
- A strong ecosystem rating and robust partnerships with both technology providers and institutes like

national registries contribute to a strong solution.

- There are roughly three models of how data flows when a verified identity is provided to a customer or relying party: identity verification is processed in the cloud, processed or stored on the mobile device, or federated directly from the identity provider.
- There are roughly four technology methods that are combined to provide a verified identity: remote automated, eID integration, federating verified accounts, and use of Verifiable Credentials.
- Orchestration features in a solution help to gain adequate global coverage of identity documents, connections to national registries, and coverage for local regulation.
- Overall Leaders in alphabetical order are: 1Kosmos, Experian, HID Global, IDEMIA, Microsoft, Ping Identity, Thales.
- Product Leaders in alphabetical order are: 1Kosmos, HID Global, IDEMIA, Experian, Ping Identity, Thales.
- Innovation Leaders in alphabetical order are: 1Kosmos, HID Global, iProov, Microsoft, Ping Identity, Thales.

1.2 Market Segment

This Leadership Compass analyzes digital identity solutions that perform identity proofing and verification or enables a verified digital identity to be imported and easily reverified. This report compares full-service verified identity providers, or vendors that conduct digital identity verification alongside providing several of the identity lifecycle stages. This could include:

- Vetting/Proofing
- Registration
- Authentication
- Additional services: fraud reduction, electronic signing, attribute verification, orchestration

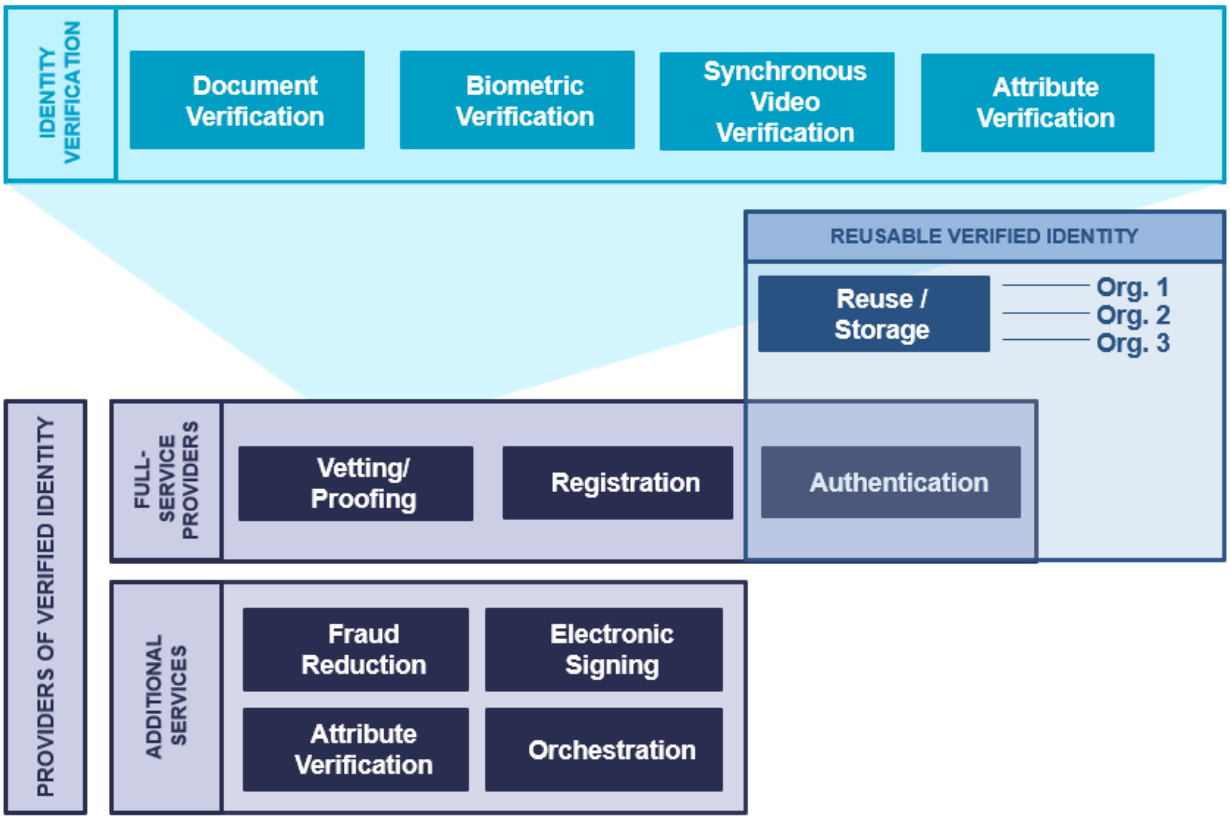


Figure 1: The Interplay of Providers of Verified Identity Market Segment with Other Market Segments

The graphic above visualizes the interplay between the three major identity verification market segments: Providers of Verified Identity, Reusable Verified Identity, and Identity Verification.

- **Providers of Verified Identity:** Full-service providers of identity verification, registration, and authentication, with additional services such as fraud reduction, attribute verification, digital signing, and orchestration.
- Reusable Verified Identity: a verified identity that can be presented to multiple organizations that are separate from the identity provider (IdP) and/or in different roles (personal, citizen, professional).
- Identity Verification: the vendors that provide best-of-breed verification solutions, often specializing in one or more of document verification, biometric verification, video verification, or attribute verification. Identity Verification vendors often provide components to Providers of Verified Identity, or have technology partnerships with them.

1.3 Delivery Models

Providers are trending towards a cloud-based delivery model, with support of multi-tenancy and containerization. The collection and processing of personal data for identity verification -- even when it is held only for the duration of the verification - must be completed in a secure and privacy-compliant manner, which raises necessary questions of where identity document data or biometric data is (temporarily) held and where data centers are located. Many vendors do offer options to deploy the solution on-premises for regulated industries.

There is a high dependence on consumer apps for verification steps - either provided by the vendor or with SDKs provided by the vendor to integrate into customer apps and services. For those vendors that provide federation to verified account information or identity attributes, an API-forward architecture is common.

A particularity of the Full-Service Providers of Verified Identity market is the reliance on technology partnerships. Since a wide range of services related or dependent on the verified identity are being offered, it is rare that a vendor can supply everything in-house and still provide excellent global coverage. Therefore, technology partnerships and ecosystem are very important to leverage best-of-breed document scanning, biometric matching, attribute verification, or federation for the target regions. In-house technology may be sufficient for one or more regions, but may not give adequate coverage of the entire world. Partnerships with national registries, law enforcement, issuing agencies, etc. are also valuable, giving access to authoritative sources to validate identity data and insight into security features of documents to better verify them. Well-integrated partnerships are one of many different signals of a strong solution.

There are differing approaches on processing and storing verified identity data. Some vendors prefer to transmit collected identity information to their cloud -- encrypted at rest and in motion -- for processing. After the verification result is reached, the data is deleted from the vendor cloud, and passed to the customer to hold based on the industry-required retention period. Some of these cloud vendors also support authentication using a verified attribute, such as facial biometrics that have been bound to an identity document. This requires a template to be stored so that future authentication attempts (a selfie) can be matched against the authoritative source (the biometric template collected during onboarding). This must be stored according to the customer's risk appetite and applicable regulatory and privacy guidelines, directives, or laws, which could be with the vendor or with the customer. Vendors that take this method typically do not trust the user device and the security features of the cloud. This method often is device-independent, meaning that the user is able to verify their identity or authenticate regardless of the device that they used to initially enroll.

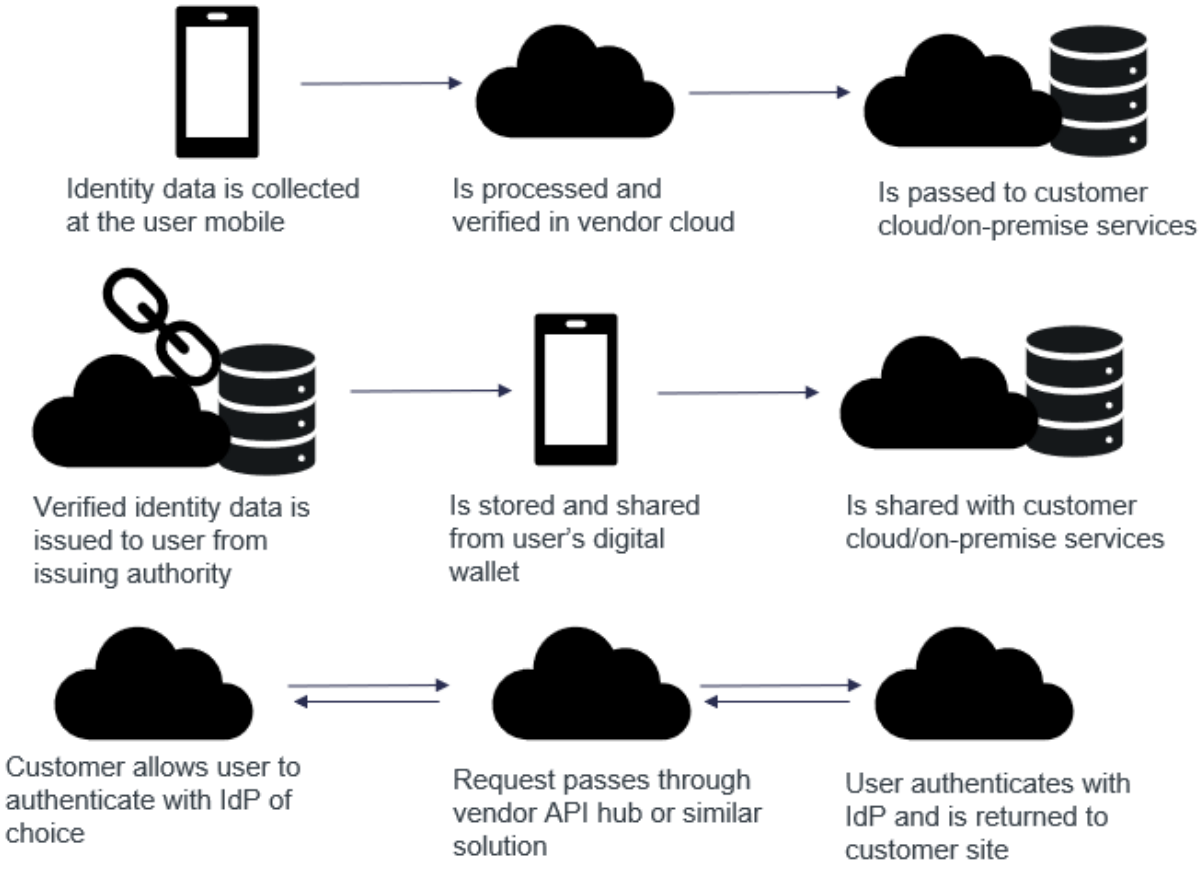


Figure 2: Flows of Data While Providing Verified Identity - Three Models

Other vendors prefer to keep identity information local on the user's device. These typically feature wallet apps, making use of a secure enclave on the device itself to store identity information and biometric templates. While wallet apps are often associated with decentralized identity solutions, this is not always the case, and can be based on other standards such as ISO 18013-5 for a mobile driving license (mDL/mDoc). Solutions like this will rely on the user's mobile device to varying degrees: it will use the built-in camera, and may use the built-in NFC reader or biometric functionality (i.e. Touch ID and Face ID with iOS devices). Some vendors also perform ownership and reputation checks via commercial service providers, or SIM/eSIM-based authentication directly with the mobile network operator (when available). Some vendors bind key device information such as a phone number or FIDO keys to the reference record for identity or credential management. Other vendors will choose to use proprietary biometric functionality and bypass the built-in features of the mobile device. Vendors that choose this method typically prefer a user-centric model where users hold and control their identity information, and choose who to share it with. No collection of identity data is created in the vendor or customer cloud using this method, but users may be limited to a single device (often their mobile phone) which holds their digital wallet for identity verification, authentication, signing, etc.

Other vendors choose a different model altogether - federation of a verified account. These vendors typically build partnerships with identity providers (IdPs) with verified account information, especially banks. When

verified identity data is required by a relying party, the user is routed by the vendor to their bank, where they securely authenticate. They approve the release of verified identity attributes to the relying party. Neither the vendor nor the user stores this identity information, which remains with the IdP. This comes with strong usability and security features as long as the IdP has adequate protections in place.

1.4 Required Capabilities

Providers of Verified Identity must provide a majority of the following capabilities:

1. **Document Verification:** Verification of government-issued and/or real-world documents. Ability to process multiple types of identity documents, from different regions, in different forms (updates, versions) and be checked for authenticity against authoritative sources such as a national registry database. Triangulate data from OCR, smartphone or hardware NFC of embedded chip, and the MRZ of identity documents to increase the confidence level that the document is valid and authentic.
2. **Biometric Verification:** Collect and process an authoritative sample for face, voice, fingerprint, and/or behavioral biometrics for initial verification and for optional later use in authentication. Secure storage, appropriate use of 1:1 and 1:n matching for adequate privacy protection and identification purposes.
3. **Attribute Verification:** Collect, verify, and share standard identity attributes (name, DOB, address, contact info, identification numbers, account numbers) and nontypical identity attributes (education credentials, employment credentials, health records, etc.).
4. **Registration:** Registration of a new identity, or registration of an existing external identity. Registration refers to storage of identity attributes in the organization's directory service and filtering of identity attributes from the IdP. In the case of the latter, the solution supports BYOID for registration and later authentication via federation with reliable IdPs like BankID in the Nordics, and that is interoperable with eID schemes like eIDAS. Capabilities such as Directory User Mapping and User-Driven Federation can play a role here.
5. **Workforce Applicability:** The solution's applicability to workforce IAM use cases, serving employees, partners, suppliers, contractors, freelancers, etc.
6. **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.
7. **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.

8. **Fraud Reduction:** Ensure that the identity documents, biometrics, attributes, or context is valid, held by the individual it describes, and not falsified through a variety of methods: IP address collection, GPS, data aggregation, sanctions lists, behavioral features, keystroke analysis, and more. Confidence scoring should provide a recommendation on the identity's reliability, and may be supported with AI/ML.

The inclusion criteria for this Leadership Compass are:

- To provide a majority of the above-listed capabilities
- 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 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.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Compass. The 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 ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market

2.1 Overall Leadership

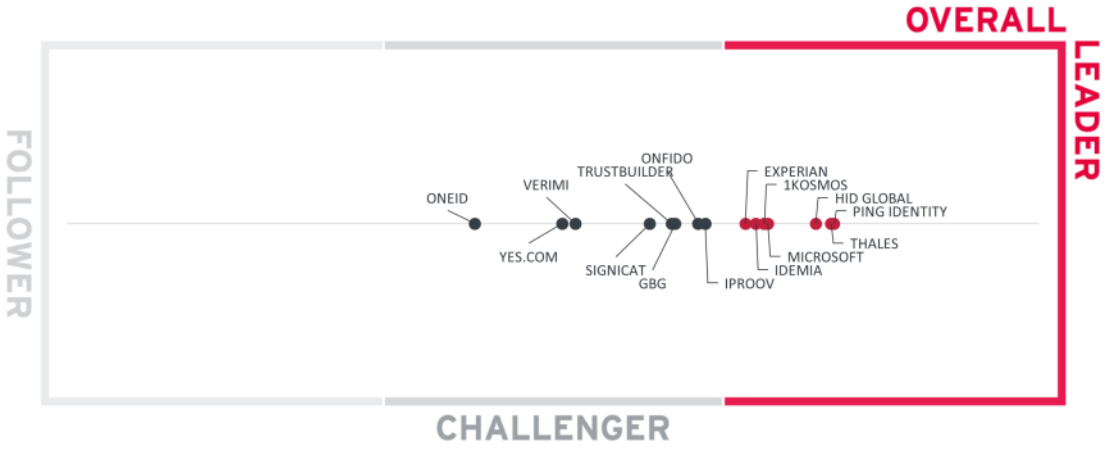


Figure 3: Overall Leadership Rating for the Providers of Verified Identity Market Segment

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 densely packed groups of competitors. There are seven vendors in the Leader section displayed in red. These include known players in the identity issuance space such as Thales, HID Global, and IDEMIA, credit scoring and identity verification actor Experian, and enterprise identity vendors Ping Identity, Microsoft, and 1Kosmos.

