

Identity Verification

Guillaume Teixeira

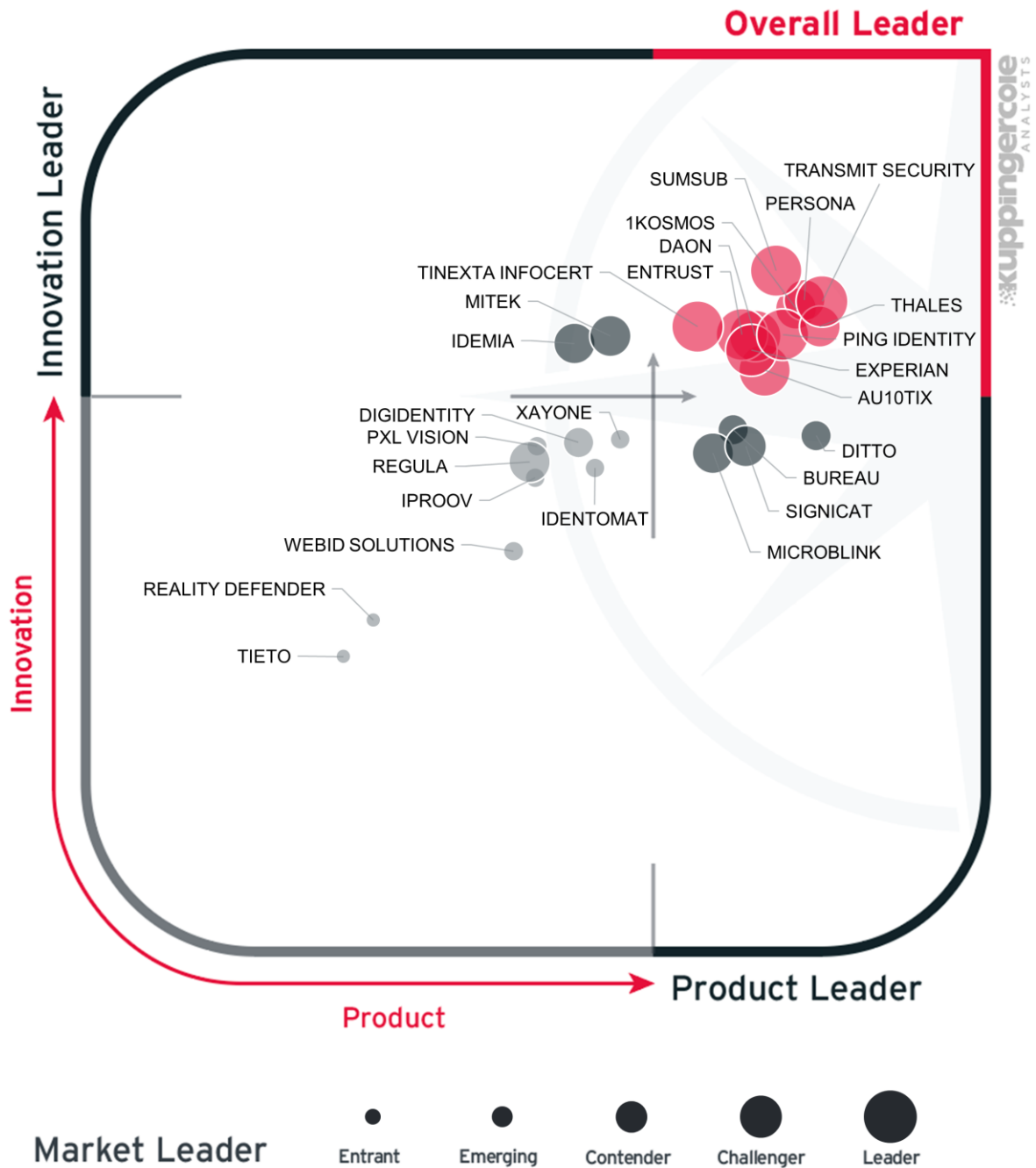
September 10, 2026



LEADERSHIP
COMPASS
2026

Leadership Compass

Identity Verification 2026



This KuppingerCole Analysts Leadership Compass provides an overview of the Identity Verification market and a compass to help you find a solution that best meets your needs. It examines solutions that establish that a person is who they claim to be during onboarding, workforce verification, account recovery, step-up verification, and age assurance. These solutions verify government-issued documents and bind them to the person through biometric verification and liveness detection. Some also use supervised video verification, eID, reusable verified identities, or authoritative data sources. They must detect deepfakes, injection attacks and forged documents, and provide the workflow and integrations needed to embed verification in business processes. The report assesses how well these solutions meet the needs of organizations in North America and Europe that must verify identities with confidence and meet KYC, AML and other regulatory obligations.