Nine vendors are placed in the challengers section. The cluster containing iProov, GBG, TrustBuilder, Onfido, and Signicat represent well-rounded products with relatively strong global presence and market size. Verimi, Yes.com, and OneID deliver quality products with 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
- Experian
- HID Global
- IDEMIA
- Microsoft
- Ping Identity
- Thales

2.2 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.

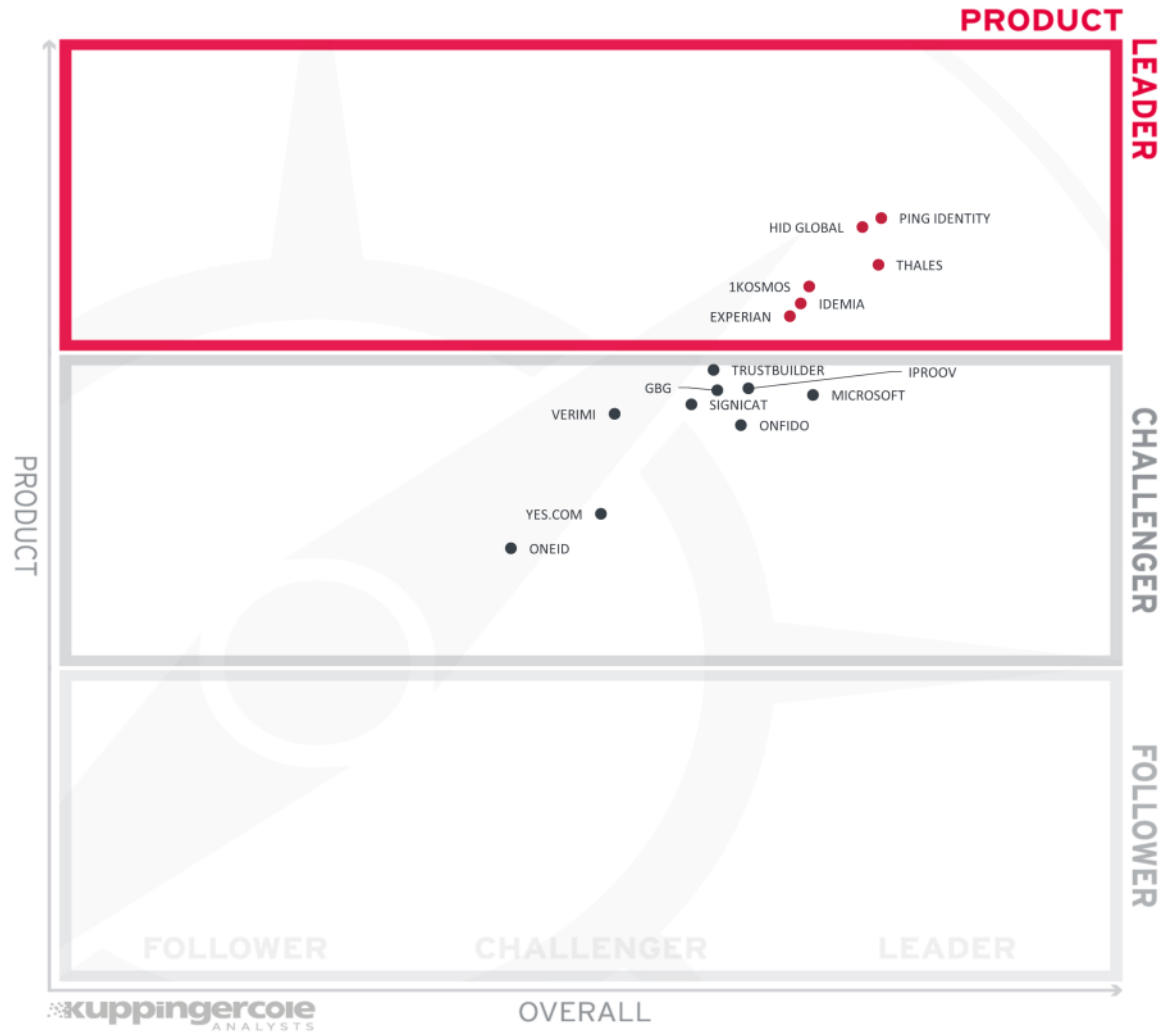


Figure 4: Product Leadership in the Providers of Verified Identity Market Segment

Product Leadership is the view in which we focus on the functional strength and completeness of the solution.

Ping and HID Global lead the way with a strong IAM foundation for the full-service identity verification capabilities, including onboarding and authentication. Thales, 1Kosmos, and IDEMIA are also in the leaders segment with strategic focus on identity verification and for its reuse during later stages of the identity lifecycle. Experian's extensive network for attribute verification and fraud prevention add to its identity verification capabilities.

Challengers include TrustBuilder and Signicat, both leveraging European eIDs focusing on different regions to provide verified identities for enterprise onboarding and authentication. iProov is a best-of-breed biometric verification vendor. GBG has an impressive range of identity verification products and capabilities and is working towards fully integrating them for a unified experience. Microsoft is making remarkable

advancements in enabling organizations to issue Verifiable Credentials backed by identity verification and exchange these across ecosystems. Onfido is a known name in providing remote identity verification, and is expanding to serve more aspects along the identity lifecycle. Verimi serves the German market as a full-service provider of verified identity. Yes.com leverages the open banking ecosystem in Germany for user-friendly access to verified identity, as does OneID in the UK.

Product Leaders (in alphabetical order):

- 1Kosmos
- HID Global
- IDEMIA
- Experian
- Ping Identity
- Thales

2.3 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.

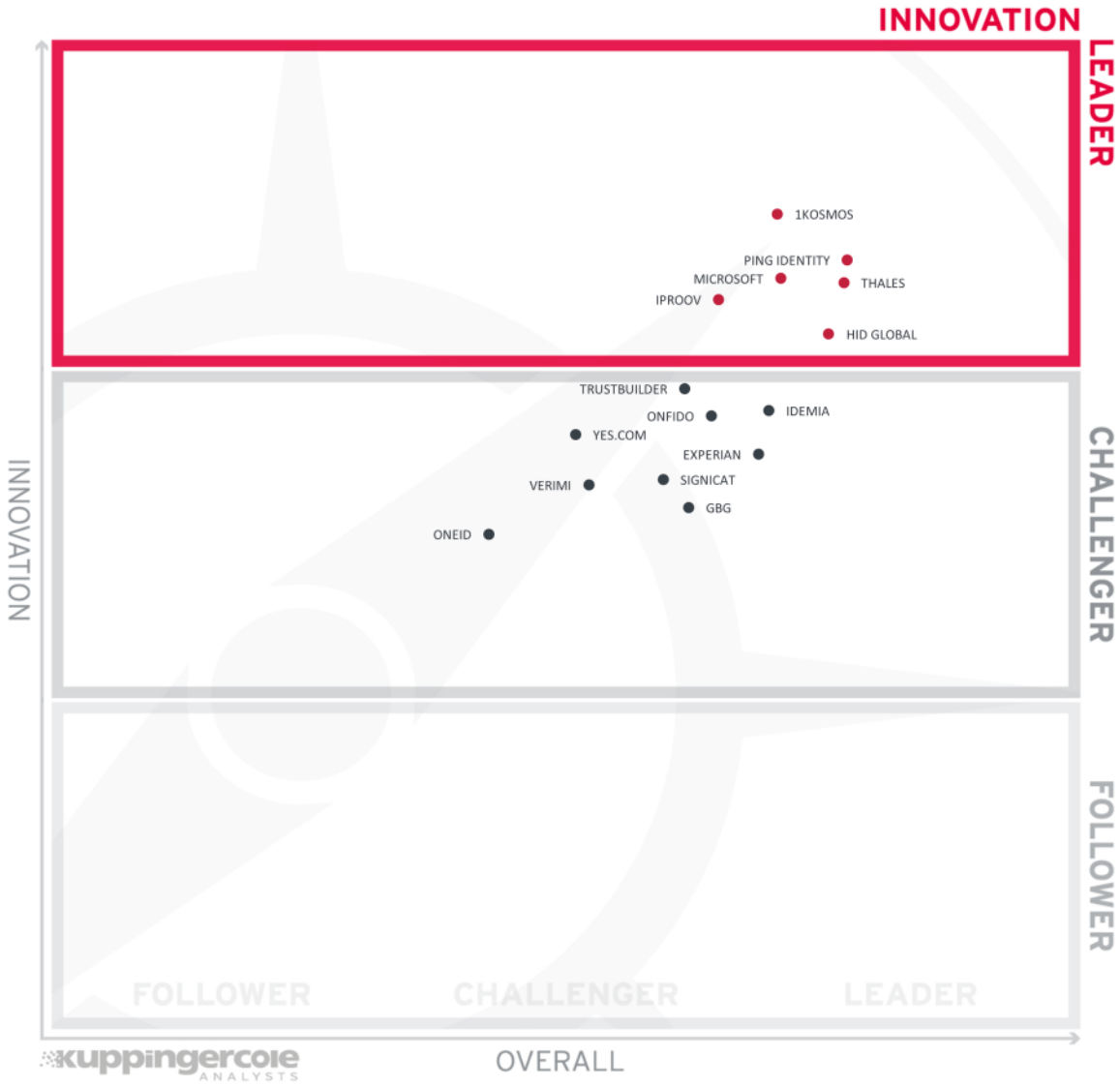


Figure 5: Innovation Leadership in the Providers of Verified Identity Market Segment

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 HID Global make strides to enable citizen IDs that interoperate with emerging Mobile Document (mDoc) standards as well as emerging decentralized wallet standards. iProov focuses on biometric matching and Genuine Presence Assurance for a user-friendly but secure approach to verifying the identity and presence of an individual.

Challengers in the innovation section still have valuable contributions. TrustBuilder works with an attribute-based access control model based on verified identity attributes and leverages the growing European eID ecosystem. Yes.com is advancing initiatives like Global Assured Identity Network (GAIN) for an interoperable and secure means of exchanging verified identity information. Onfido has made strides in establishing the smooth user experience of remote identity verification. IDEMIA, Experian, and GBG expand their traditional portfolios to include identity verification. Signicat brings valuable insight into the digital signatures space. Verimi and OneID leverage existing ecosystems to advance new use cases for verified identity.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- HID Global
- iProov
- Microsoft
- Ping Identity
- Thales

2.4 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.

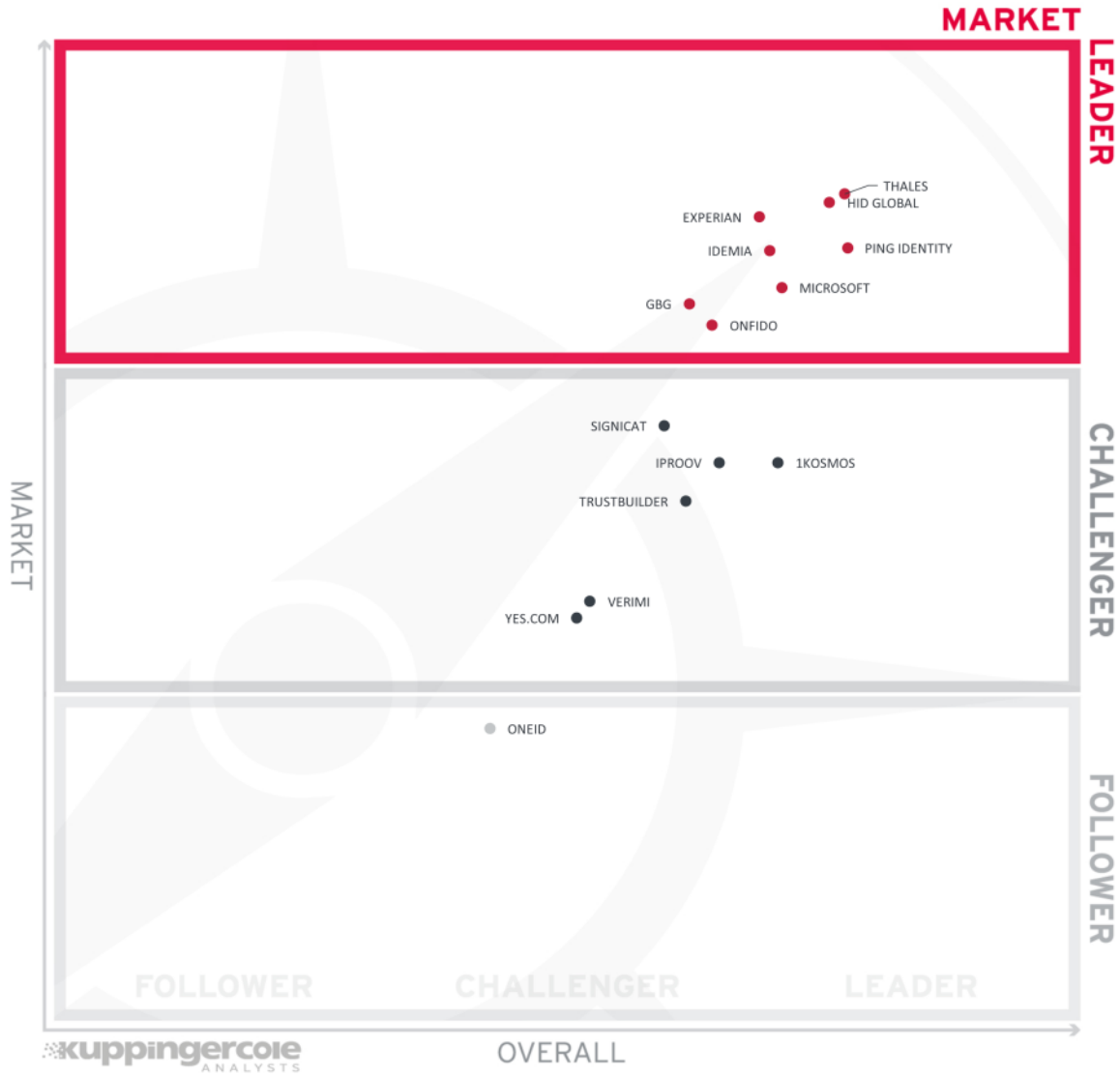


Figure 6: Market Leadership in the Providers of Verified Identity Market Segment

Thales, HID Global and Experian lead the segment. IDEMIA and Ping Identity follow, with GBG, Microsoft, and Onfido rounding off the Market Leaders. These vendors all have a global presence and reputation, with product capabilities spanning the globe.

Signicat leads the challengers with a strong market presence in the Nordics. iProov and 1Kosmos are both growing their global market share and expanding the regions in which they serve customers. TrustBuilder has a strong European presence. Verimi and Yes.com are both focused on the German/DACH market.

In the followers section, OneID currently serves the UK market.

Market Leaders (in alphabetical order):

- Experian
- GBG
- HID Global
- IDEMIA
- Microsoft
- Onfido
- Ping Identity
- Thales

3 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.

3.1 The Market/Product Matrix

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

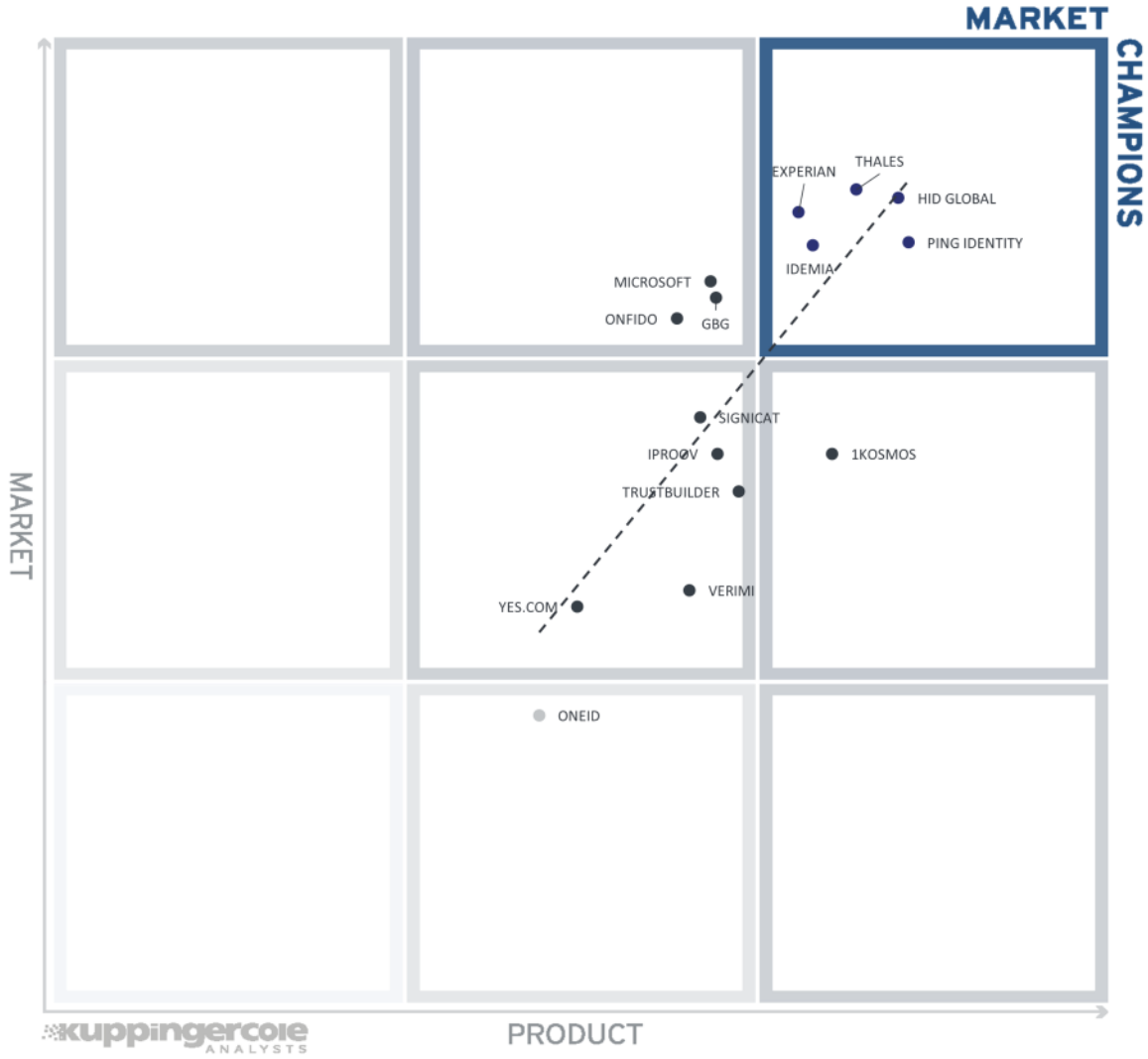


Figure 7: The Market/Product Matrix for the Providers of Verified Identity Market Segment

Vendors below the line have a relatively stronger product maturity in contrast with their market position, but with opportunity for growth. Vendors above the line can be considered "overperformers" when comparing Market Leadership and Product Leadership.

The correlation between market position and product maturity is close overall, with most vendors clustered near to the trend line. The Market Champions listed in alphabetical order are Experian, HID Global, IDEMIA, Ping Identity, and Thales. With relatively stronger market presence than product performance are GBG, Microsoft, and Onfido. Conversely, with stronger product performance than market presence is 1Kosmos.

Grouped near the trend line with capacity to grow both market presence and product capabilities are (in alphabetical order) iProov, OneID, Signicat, TrustBuilder, Verimi, and Yes.com.

3.2 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.

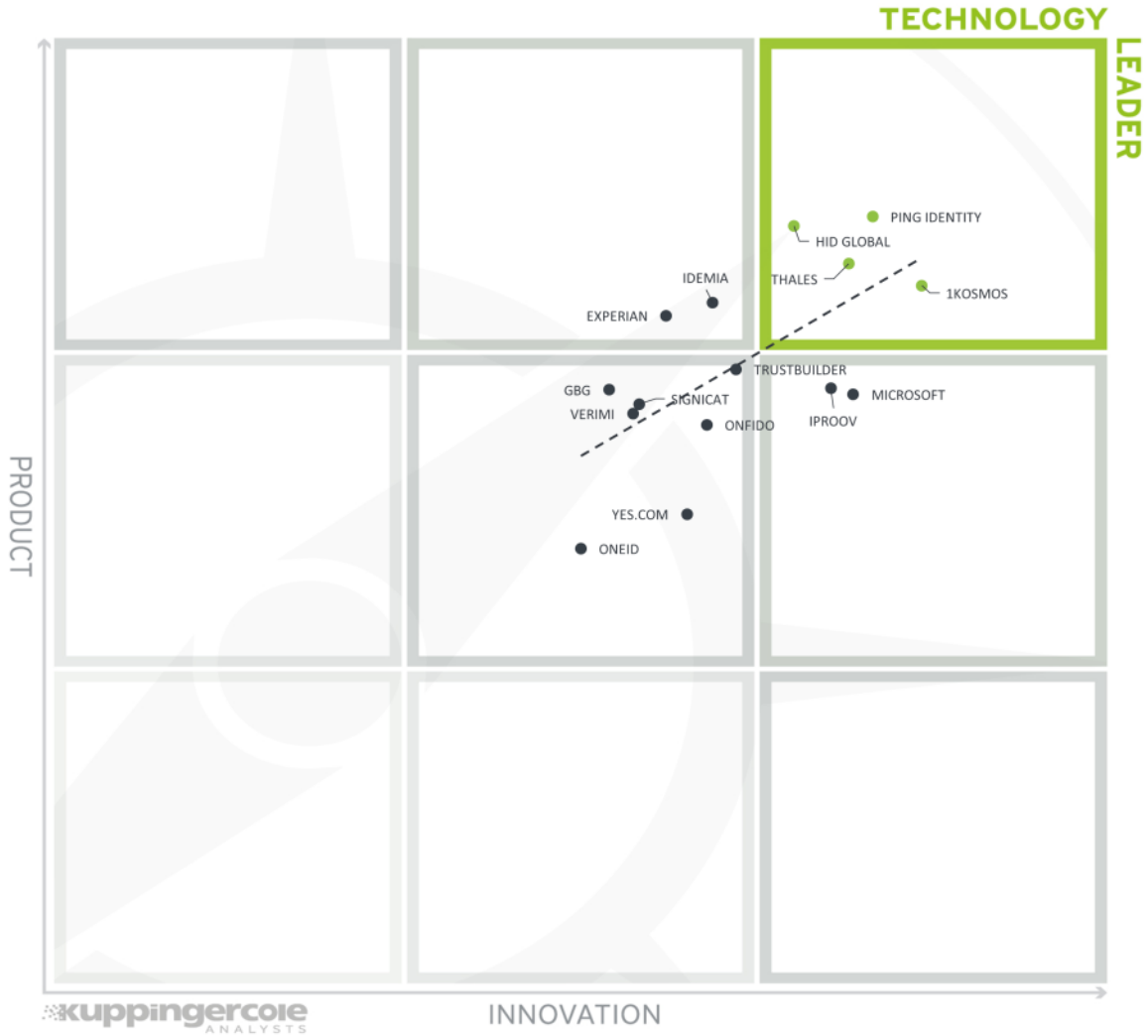


Figure 8: The Product/Innovation Matrix for the Providers of Verified Identity Market Segment

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

Vendors are more spread across the matrix in this view. The technology leaders in alphabetical order are 1Kosmos, HID Global, Ping Identity, and Thales. Though vendors overperforming on the innovation side include iProov, Microsoft and Yes.com, seen far below the trend line. iProov makes its mark with biometric matching and Genuine Presence Assurance, Microsoft with its efforts to easily enable Verifiable Credentials to be issued and accepted in often used infrastructures, and Yes.com for its work on facilitating global interoperability for verified identities are all important contributions to the Providers of Verified Identity market space.

3.3 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 9: The Innovation/Market Matrix for the Providers of 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: HID Global, Microsoft, Ping Identity, and Thales.

Experian, IDEMIA, GBG, and Onfido have room for growth in their innovative portfolios, while 1Kosmos, iProov, Yes.com, and OneID can focus on improving their market positions to take advantage of their innovative products.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Providers of Verified Identity. 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.

Product	Security	Functionality	Deployment	Interoperability	Usability
1Kosmos Block ID	●	●	●	●	●
Experian CrossCore	●	●	●	●	●
GBG PLC Id3 Global, IDScan, GreenID, Verify, and ExpectID	●	●	●	●	●
HID Global Identity Verification Service	●	●	●	●	●
IDEMIA Digital ID	●	●	●	●	●
iProov Face Verifier	●	●	●	●	●
Microsoft Entra Verified ID	●	●	●	●	●
OneID	●	●	●	●	●
Onfido Real Identity Platform	●	●	●	●	●
Ping Identity PingOne Verify and DaVinci	●	●	●	●	●
Signicat Digital Identity Platform	●	●	●	●	●
Thales Digital Identity and Security	●	●	●	●	●
TrustBuilder.io Suite	●	●	●	●	●
Verimi Ident, Access, Sign, Pay	●	●	●	●	●
Yes.com Yes Open Banking Ecosystem	●	●	●	●	●
Legend		● critical	● weak	● neutral	● 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.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
1Kosmos	strong positive	neutral	positive	neutral
Experian	positive	strong positive	strong positive	strong positive
GBG PLC	neutral	strong positive	strong positive	positive
HID Global	positive	strong positive	strong positive	strong positive
IDEMIA	positive	strong positive	strong positive	strong positive
iProov	strong positive	neutral	neutral	positive
Microsoft	strong positive	positive	strong positive	strong positive
OneID	positive	weak	weak	weak
Onfido	positive	strong positive	positive	positive
Ping Identity	strong positive	positive	strong positive	positive
Signicat	positive	positive	positive	positive
Thales	positive	strong positive	strong positive	strong positive
TrustBuilder	positive	neutral	neutral	positive
Verimi	positive	weak	neutral	neutral
Yes	positive	weak	weak	neutral
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 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 LC Providers of Verified Identity , we look at the following six categories:

1. **Document Verification:** Verification of government-issued and/or real-world documents. Ability to process multiple types of identity documents, from different regions, in different forms (updates, versions) and be checked for authenticity against authoritative sources such as a national registry database. Triangulate data from OCR, smartphone or hardware NFC of embedded chip, and the MRZ of identity documents to increase the confidence level that the document is valid and authentic.
2. **Biometric Verification:** Collect and process an authoritative sample for face, voice, fingerprint, and/or behavioral biometrics for initial verification and for optional later use in authentication. Secure storage, appropriate use of 1:1 and 1:n matching for adequate privacy protection and identification purposes.
3. **Attribute Verification:** Collect, verify, and share standard identity attributes (name, DOB, address, contact info, identification numbers, account numbers) and nontypical identity attributes (education credentials, employment credentials, health records, etc.).
4. **Registration:** Registration of a new identity, or registration of an existing external identity. Registration refers to storage of identity attributes in the organization's directory service and filtering of identity attributes from the IdP. In the case of the latter, the solution supports BYOID for registration and later authentication via federation with reliable IdPs like BankID in the Nordics, and that is interoperable with eID schemes like eIDAS. Capabilities such as Directory User Mapping and User-Driven Federation can play a role here.
5. **Workforce Applicability:** The solution's applicability to workforce IAM use cases, serving employees, partners, suppliers, contractors, freelancers, etc.
6. **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.

7. **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.
8. **Fraud Reduction:** Ensure that the identity documents, biometrics, attributes, or context is valid, held by the individual it describes, and not falsified through a variety of methods: IP address collection, GPS, data aggregation, sanctions lists, behavioral features, keystroke analysis, and more. Confidence scoring should provide a recommendation on the identity's reliability, and may be supported with AI/ML.

5.1 1Kosmos

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 authentication factors that are bound to the verified identity for passwordless experiences. 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.

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. 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, and banking credentials. The document is verified to be held by the user it describes by onboarding facial biometrics and conducting a liveness check. 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 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 passwordless authentication. Authentication methods include QR code scan, push notification, time-based OTP, biometrics, TouchID/FaceID, 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	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

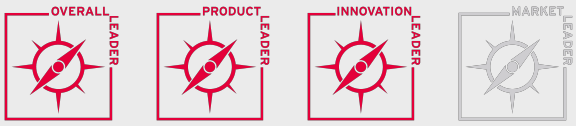
Strengths

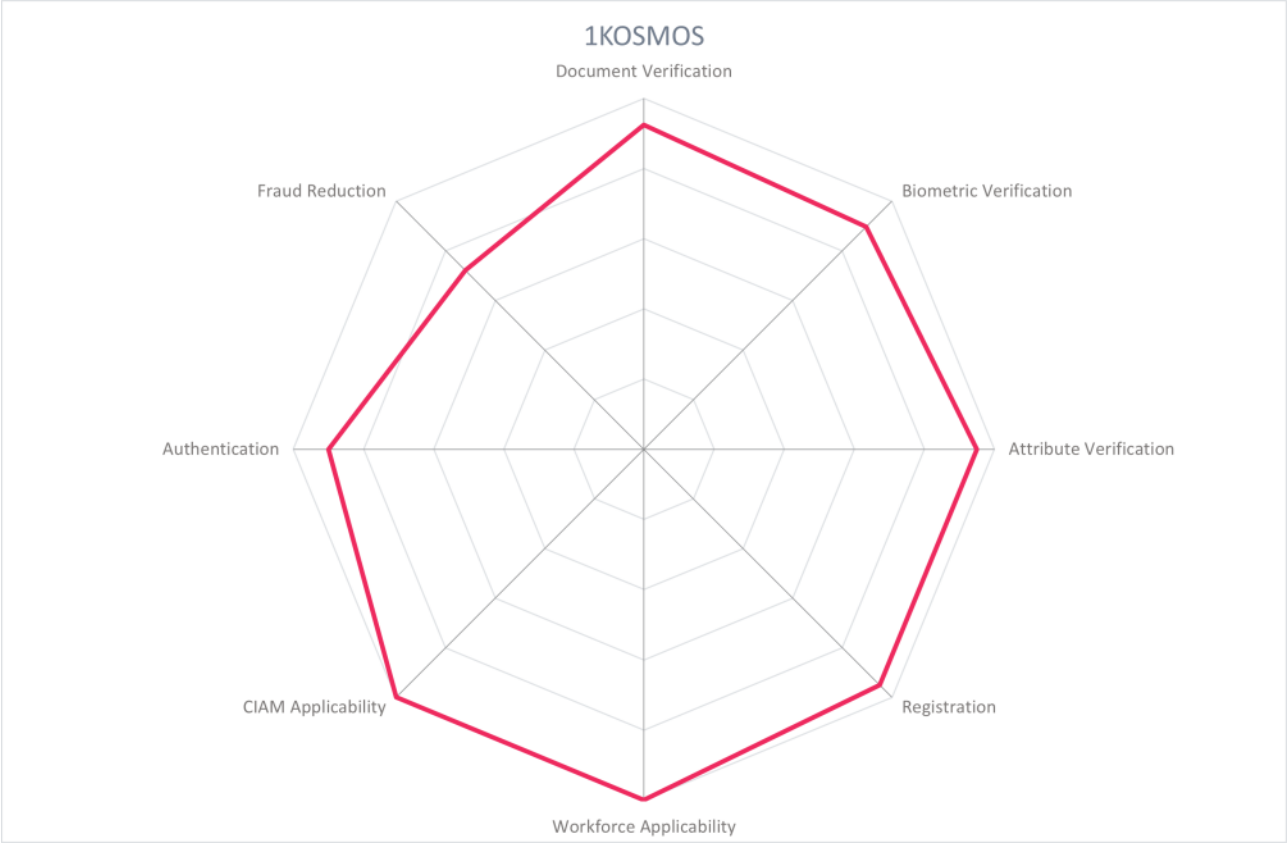
- Biometric authentication factors include face, voice, and fingerprint, and are independent from device biometric capability
- Has backend integration with trusted governmental institutions to verify ID documents
- Provides strong enterprise workforce authentication to achieve critical mass of users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

Challenges

- Support for eIDAS is on the roadmap
- Requires the user to have a smart mobile device with camera functionalities
- Is a small vendor with some restrictions on regional document coverage?
- Blockchain scalability?
- No support yet for behavioral biometrics

Leader in




1KOSMOS
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.2 Experian

Experian was founded in 1996, and is based in Dublin, Ireland. It is one of the "big three" credit rating agencies, processing information on over one billion people worldwide. It provides credit history information to financial institutions, and analytics and marketing information for other customers. It also provides identity verification and fraud prevention functions with its product, CrossCore. CrossCore is a fraud detection and identity verification platform for new account registration, low and high-value transactions (both monetary and non-monetary transactions) and account management. CrossCore provides verification for incoming identity attributes from other providers for a variety of use cases and across industries by leveraging its multi-regional, credit bureau-based authenticated identity assets in products -- PreciseID in North America, ID Authenticate in the UK, ProveID in EMEA - along with its proprietary device intelligence and additional partner data and insights. Experian's geographical reach enables identity verification globally.