Contents

Contents	3
Introduction	6
Key Findings.....	7
Market Analysis.....	8
Delivery Models	9
Required Capabilities	9
Leadership	12
Overall Leadership	12
Product Leadership	14
Innovation Leadership	16
Market Leadership.....	18
Product and Vendor Evaluation.....	20
1Kosmos – 1Kosmos Verify.....	21
AU10TIX – AU10TIX Identity Verification Platform.....	25
BUREAU – IDENTITY VERIFICATION.....	29
Daon – xProof	33
Digidentity – Digidentity Identity Wallet and eHerkenning	37
Ditto – Ditto Verify.....	41
Entrust – Entrust Identity Security Platform.....	45
Experian – CrossCore on Experian Ascend Platform.....	49
IDEMIA – Identity Proofing Platform	53
Identomat – Identomat.....	57

iProov – iProov	61
Microblink – Identity Intelligence OS	65
Mitek – Mitek Verified Identity Platform (MiVIP)	69
Persona – Persona Identity Platform	73
Ping Identity – PingOne Verify and PingOne Recognize	77
PXL Vision – PXL Ident	81
Reality Defender – Real Suite (RealScan, RealCall, RealMeeting, RealAPI)	85
Regula – Regula IDV Platform, Document Reader SDK, Face SDK	89
Signicat – VideoID, ReadID, eID and Wallet Hub, and Signicat Flow	93
Sumsb – Sumsb User Verification Platform	97
Thales – Identity Verification Suite, OneWelcome Identity Platform	101
Tieto – Identity Proofing	105
Tinexta Infocert – TOP (Trusted Onboarding Platform)	109
Transmit – Mosaic Platform	113
WebID – Identity Verification Product Suite	117
XAYONE – XAYONE ID Verification (Trust Platform)	121
Vendors to Watch	125
AccuraScan	125
CLEAR	125
Cognito	125
DuckDuckGoose AI	126
Element	126
FACEKI	126
Facephi	127
GBG	127
HyperVerge	127
iDenfy	128
IDENTT	128
Identityum	128
Incode	128
LexisNexis IDVerse	129
Jumio	129
Nametag	129

Nomidio	130
Microsoft.....	130
OARO.....	130
Prembly	131
ProofID	131
Prove.....	131
ShareID	132
Shufti.....	132
Smile Identity.....	132
Toppan iDGate.....	132
Trustmatic.....	133
uqudo	133
Veratad Technologies.....	133
Veriff.....	134
Verimi	134
Veritran.....	134
VU Security	135
Yes:ID	135
Related Research	136
Copyright	136

Introduction

Identity verification has undergone a significant transformation in recent years from longstanding manual methods to fully remote, automated processes. These developments follow the market changes of increasingly global consumer user bases, increasing fraud, compliance requirements, and demands for secure but friendly user experiences. KuppingerCole Analysts has been at the forefront of these developments, tracking how identity verification capabilities evolve to meet organizational needs and align with the ongoing shift to user-held digital identities.

Identity verification is no longer limited to regulated customer onboarding: it now supports consumer and workforce onboarding, account recovery, step-up verification, high-risk transaction approval, fraud and risk-led identity checks, re-verification, and age assurance across digital journeys. This Leadership Compass serves as the guide to the current market state, major vendors, and an assessment of their capabilities.

Market drivers from four directions apply pressure on organizations to increase the quality of their identity verification processes: fraud increase, compliance requirements, user expectations, and technological advancements. Account opening and takeover fraud are increasing, in part from the weaponization of generative artificial intelligence (GenAI) for deepfakes, injection attacks, and AI-edited document images. There are long-standing compliance requirements like Know Your Customer (KYC), Anti-Money Laundering (AML), and other related requirements, but intensified attention to age verification for digital services makes identity verification solutions essential for many organizations that would not typically require identity verification.