CrossCore is a platform that provides verification, ranging from attribute verification, document verification, behavioral biometrics, and business verification with a strong fraud prevention aspect. Crosscore analyzes user data during input, generates a fraud risk score, assesses KYC and CIP risk for compliance, and yields a decision to accept or to require additional verification. As an authoritative attribute provider, Experian offers comprehensive identity proofing services with bi-directional links to various government agencies and financial institutions and partnerships with vendors of app-based remote document verification with liveness detection functions, behavioral and traditional biometric capabilities, email verification, alternative identity data, and mobile verification solutions. Partners include Acuant, Daon, Prove, IDfy, Mitek, eMailage, Ekata, BioCatch, GDC, Boku, and RapidID.

The user inputs their data for onboarding or application screening, and if required, may also prompt a scan of government-issued ID and a selfie for liveness detection which is scored by a collection of first-party and third-party fraud and verification applications. Fraud detection includes account compromise confidence scores, credit reporting, detection of synthetic identities, behavioral biometrics, device and context intelligence, and consistency of identity elements in transactions. This process is supported by its growing database of over 1 billion authenticated identity data assets. The user is then segmented into an appropriate risk group for either successful acceptance or an additional step-up verification before acceptance. This solution achieves up to eIDAS High NIST 800-63-3 IAL2 for Levels of Assurance, able to dial the level up or down based on the use case. CrossCore does enable authentication, but not necessarily using authenticators based on the verified identity.

CrossCore is a SaaS platform. Locations of data centers include US, UK, Germany, Spain, Brazil, Singapore, India, South Africa, and Australia. Data storage is compliant with the requirements of financial and government regulated industries, thus the system is configurable to meet the data storage needs of the customer. Experian supports the range of traditional remote and digital verification procedures for both low and high value transactions, including call center verification with knowledge-based questions.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●●
Interoperability	●●●●○
Usability	●●●●●

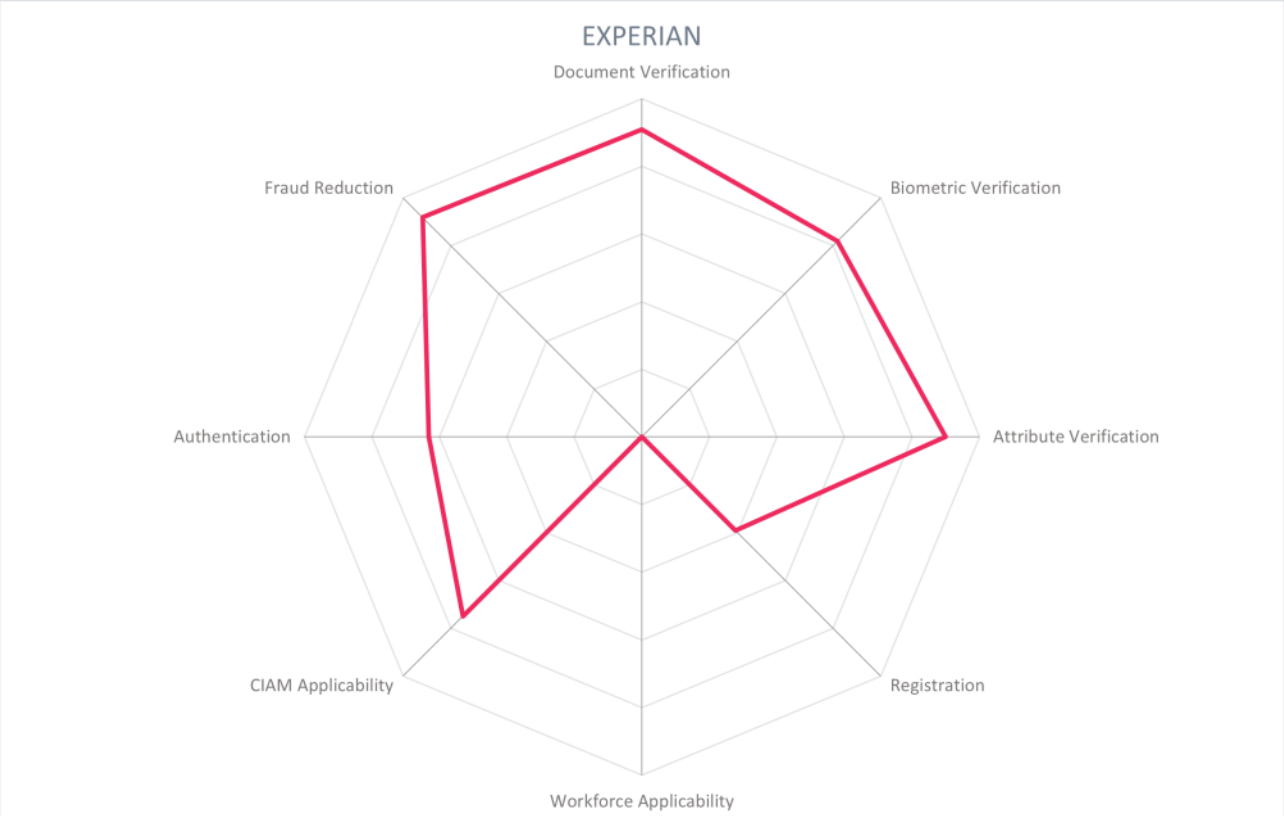
Strengths

- Established market player in credit rating, fraud reduction, and identity verification
- Extensive partner network for global coverage
- Strong fraud detection capabilities
- API-forward architecture
- Decisioning and analytics strengthened with Machine Learning
- Supports both NIST and eIDAS LoA
- Orchestration functionality

Challenges

- Limited ability to save and reuse verified identities
- A secure but less user-centric approach to data storage
- Could support OpenID Connect
- Could offer more authentication options based on verified identity attributes

Leader in


EXPERIAN
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.3 GBG PLC

GBG PLC was founded in 1989 and is headquartered in Chester, UK. Globally, it provides solutions on fraud, location, and identity data intelligence. Identity verification is one aspect of GBG's product offerings, which is comprised of several acquisitions - IDology, Acuant, and GreenID - along with GBG's in-house capabilities. GBG's identity verification solutions primarily serve consumer IAM use cases

GBG is able to support in-person and virtual verification. The capabilities include data and document verification, biometric verification, attribute verification (including date of birth, address, mobile, email, bank account, and national identity numbers), fraud and AML screenings, and authentication. While integration between all identity product offerings is still in process, the Global GBG Platform gives customers an end-to-end verification and onboarding experience with use of the GBG Global Network for verification decisions. Fuller integration with IDology, Id3, and GreenID on the roadmap and stand-alone document and biometric verification solutions from GBG and Acuant are in process of being integrated. For document verification, GBG's combined product offerings have a document library of over 6,000 document types and coverage of over 200 countries, with a suite of third-party biometrics partners, proprietary NFC functionality, verification of template-less documents, and more.

GBG's identity verification products can achieve eIDAS High and NIST IAL3, as well as UK GPG 45. To verify an identity, the user scans their identity document, processes the MRZ, and can read an embedded chip using NFC of the mobile device. Document verification is provided by in-house technology and partners for any manual review that is required by the customer. This is supported by biometric verification and active and passive liveness. Only 1:1 facial matching is used for the solutions, provided by technology partners. Attribute verification and AML screening including PEPs and sanctions lists can also be integrated in the user flows. Attributes are verified by checking against national registries, aggregating data from a variety of sources, via Verifiable Credentials, or via the proprietary eDNA which utilizes machine learning to make a decision whether there is a government source of truth or not.

An administrative view provides an overview of which steps the user passes - document, correlation with data on embedded chip, and liveness - as well as insights into analytics and user journeys. The orchestrator allows for streamlined customization of different requirements for different transaction types, ranging from identity document scans with OCR only, use of NFC, and active liveness detection, facial matching, health passes, Verifiable Credentials, etc.

GBG document and biometric verification solutions are primarily SaaS products with public cloud, private cloud, desktop, hardware, self-hosted use cases, but also supporting on-premises deployments. These deployment options are omni-channel with mobile, mobile web, desktop, kiosk, terminal, and scanner options. Most major cloud vendors are supported and is cloud agnostic. It takes a microservice approach and uses containers for deployment pipelines. Data centers are in Australia, US, Ireland, and Germany. SDKs are available for customer to configure the solutions into their own UIs.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

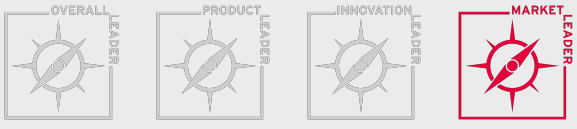
Strengths

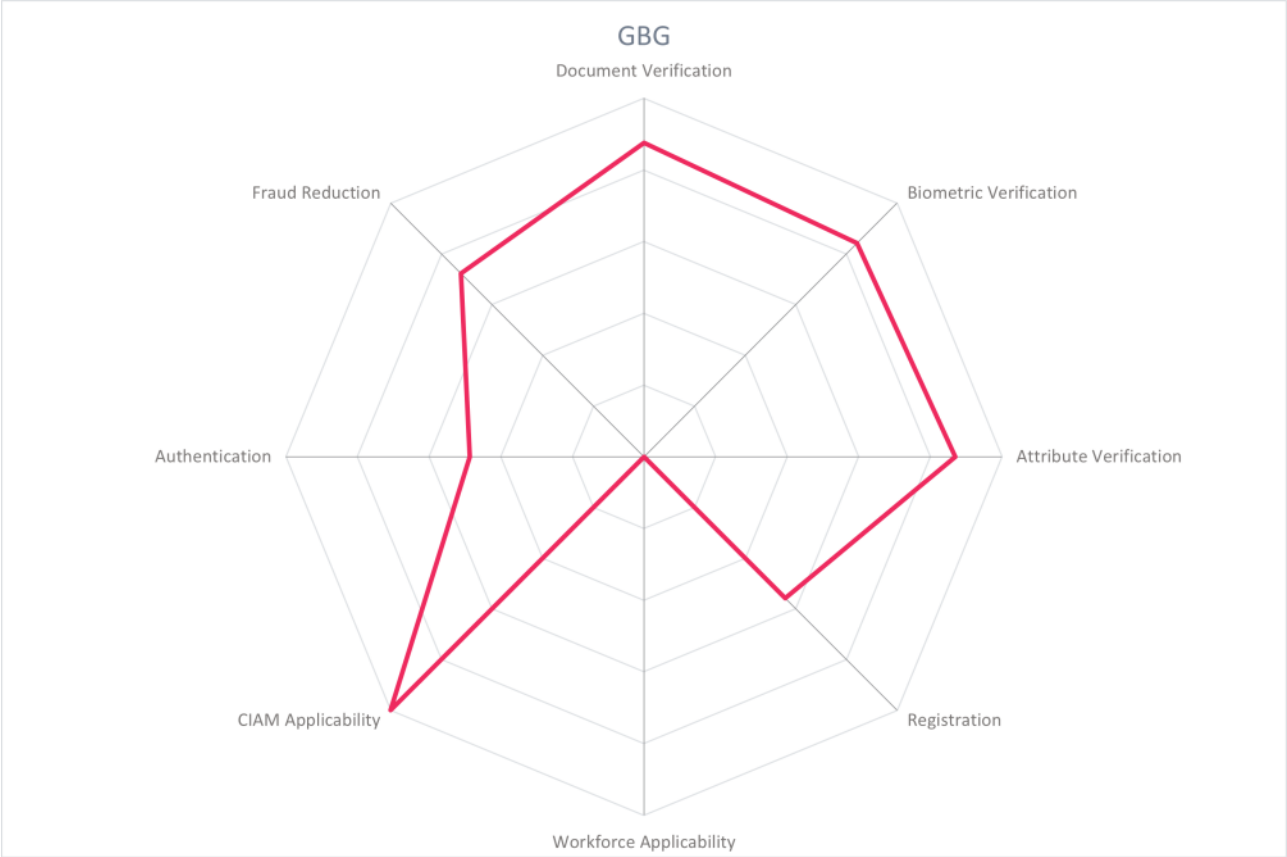
- Supports remote and in-person verification flows
- Has a strong regional Data Network for identity attributes
- NFC functionality for reading embedded chips
- Orchestration of user journeys is available with data triangulation
- ISO 27001 certified, and iBeta certified for Presentation Attack Detection (PAD)
- Can achieve eIDAS High and NIST IAL3
- All major cloud providers are supported

Challenges

- Adaptive authentication could be used to create access policies
- Is growing the product capabilities through organic development and acquisitions, not all products are completely integrated yet
- Primary focus on the North American, UK, and APACmarkets

Leader in




GBG
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.4 HID Global

HID Global, part of the ASSA ABLOY group, was founded in 1991 and is based in Austin, Texas, USA. HID Global provides IAM solutions, and also designs and prints passports, produces physical access controls systems, RFID tags and readers, biometric readers, and mobile apps capable of remote identity verification. Their intersection of IAM, biometrics, and SDKs allows them to perform identity card issuance for numerous organizations. The Identity Verification Service, supported by the Authentication Platform and Risk Management Solution, offers fraud prevention components including ID proofing, credential and device intelligence, behavioral biometrics, user behavioral analytics (UBA), and bot detection.

HID Global provides identity assurance verification and credential issuance services. Government and enterprise customers can utilize HID Global for authoritative lookups, remote document verification, and electronic credential assignment. For remote identity proofing scenarios, users utilize the smartphone app to scan and register the authoritative documents, take selfies, and perform real-time biometric matching. HID can assess the validity of over 13,000 documents, checking against government agencies or using ML to assess the documents. Users initiate and complete identity verification via the customer website or app, supported by SDKs. Users provide requested information with manual data entry, or auto-filled forms and scan their government-issued identity document with OCR and read the MRZ, and conduct onboarding and a liveness check. The facial biometric template that is onboarded is matched against the photo in the identity document. Parallel to these steps, HID captures device identifiers and other risk factors and determines a level of risk associated with the identity verification transaction. Once these processes are passed, an account is opened for the user and credentials can be issued.

When the user returns to the customer's platform, they may authenticate using HID's Authentication Platform, which supports a variety of authenticators, one of the options being to use the biometric template collected at onboarding to leverage the identity verification process for authentication -- this depends on customer preferences for storage and retention of biometric templates. The Authentication Platform utilizes in-network compromised credential intelligence with support from the Risk Management Solution. When the user accesses the customer app via their mobile device, passive authentication can be used with indicators of location, device, time, presence of (or lack of) malware. A risk score is calculated and a decision is made based on the customer's thresholds and weights assigned to risk attributes. The score output ranges from 0-1000 with four major action recommendations. The policy authoring interface is flow-chart driven. The fraud analyst interface is very intuitive and includes a detailed timeline view to expedite investigations. The solution does not offer integration with 3rd-party ITSM or SIEM systems. Customer apps communicate via REST APIs. JWT, OAuth, OIDC, and SAML can be used for API authentication. External feeds of compromised credential intelligence are not yet considered. HID Global's UBA functions encompass full transaction history details. Per-tenant crypto keys are managed to promote maximum data security.

HID Global is a market leader in authentication solutions. Their focus is on B2C use cases in the finance and healthcare industries and providing G2C solutions for government agencies around the world. In fact, some implementation partners package HID Global Authentication Platform to serve as the consumer front-end for their "bank-in-a-box" offerings. HID Global attests and/or has certified on FIPS 140-2, ISO 27001,

ISO 27018, SOC 2 Type 1 and SOC2 Type 2. Inclusion of 3rd-party intelligence sources in the risk evaluation would strengthen the offering.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

HID®

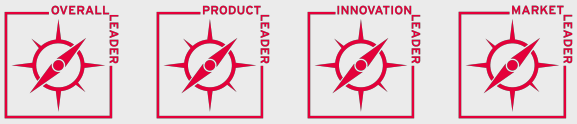
Strengths

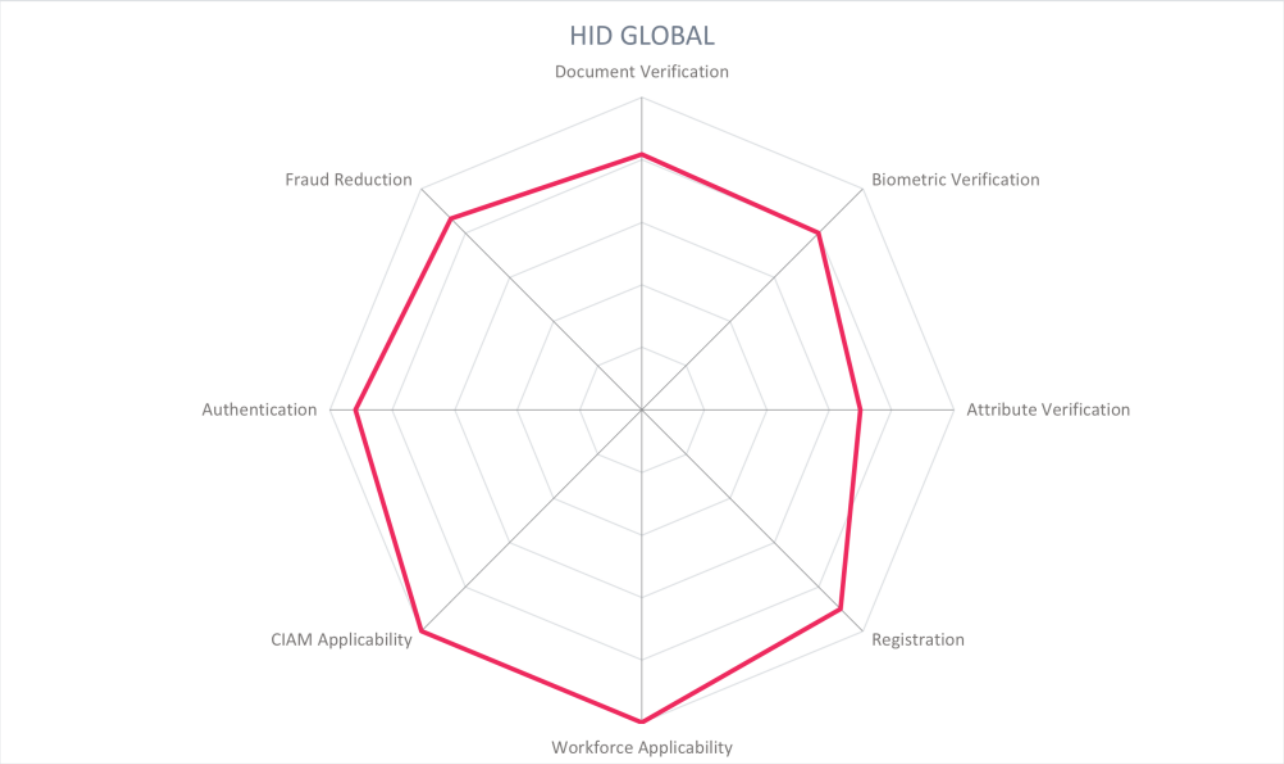
- FIDO 2.0 and FIPS 140-2 certified components
- ISO 27001, 27018 and SOC 2 compliant
- Has identity assurance and strong credentialing capabilities, including some government IDs
- App for remote document verification
- Comprehensive device intelligence can be collected using secure SDK
- Risk engine can output to payment processing services
- Incident response and site takedown services
- Language can be localized with app SDK

Challenges

- No OOTB connectors for SaaS apps
- No PAM interoperability
- Risk engine does not interoperate with external authorization systems
- Internal-only compromised credential intelligence
- Document validation checks could expand to include stolen and/or synthetic identities
- Does not yet support NFC for reading embedded chips of eIDs/biometric passports

Leader in




HID GLOBAL
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.5 IDEMIA

IDEMIA is the product of a history of mergers and acquisitions with over 70 years of experience in identity. It exists in its current for 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, Mississppi, 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.

The Digital ID suite covers many offerings and modules, one of them being the Identity Proofing and Verification which leverages 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 an active liveness 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 Apple Wallet. 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 customer, 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	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

IDEMIA

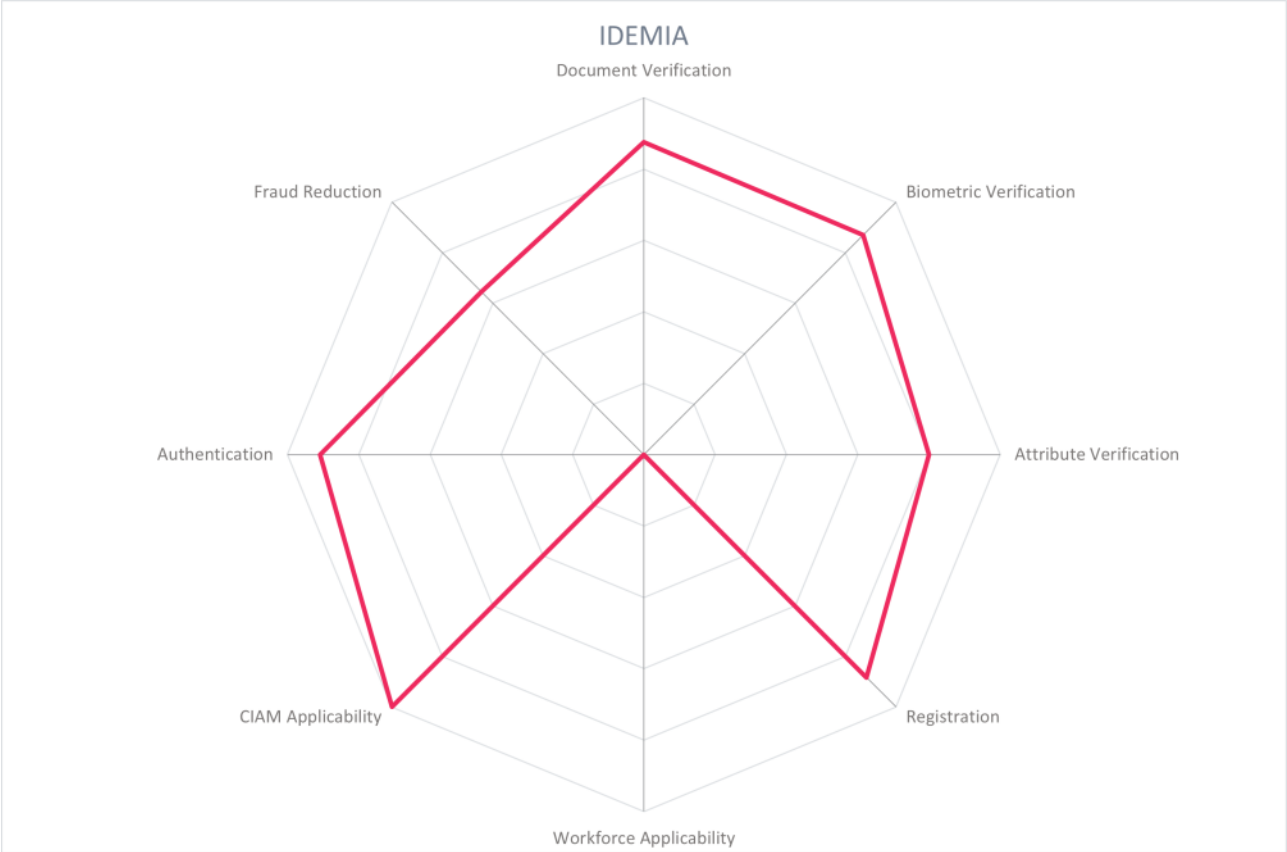
Strengths

- 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

Challenges

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

Leader in


IDEMIA
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.6 iProov

iProov was founded in 2013 and is headquartered in London, UK. Its Biometric Face Verification, Genuine Presence Assurance, and Liveness Assurance technologies support a suite of products: iProov Enroller, iProov Face Verifier, and iProov Basic Face Verifier. iProov is a focused biometric verification vendor that is supported by partners to complete document verification, attribute verification, authentication, and orchestration for a full-service identity verification solution.

iProov Enroller works with partners to scan and verify the user's identity document using OCR and NFC to intake and analyze data. Upon verification, the photo from the identity document is shared with iProov and synchronized keys stored with the customer, with defined data retention policies and encrypted at rest and in transit. The biometric components are handled by iProov's proprietary technology: The user takes a selfie which is matched to the photo extracted from the identity document. This biometric template, stored with iProov, is the basis to establish liveness and genuine presence, and to later authenticate.

iProov's Face Verifier (both basic and regular versions) use the onboarded biometric template for future authentications and transactions. Basic Face Verifier uses iProov's face matching and fraud detection algorithms to determine if the user is the one described in the identity document for liveness detection. The Genuine Presence Assurance product adds an additional layer of protection against deepfakes or digital injection attacks. It uses iProov's patented Flashmark technology to generate a one-time biometric that cannot be reused or falsified to ensure that the user is present during the transaction. While the user takes a selfie of themselves, a sequence of colored light is reflected on their face. Along with the typical facial matching between a biometric template or identity document, the sequence of colors is analyzed to ensure that no malicious file was injected such as deepfakes or presentation attacks. The product conforms to eIDAS High. The biometric profile can be stored by iProov for future authentication.

The Liveness Assurance and Genuine Presence Assurance products both use a selfie abstraction feature to reduce drop-off and selfie retakes. By presenting the selfie as a sketch and not as a realistic photo, the user is less likely to be judgmental of their appearance and retake the selfie unnecessarily. The products are cloud-based -- including authentication -- which allows users to authenticate using different devices without having to enroll a new device. 1:1 facial matching is used for the solutions.

iProov products are deployed as cloud or managed services with support for multi-cloud, multi-tenant environments and the major cloud providers. An SDK is provided to integrate iProov verification into the customer's applications, inclusive of mobile, desktops, laptops, tablets, and kiosks. Customization is primarily used for specialized user journeys, and roll-out time is typically a few days to weeks depending on customer requirements. Data centers are in the UK, Netherlands, Australia, USA, and Singapore, with instances in other regions provided as necessary. iProov adheres to GDPR principles.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●

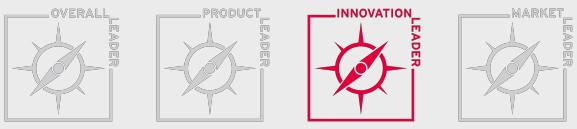
Strengths

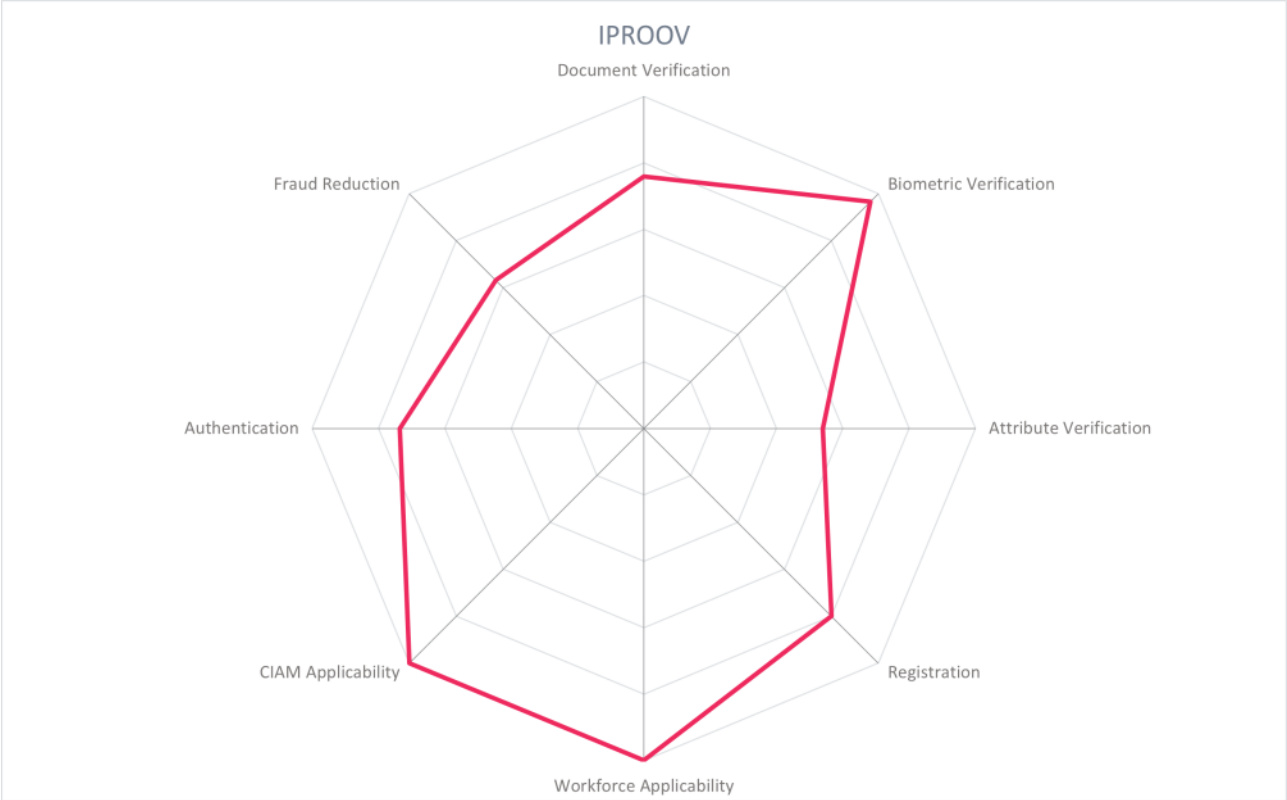
- Supports multi-cloud environment
- ISO 27001 certified
- PAD Level 1 and Level 2 certified
- Strong usability features such as abstracted selfie view
- Actively monitors training datasets for bias and deviations that correspond to ethnicity, gender, or age
- Supports risk-adaptive and step-up authentication
- Biometric verification of palms is also supported
- Uses 1:1 facial matching only

Challenges

- Could expand offering by including sanctions, blacklists and PEP checks for KYC
- Could increase the fraud reduction offering with user behavior analytics
- Integration with SIEM would strengthen the products
- As a biometric authentication system, does not support 0Auth2, SAML and OIDC
- While storage of biometric templates is encrypted with customizable data retention/deletion policies, it may not fit customer's risk appetite

Leader in




IPROOV
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.7 Microsoft

Microsoft, founded in 1975 and based in Redmond, USA, is a familiar figure in hardware and software, digital services, and cloud infrastructure businesses. In August 2022, Microsoft has released Entra Verified ID product (based on Verifiable Credentials and Decentralized Identifiers) as generally availabile 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.