Large-scale initiatives in the European Union (EU), where member states are required to offer European Digital Identity (EUDI) wallets to citizens, and comparable programs globally intensify the demand for reliable remote identity verification and establish reusable verified identity as a distinct market segment. KuppingerCole Analysts views the identity verification market as three closely related segments: Full-Service Identity Verification, best-of-breed Identity Verification, and Reusable Verified Identity. All industries are expected to deliver digital onboarding and services in a secure manner, ranging from consumer-facing onboarding, authentication, account reset, multi-channel support from in-branch, call centers, and online, purchases and high-risk transaction use cases to onboarding and authenticating the workforce including full-time employees, contractors, freelancers, suppliers, and more. Technology advancements on document verification, document forensic analysis, AI-supported matching (of faces and documents), and fraud detection of an increasingly varied list of attacks from deepfakes to injection attacks make identity verification solutions more capable and enterprise ready than ever before.

KuppingerCole Analysts forecasts that the market size for identity verification will reach \$22.22 billion USD by 2026, representing a compound annual growth rate (CAGR) of 20.70%. The market is projected to grow to \$50.07 billion USD by 2030. KuppingerCole Analysts also expect to see a sharp increase in remote identity verification usage as organizations react to the increasing threats of fraud, compliance demands, and

opportunities for new business related to the transition to user-held digital identities. Consumer-facing organizations in financial services and fintech/crypto/foreign exchange are typical buyers of identity verification services. However, this is expanding across digital services including gaming and betting, eCommerce and marketplaces, telecom, social media and streaming services, and regulated industries such as government and public services, healthcare, and travel. Although market adoption is still early, there is a strong use case for organizations to verify and onboard their workforce and contractors with identity verification solutions. This edition assesses vendors primarily in the context of buyer requirements in North America and Europe, the reference regions for demand, regulatory expectations, and market maturity.

To understand our research approach, please refer to the [KuppingerCole Leadership Compass Methodology](#).

Key Findings

What are the top considerations buyers should know about?

- Identity verification is increasingly conducted in fully remote, automated processes, and its use cases have expanded beyond regulated onboarding to account recovery, step-up verification, high-risk transaction approval, workforce onboarding, and age assurance.
- Four main drivers drive the rising need for identity verification services: increasing fraud, compliance requirements, user expectations, and technological advancements.
- KuppingerCole Analysts views the broader market as three closely related segments: Full-Service Identity Verification, best-of-breed Identity Verification, and Reusable Verified Identity.
- Many organizations engage multiple identity verification vendors for coverage, redundancy, and service continuity.
- Identity verification solutions are being adopted across consumer-facing sectors like financial services, gaming and betting, eCommerce, telecom, and social media, as well as regulated industries such as government and healthcare.
- This edition broadens the evaluated scope beyond vendors combining document verification with biometric matching: solutions qualifying through supervised video verification, high-assurance and reusable verified identity, or authoritative data sources are assessed in one shared evaluation model, with a focus on the North American and European markets.
- The diverse vendor landscape is characterized by various technological approaches, differentiating on regional expertise and best-of-breed capabilities. Key functional areas evaluated by KuppingerCole Analysts include document verification, biometric verification, additional verification methods, automation and AI, privacy, and orchestration.

Market Analysis

The identity verification market is expected to grow significantly in the next five years with sustained long-term growth. Vendors are preparing by asserting their expertise in essential capabilities: broad coverage of identity documents, future-proof methods of physical and digital document verification, fit-to-purpose matching and detection algorithms, and fraud prevention including deepfake and injection attack detection and the detection of AI-edited or template-generated document images, to name just a few.

There is a high variety of solutions in the market. Vendors differentiate themselves with different technological approaches to identity verification, specialize in verifications for a certain country or region, and compete through achieving broad coverage on in-house technology alone or by using a network of technology partners. KuppingerCole Analysts views the broader market as consisting of three closely related segments. Full-Service Identity Verification vendors provide integrated enterprise offerings that apply identity verification directly to business processes such as onboarding, workforce verification, account recovery, step-up verification, fraud reduction, and age assurance, typically combining document verification, biometric verification and liveness, additional verification methods, workflow and orchestration, manual review, and enterprise integrations in one commercial offering.

Identity Verification vendors provide best-of-breed capabilities that are consumed directly by enterprise buyers or embedded within broader platforms; strong document authentication and biometric core technology, and deep yet easy-to-use workflow management that connects to multiple attribute verification services and sources of truth, are examples of the capabilities that differentiate leading products. These vendors remain in scope when they provide sufficient workflow, decisioning, and enterprise integration to function as products rather than isolated technical components. Reusable Verified Identity covers user-held or scheme-based verified identities that can be presented across multiple relying parties; vendors in this segment are rated only when they directly support enterprise verification of natural persons at a comparable level of assurance and operational integration.

The scope of this edition is intentionally larger than in the prior edition, but it is not unlimited. Government-issued document verification combined with biometric binding remains the center of gravity of the market, but vendors may also qualify through document verification combined with synchronous supervised video verification, through high-assurance national digital identity scheme (eID) or reusable verified identity combined with person binding and enterprise workflow integration, or through authoritative government or regulated data sources used as part of a direct identity verification process. Not all capabilities need to be fully native, as many buyers consume integrated offerings that mix proprietary and third-party capabilities; however, the distinction between native and Original Equipment Manufacturer (OEM) functionality remains analytically important and is reflected in the assessment. This Leadership Compass focuses on the North American and European markets, and vendors are assessed primarily on their ability to serve buyer requirements in these regions.

With the market far from being settled, this Leadership Compass presents the vendors that are most comparable based on the inclusion criteria, with each bringing different strengths and differentiators to serve their customers. Several adjacent market categories intersect with identity verification without being rated in this report unless they also provide substantive identity verification capability of their own: orchestration and broker platforms that route between identity verification providers; identity intelligence, attribute verification, and data verification services based on telecom, credit, or device data; fraud and risk platforms focused on fraud scoring, authentication and Customer Identity and Access Management (CIAM) platforms with proofing extensions; Know Your Business (KYB) and legal entity verification platforms; and national or scheme-specific digital identity services tied to one closed relying-party context. The Vendors to Watch section includes identity verification vendors that did not participate in this report but present valid solutions in these adjacent categories or with a focused regional footprint.

Delivery Models

Organizations require a variety of delivery models. The regulated industry may need strict control over data for privacy and data residency requirements and may prefer on-premises or private cloud deployments. Fast-moving digital services often opt for cloud deployments. Vendors rarely provide only one or the other, but most often the choice between on-premises or cloud deployments is possible. Vendor products either have roots in on-premises deployment or take a cloud-first approach, with regional hosting options increasingly offered to address data residency expectations in North America and Europe.

Required Capabilities

When evaluating the products, besides looking at the overall aspects of the solutions and their respective vendors, like overall functionality, stability of the company, number and geographic distribution of customers, licensing models, and so on, KuppingerCole Analysts considers the following key functional areas of identity verification solutions:

Document Verification: Ability to verify government-issued documents using optical character recognition (OCR), scanning the machine-readable zone (MRZ), and reading embedded chip data via near-field communication (NFC). Cryptographic and forensic checks to detect fraud, counterfeits, and expired documents should also be performed, including detection of tampering, compositing, template-based generation, and AI-edited document images, and when verifying a document optically, the solution should validate the document against authoritative sources. Geographical coverage across issuing countries availability of country-specific eID, BankID-style, with particular depth expected for North American and European buyer requirements.

Biometric Verification: Use of facial analysis for 1:1 matching against the scanned identity document. This typically requires a selfie or video of the end-user to compare against the photo used by the identity document, with different methods available to compare against the photo printed on the document and the photo stored in the document chip. Additional checks for liveness to identify and prevent deepfakes, presentation attacks, replay and

virtual camera attacks, Software Development Kit (SDK)/Application Programming Interface (API) injection attacks, etc. are required, with independent testing such as ISO/IEC 30107-3 presentation attack detection evaluations as supporting evidence. Use of 1:N biometric searches to check watchlists of known bad actors or recent applicants looking for duplicate accounts and/or 1:N full database searches to find actors with multiple identities or multiple attempts to register.