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 Azure AD 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. 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	● ● ● ● ●
Functionality	● ● ● ● ○
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

Microsoft

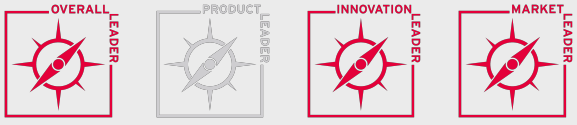
Strengths

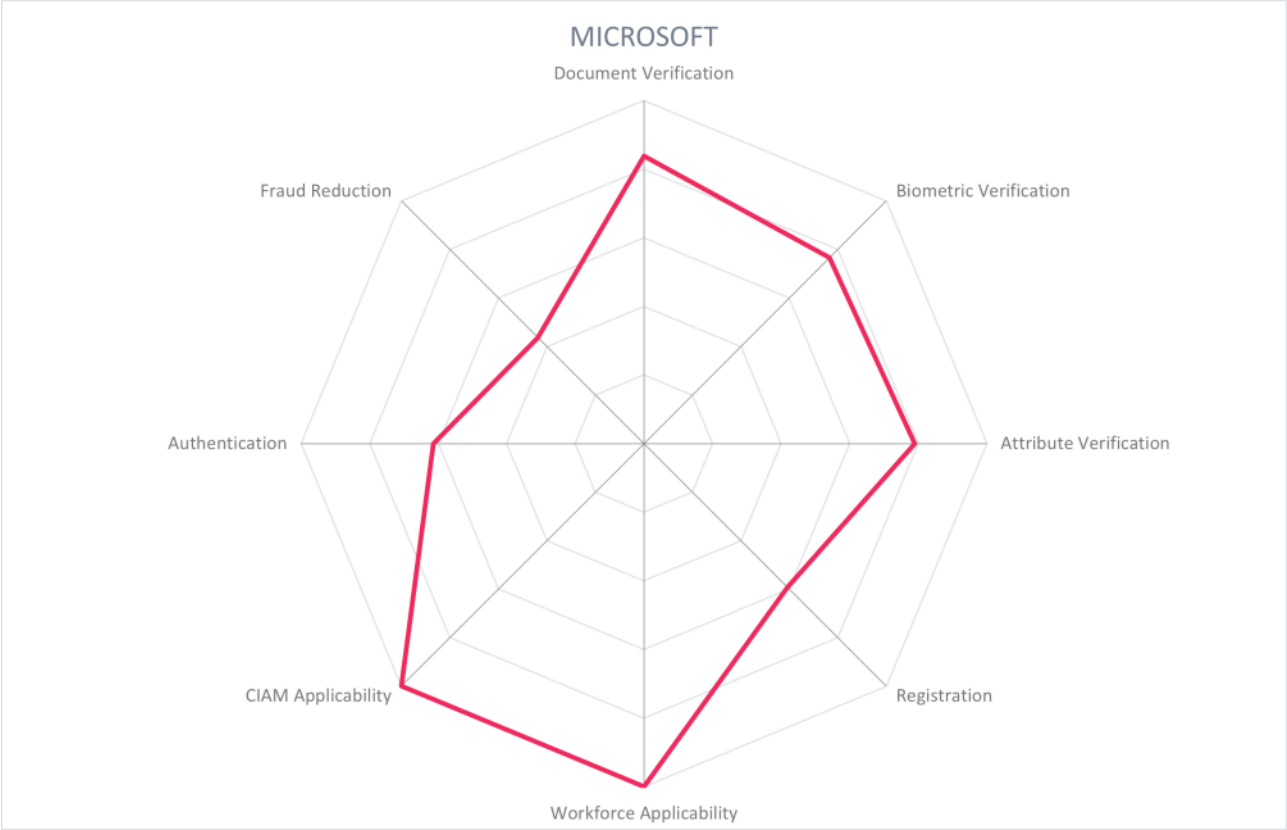
- A strong market player with path to attaining critical mass of users
- Close collaboration with DIF and W3C to establish standards
- Open-sourced the Verifiable Credential SDK for open access to and innovation in secure digital identity exchange
- Participates in interoperability groups
- Supports 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
- Could have a stronger fraud reduction offering

Leader in




MICROSOFT
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.8 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, 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 along with KYC/AML functions, strong customer authentication (SCA), biometric authentication, fraud monitoring and other security functions. 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.

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 trust scheme framework as an Identity Service Provider and Orchestration Service Provider. 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. With capacity to expand regionally and into electronic signature use cases, OneID is a compelling option for those looking to leverage online banking for verified identity.

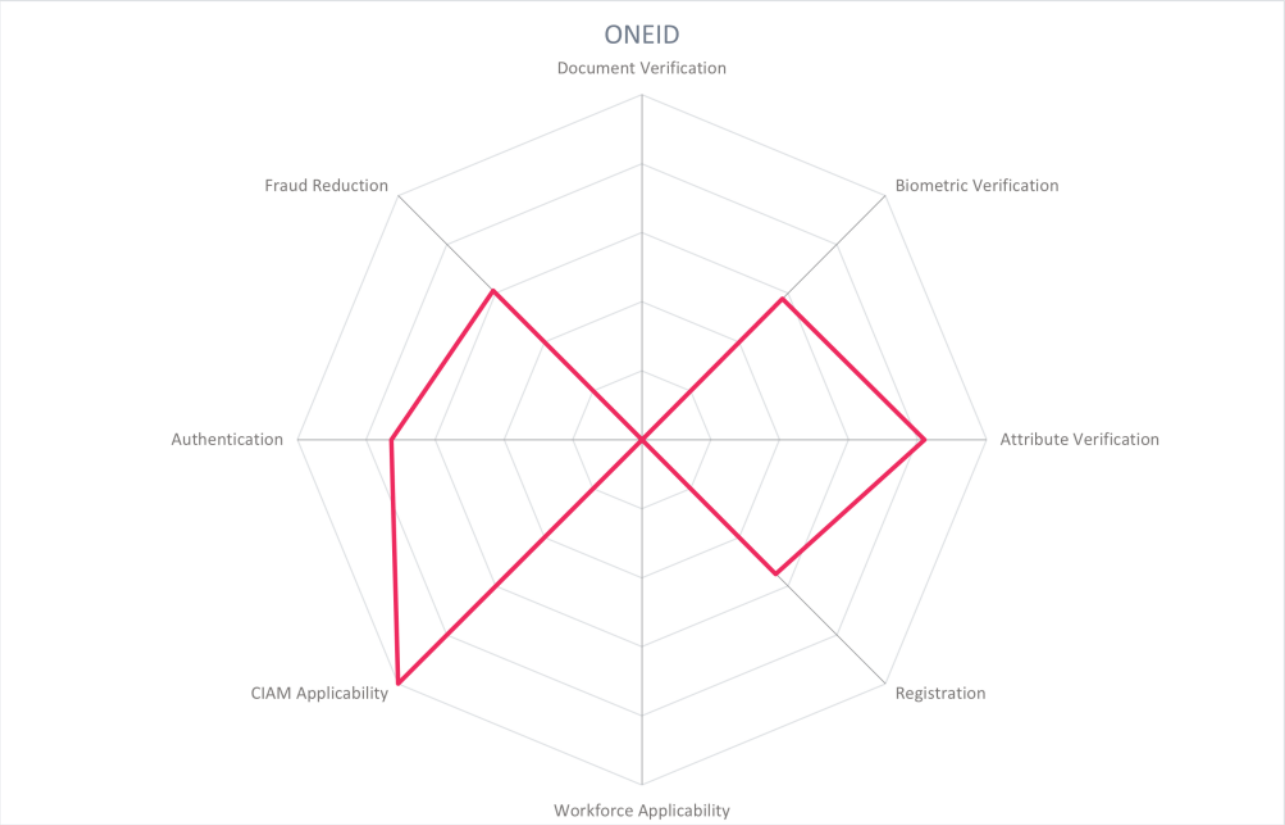
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●●○

Strengths

- Supports DCMS GPG 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 support additional authentication standards such as OAuth2, and FIDO2
- Could offer connectors to SIEM
- Focused on serving the UK market only


ONEID
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.9 Onfido

Founded in 2012, Onfido is based in London, UK. It provides fully automated as well as hybrid identity verification solutions, supported by its proprietary AI for document verification, biometric matching, and fraud signal detection. The Real Identity Platform serves primarily CIAM use cases ranging from onboarding and enrollment, deterring fraud, authentication, and step-up verification. Onfido provides wide geographical coverage for document verification and serves customers globally.

Onfido's Real Identity Platform provides automated identity verification at multiple points along a user journey: during onboarding, authentication, or during high-value transactions. The platform contains the Verification Suite made up of document verification, biometric verification, data verification, and fraud verification. This suite of verifications is flexible and can be configured to meet local requirements using Onfido Studio with no-code workflows, enabling businesses to customize which verification signals they deploy and when. Onfido's proprietary Atlas AI enables automation of identity verification and powers the risk and decisioning engine. The platform contains a no-code UI, analytics and dashboarding, and API support.

During an onboarding process, a user is prompted to scan an identity document with their mobile device. The document is first classified to determine the type and country it is from, then data is extracted both for verification against authoritative registries and for form auto-filling before data fraud and visual fraud analysis is performed. NFC verification supplements if the identity document has an embedded chip. Biometric verification is done by the user taking a selfie or asynchronous video, which is then analyzed for spoofing attacks, liveness detection, facial matching with the identity document and checking against a database of known fraudsters. Onfido's suite of data verifications check user data against authoritative sources such as the global sanctions watchlists, identity record databases, and SSN and the American Association of Motor Vehicle Administrators (AAMVA) for US users. Fraud detection is applied, including checking signals for device integrity, IP address, and geolocation signals. The results of the document, biometric, attribute, and fraud signals are fed to the risk engine which returns a verification result to the customer within approximately 10 seconds. The identity verification solution helps customers align with NIST IAL2.

The verified biometric information collected at onboarding can be reused for authentication. Use cases such as high-value transactions or account recovery are particularly suitable since the biometric template is linked to the verified identity. To use, the user takes a face scan, which is matched against the biometric template they provided during onboarding.

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

Security	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●

onfido

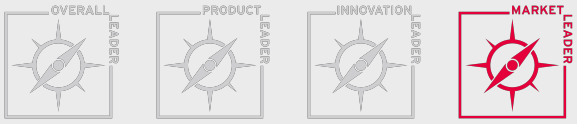
Strengths

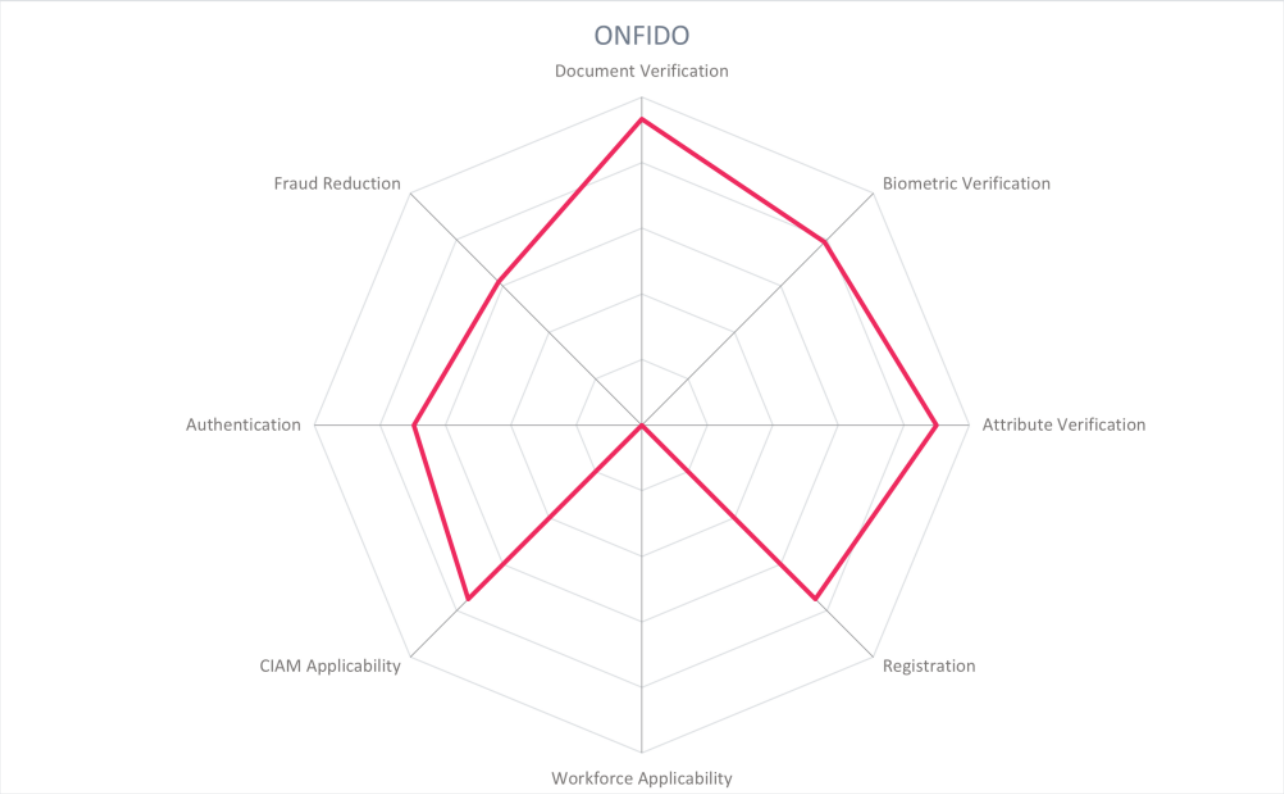
- Certified ISO 27001 and SOC 2 Type II compliant
- ? WCAG 2.1 compliant with accessibility SDKs and considerations for users with disabilities
- Strong go-to-market model using a partner ecosystem to introduce them to a specified geography or market
- Worked with the ICO in its Regulatory Sandbox on compliant handling of training data
- Cross-checks documents against proprietary compromised document database
- Onfido technology is integrated in many other identity verification solutions
- Uses in-house technology for both document verification and biometric verification
- Launched new active liveness solution in September 2022