Additional Verification Methods: Use of other verification methods, including federation of an electronic ID (eID), mobile driving license (mDL) and Mobile Document (mDocs) following ISO/IEC 18013-5, BankID-style schemes, trusted government data sources (some governments will allow financial services firms to check a face capture against a face record on file for passports, driver's license or national ID) and other financial information, attribute verification such as name or address, synchronous video verification, or accepting [verifiable credentials](#) and other reusable verified identities to present previously verified information.

Automation and AI: Use of automation, machine learning (ML), and AI to improve functionality and user experience, accompanied by appropriate governance of algorithms used for matching, decisioning, and fraud detection, including manual-review routing, reason-code generation, and model monitoring.

Privacy: Specific attention to end-user privacy in solution design, information collection, storage, and transactions. Privacy-by-design, data minimization, and proportionality of data usage/storage must be taken into account, including the storage, protection, and retention of biometric templates. Ability to address data residency requirements and compliance with regulations such as General Data Protection Regulation ([GDPR](#)), California's Consumer Privacy Act ([CCPA](#)), and other global privacy laws is required.

Orchestration: The automated coordination and management of the identity verification components with enterprise systems, services, and processes. The ability to use identity verification to support onboarding, KYC, authentication, account recovery, and fraud reduction processes is a large value-add which orchestration helps to facilitate.

Other key criteria that vendors should provide (but are not limited to) include:

- Support for digital remote verification flows
- Compliance with US National Institute of Standards and Technology (NIST) 800-63 Revision 4 Identity Assurance Level (IAL), ISO/IEC 18013-5 mDL and EU Regulation on electronic IDentification, Authentication, and trust Services (eIDAS) standards
- Use of the verified identity for authentication purposes, including step-up, and for account recovery and re-verification
- Support for KYC/AML checks against blacklists, sanctions lists, for politically exposed persons (PEPs) and ultimate beneficiary owners (UBOs)
- Integration and orchestration into key systems, such as onboarding tools, authentication, and risk engines
- High attention to privacy and data protection
- Modern architecture with support for Software Developer Kit (SDKs) and Application Programming Interface (APIs)

- Wide geographical coverage (for document verification, video-based verification, algorithmic accuracy, etc.) and deployment, with depth in North America and Europe