Challenges

- Integrations with standard authentication sources like OpenID Connect or SAML will improve this solution
- Authentication products require the biometric capture experience to be done via the Onfido SDK, could offer more authentication options
- Does not yet support verified identity to be accessed from multiple user devices
- Only available on Amazon AWS cloud infrastructure
- Not yet accredited for eIDAS levels of assurance
- Not available on premises

Leader in




ONFIDO
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.10 Ping Identity

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 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 3rd 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	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

Ping Identity

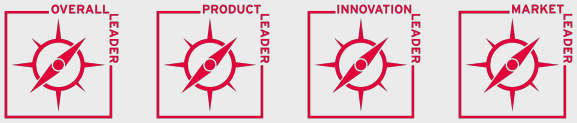
Strengths

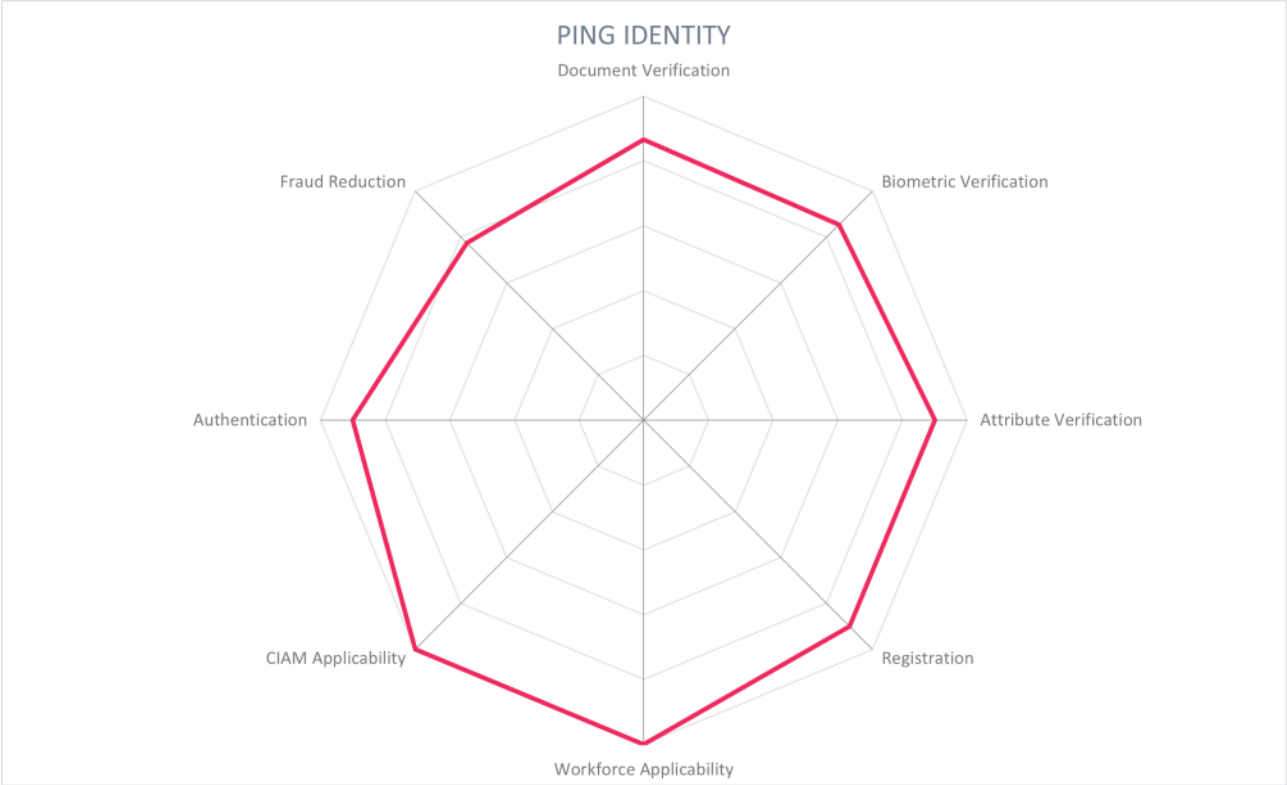
- Able to integrate identity verification into Ping's established platform
- Account and password recovery are possible
- Individual attributes such as date of birth or name are certified
- Ping provides interoperability with its large customer base
- Strong APIs and connectors to other SaaS services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

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 PingOneVerify
- Does not yet provide assistance for incident analysis and/or remediation
- Cloud infrastructure only available on Amazon AWS

Leader in




PING IDENTITY
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.11 Signicat

Signicat is headquartered in Norway and has been delivering identity solutions since 2006. It enables the customer to verify user identities by orchestrating verification steps across many regional partners, packaging identity information and delivering it to the customer. Signicat's Digital Identity Platform offers a suite of Sign-up, Sign in, and Sign it products, leveraging the verified identities of primarily European eIDs for onboarding, authentication, electronic signatures, seals, and time stamps. 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.

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. 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. NIST Identity Assurance Level 2 and eIDAS high can be achieved with the solution.

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. The customer's target assurance level for onboarding and authentication can be customized and determines the strength of verification. 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. The user can authenticate using a variety of authenticators, including eID or by using Signicat's MobileID, compliant with PSD2/SCA.

The solution can be offered using all major cloud platforms, Signicat does not hold any customer data, but it is stored based on customer requirements. Signicat's standardized APIs can be web-based or built into a customer application.

Security	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

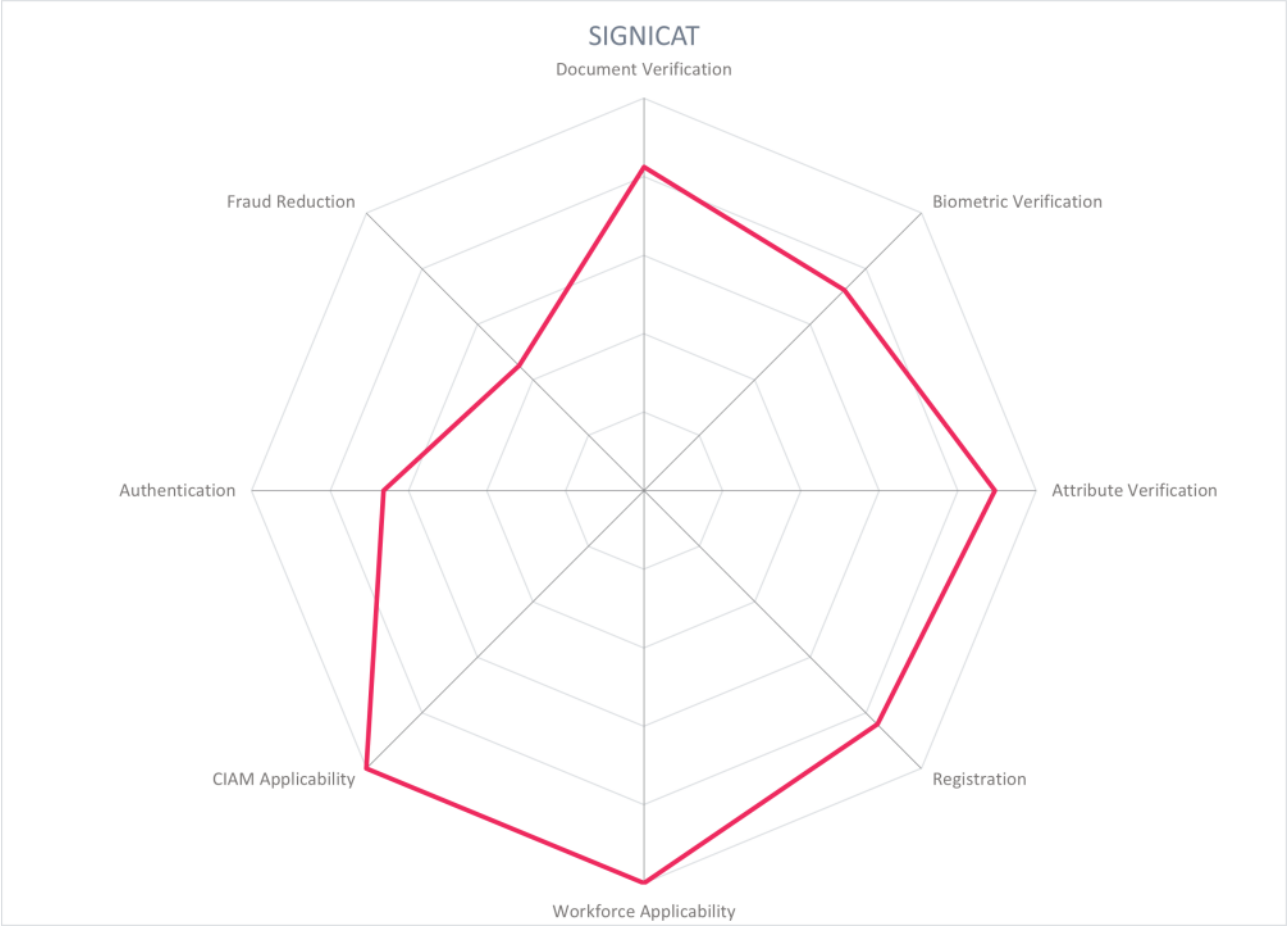
SIGNICAT

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


SIGNICAT
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.12 Thales

Thales Digital Identity and Security (DIS) division, formerly called Gemalto, is based in Paris, France, and supports governments with their digital ID schemes with a wide portfolio of mobile and wallet ID solutions for citizens to provide a digital online identity. 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 drivers 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 can provide both the user identity wallet and the verifier app. Offline verification of identity credentials is also supported. 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	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

THALES

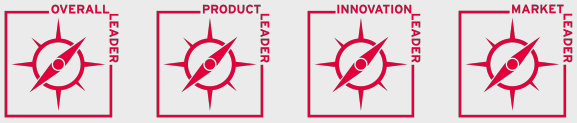
Strengths

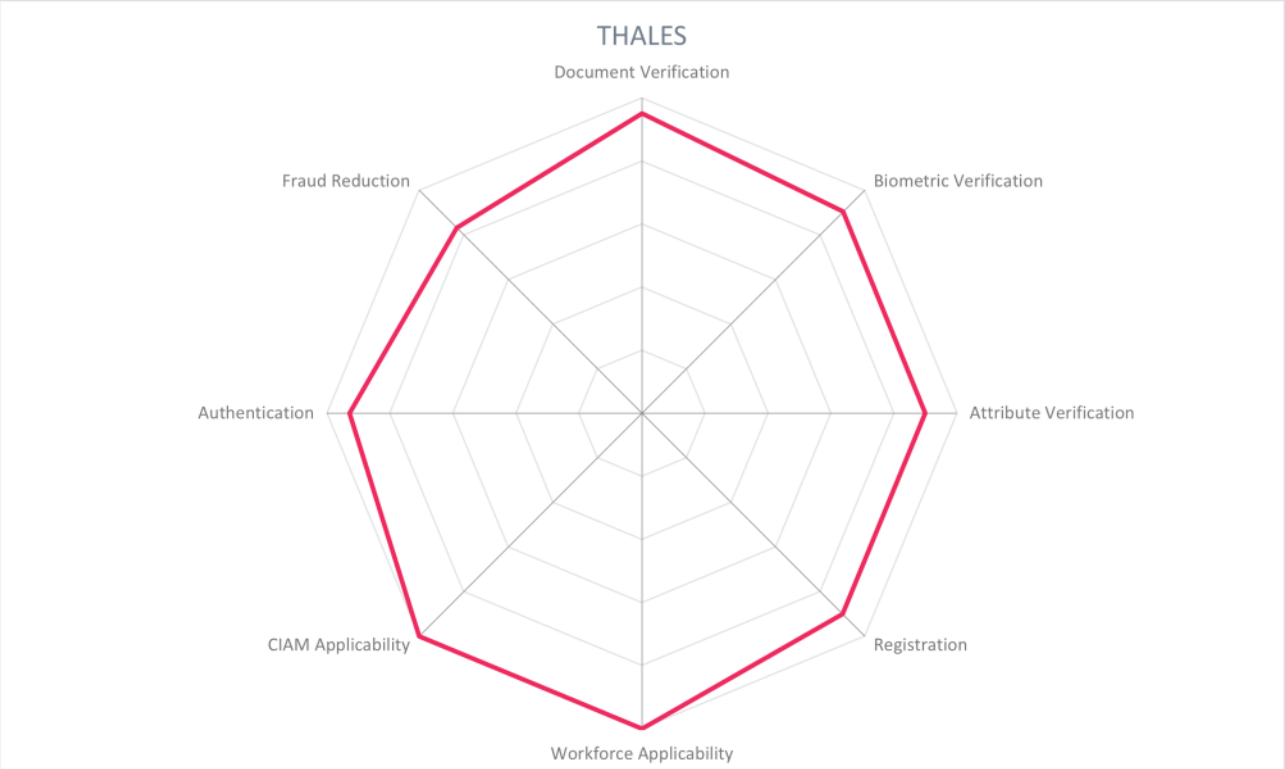
- Strong case for verification, integrating use of physical IDs with reusable digital attributes
- Supports high assurance PKI use cases, strong representation in the banking and government sectors
- Identity verification and attribute sharing is possible offline
- Device synchronization is possible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

Challenges

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

Leader in




THALES
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.13 TrustBuilder

TrustBuilder is based in Gent, Belgium and was founded in 2017 with development beginning in 2016. It provides a full-service identity solution consisting of onboarding, verification, authentication, and authorization. Analytic insights and crafting of the user journey are also available. It joins identity providers (IdPs), service providers, and security providers together with an orchestrator and service catalog, provides MFA, and provides monitoring capabilities.

To onboard and verify users, TrustBuilder federates with different official IdPs of European countries like EHerkenning, itsme, and France Connect, as well as global social networks. Federation through eID IdPs bring verified identity attributes to the TrustBuilder identity service. If additional identity verification and KYC is required by the customer, TrustBuilder enables it by leveraging partners to scan the user's passport or drivers' license and do biometric onboarding. Document verification and biometric onboarding is completed by partners including Signicat, Veridas, and Onfido and are embedded in the product, providing regional coverage of over 100 countries. Customers may choose custom identity verification vendors to integrate the product with. Additional identity attributes can be verified by checking against national registries, by verifying Verifiable Credentials, and through data aggregation with credit bureaus, telecom, banks, universities, insurance, and employers.

TrustBuilder works with the concept of policy-driven access control based on personas, building on Attribute-Based Access Control (ABAC). A persona refers to a person's role or relationship to an organization with sub-attributes, allowing rules to be centered on personas rather than individual attributes. A single user will have multiple attributes, such as being an employee and part of a particular department, as well as a private customer in other contexts. That single user can login to the system and select the persona they are currently operating under, which provides fine-grained access to resources. If the user has already authenticated, they can switch personas without reauthenticating. Delegated administration is supported, also using the persona-driven access control and policy engine, building off information from external IdPs and databases.

Multifactor authentication is provided, consisting of TrustBuilder's Bring Your Own Authentication (BYOA) integration with numerous IdPs, push notification, and/or biometrics including server-side facial recognition, allowing the user to login with the IdP of their choice. TrustBuilder has a stand-alone authenticator app or provides an SDK for the customer's mobile app. Step-up, adaptive, and risk-based authentication is supported, as and allows for strong authentication through a desktop application or a users' registered web browser for independence from a mobile device. A self-service module allows users to register all available identity providers and MFA solutions, change their password, update credentials, manage consent, and other information. TrustBuilder has advanced orchestration and a configurable policy engine that specifies identity data to be verified, the internal and external databases used, and workflows. The service catalog contains out of the box integrations with IdPs, services, and security services.

TrustBuilder runs in the cloud using Google Cloud Platform with data centers in Belgium and France or can have a local component on premises. Mobile SDKs for Android, iOS, and Huawei, web components, and

APIs are provided. No personal data is stored on the user's mobile device, but instead in TrustBuilder's cloud server using HSM encryption or on the customer side.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

trustbuilder®

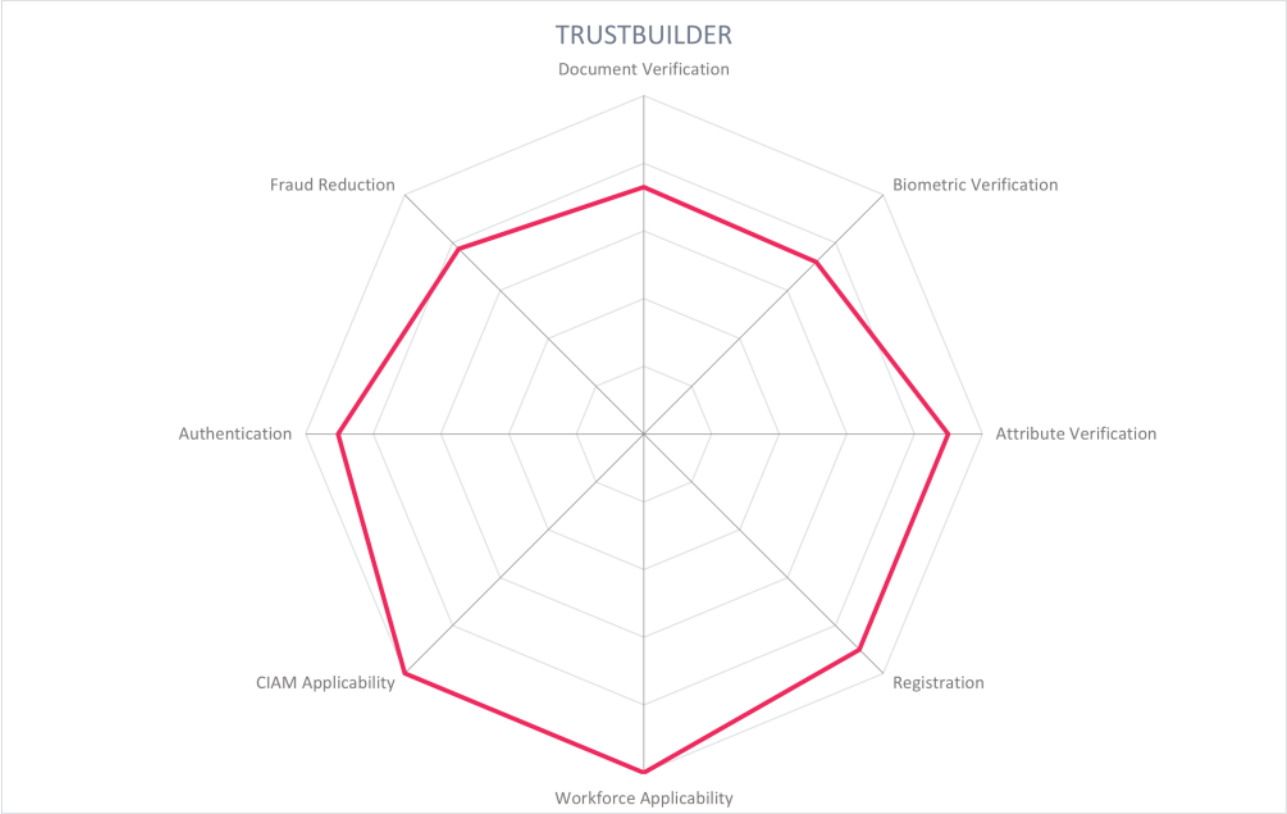
THE POWERFUL IAM

Strengths

- Pre-integrated IdPs and connectors
- Strong orchestration capabilities
- Compelling use of persona-based access control
- Strong federation model for European IdPs
- Growing coverage for workforce IAM use cases, especially supporting cloud applications
- Delegated administration is supported
- Various options for MFA
- OAuth2, SAML, OpenID Connect, JWT, Kerberos, ADFS, and WSFed are supported
- Strong fraud reduction capabilities including behavioral biometrics

Challenges

- Currently focuses on the EU market only
- Could expand the document and biometric verification partner ecosystem for wider country coverage
- No support for device synchronization is yet provided
- A small but growing company


TRUSTBUILDER
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.14 Verimi

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. 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 drivers 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.

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.

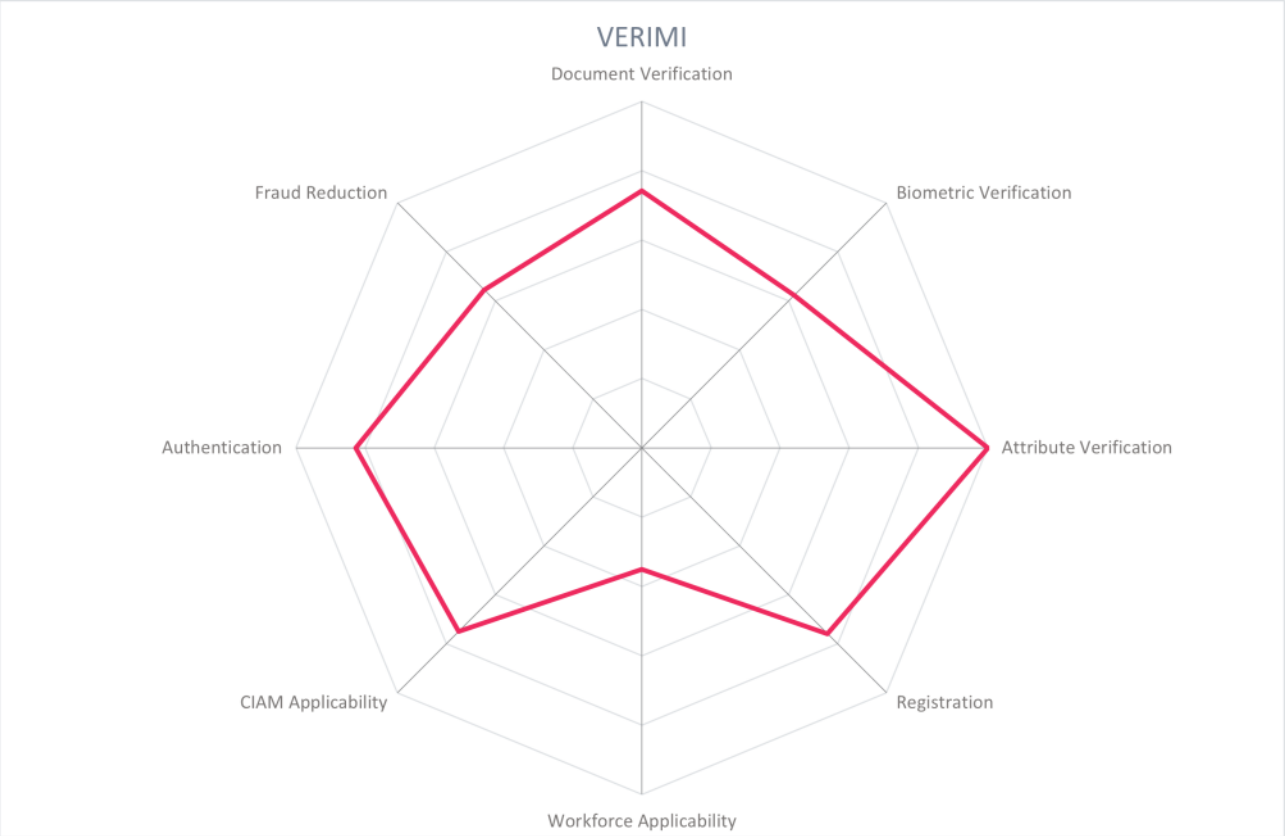
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●○

Strengths

- Strongly contributes towards a reusable digital ID with selectively sharable attributes
- Digital wallet can be accessed from desktop, mobile, or other smart device.
- 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
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

5.15 Yes

Yes was founded in 2016 and is based in Switzerland. Yes is an Open Banking ecosystem, composed of 1,000 active bank partners and over 4,000 passive bank participants. The 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 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.

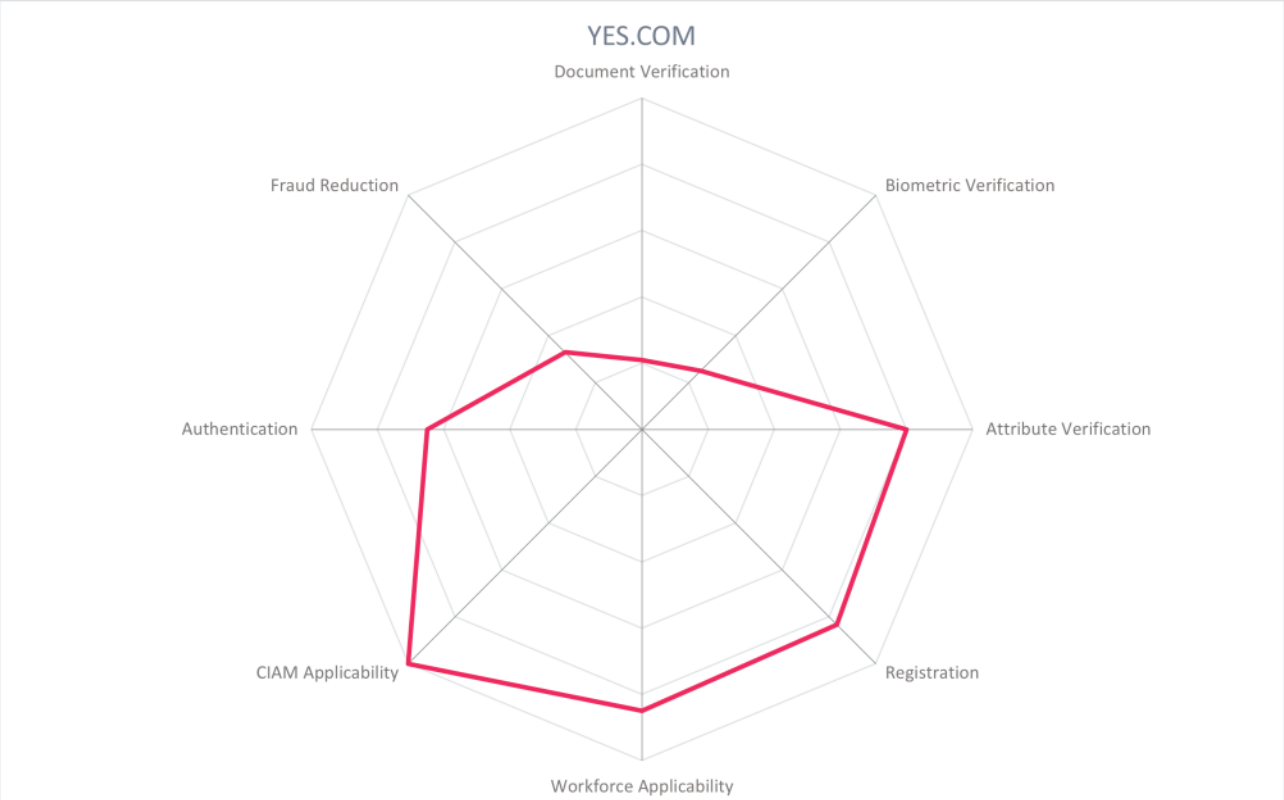
yes®

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
Document Verification
Biometric Verification
Attribute Verification
Registration
Workforce Applicability
CIAM Applicability
Authentication
Fraud Reduction

6 Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition, but 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.

- **CallSign** - Headquartered in London, UK, CallSign is a provider of an identity platform that integrates consumer onboarding, authentication, and fraud management in a tightly integrated manner.
  Why worth watching -- CallSign uses AI/ML for risk analysis and supports passive and continuous authentication.
- **cidaas** - Based in Wimsheim, Germany, cidaas provides identity and authentication solutions. Its ID Validator uses digital-only flows to validate an ID card, passport, or drivers license.
  Why worth watching: cidaas is a vendor working in a highly-regulated country - Germany. Its digital-only identity verification products must take these regulations into consideration.
- **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.
- **Devcode Identity** - Based in Stockholm, Sweden, Devcode Identity provides an identity platform to verify customers using eIDs and an API hub to video and document-based verification services. Additional services include address verification, registry checks, PEP and sanction checks, digital signatures, and use of the open banking ecosystem.
  Why worth watching: Devcode Identity is a lean and competitive alternative to vendors featured in this Leadership Compass.
- **esatus** - 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.
Why worth watching: esatus offers a way for organizations to issue and manage employee credentials in a decentralized manner.

- **FacePhi** - based in Alicante, Spain, FacePhi provides a digital identity platform for digital identification and verification, particularly for KYC and AML compliance. Services include onboarding and authentication.
  Why worth watching: FacePhi specialized in biometrics and is expanding in the EMEA region.
- **Hive.ID** - Based in Tallinn, Estonia, Hive.ID combines identity verification and passwordless authentication for a growth-driven identity platform.
  Why worth watching: Hive.ID is using verified identities to drive passwordless authentication initiatives.
- **IdRamp** - Based in Indianola, US, IdRamp enables the organization to issue Verifiable Credentials from numerous data sources as well as orchestrate and coordinate the management of all identity providers and services.
  Why worth watching: IdRamp has a strategic focus on decentralized identity and identity orchestration.
- **Jumio** - Based in Palo Alto, US, Jumio provides enterprises with he means to do KYC checks for individuals, organizations, and employees. Identity verification is integrated into the onboarding process with fully automated solutions.
  Why worth watching: Jumio is an early leader in the Providers of Verified Identity space with valuable experience.
- **Liga** - Based in Denmark, Liga provides a cybersecurity platform that harnesses trusted identities for enterprise workforce use, connecting identity sources with validation systems and authentication factors.
  Why worth watching: Liga uses existing infrastructure to provide verified identities to the workforce.
- **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.
- **Transmit Security** - Based in Boston, US, Transmit Security specializes in passwordless authentication using biometrics.
  Why worth watching: Transmit Security serves both the consumer and enterprise IAM market with passwordless solutions.
- **Tru.id** - Based in London, UK, Tru.id uses SIM security as a verified attribute to allow enterprises to leverage verified identity attributes.
  Why worth watching: As the Providers of Verified Identity space continues to debate which method is most appropriate for which levels of risk, verified SIM and mobile number could be a compelling option.

- **Veridas** - Based in Tajonar, Spain, Veridas does customer identity verification for onboarding, document, and biometric verification.
  Why worth watching: Veridas include voice biometrics, opening interesting doors to new use cases.
- **ZignSec** - Based in Sweden, Zignsec is an orchestration platform to complete KYC processes including identity verification, fraud detection, and onboarding.
  Why worth watching: Zignsec offers a coordinated solution for complex, cross-border requirements.

7 Related Research

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: HID Global Fraud Prevention Offering - 81104
Executive View: Signicat - 72537

Methodology

About KuppingerCole's Leadership Compass

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 Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

Figure 1: The Interplay of Providers of Verified Identity Market Segment with Other Market Segments

Figure 2: Flows of Data While Providing Verified Identity - Three Models

Figure 3: Overall Leadership Rating for the Providers of Verified Identity Market Segment

Figure 4: Product Leadership in the Providers of Verified Identity Market Segment

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

Figure 6: Market Leadership in the Providers of Verified Identity Market Segment

Figure 7: The Market/Product Matrix for the Providers of Verified Identity Market Segment

Figure 8: The Product/Innovation Matrix for the Providers of Verified Identity Market Segment

Figure 9: The Innovation/Market Matrix for the Providers of Verified Identity Market Segment

Copyright

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.