Leadership

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

Overall Leadership

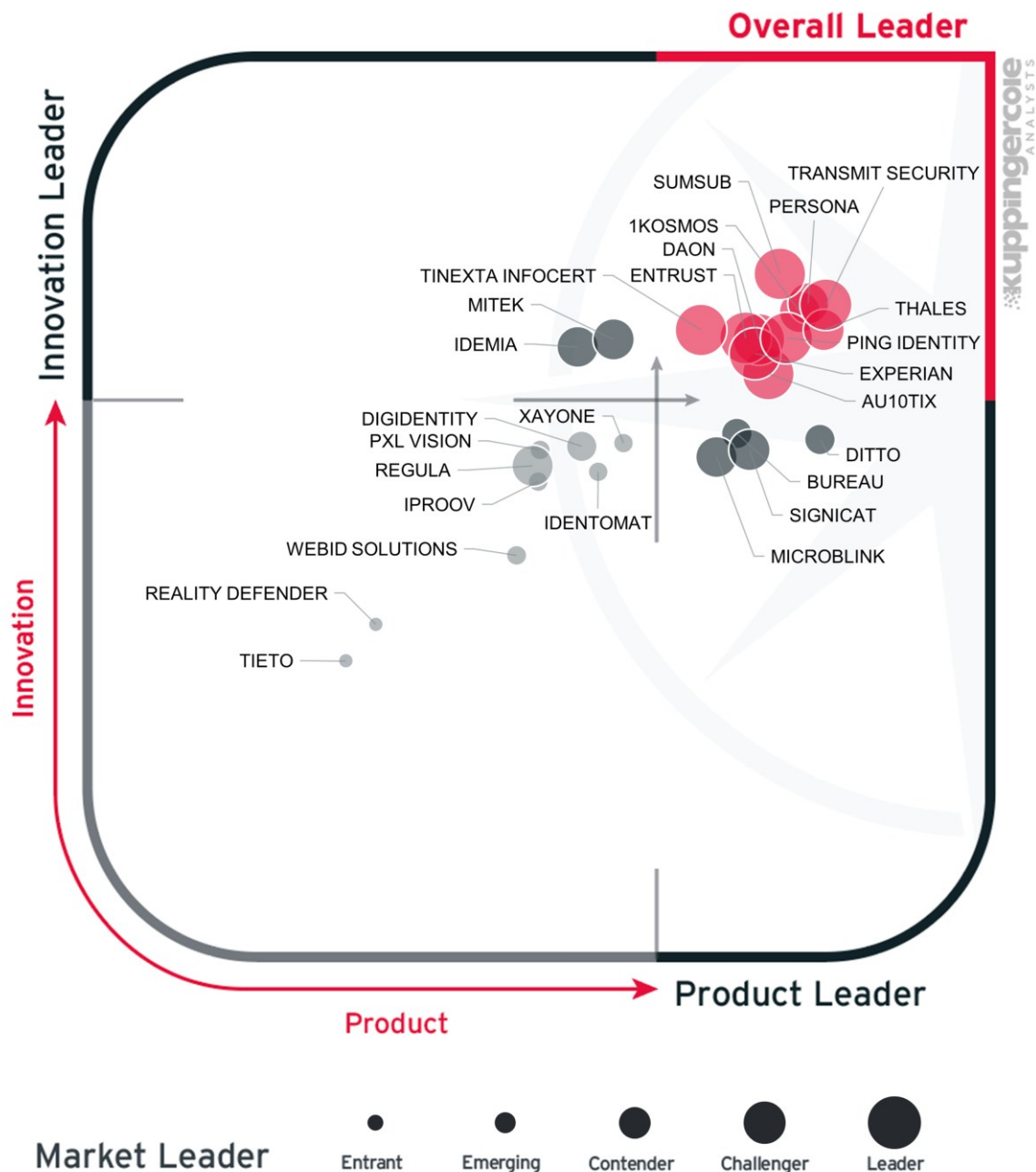
The Overall Leadership chart reflects how vendors balance product strength, innovation, and market presence. The chart evaluates vendors in this market across two dimensions. The horizontal axis measures Product Leadership, and the vertical axis measures Innovation Leadership. Overall Leaders are those in the upper right-hand quadrant, with the bubbles colored red. Vendors in this quadrant score highly in both dimensions, earning Overall Leadership status. These organizations ship mature products while maintaining strong innovation.

The bubble size reflects each vendor's relative strength in terms of Market Leadership. Further details on Market Leadership can be found in the Market Leadership section.

Product Leaders are found to the right of the vertical dividing line. The vendors in the lower right quadrant, colored black, are established vendors with full-featured products but fewer innovative differentiators. These providers demonstrate solid execution using conventional methods. Further details on Product Leadership can be found in the Product Leadership section.

Innovation Leaders are found above the horizontal dividing line. Vendors in the upper left-hand quadrant, colored black, have advanced technology approaches but less mature product offerings. These companies often introduce new technical approaches that are not yet widely adopted. Further details on Innovation Leadership can be found in the Innovation Leadership section.

Vendors in the lower left-hand quadrant, colored grey, are challengers for both product and innovation leadership. Those toward the bottom left-hand corner are mainly niche vendors with products focused on specific market segments and geographical areas.



The 2026 Overall Leaders by alphabetical order, 1Kosmos, AU10TIX, Daon, Entrust, Experian, Persona, Ping Identity, Sumsub, Thales, Tinexta Infocert, and Transmit Security; form a closely matched group, each combining product depth, sustained innovation, and market execution.

Within this group, AU10TIX and Sumsub stand out for highly automated verification at global scale, pairing broad document coverage with layered defenses against deepfakes and injection attacks, while Persona differentiates through orchestration flexibility and developer-centric configurability. 1Kosmos and Daon carry verified identities forward into authentication and reusable-identity scenarios that regulated buyers increasingly demand, and Ping Identity and Transmit Security deliver verification as part of wider customer and workforce identity

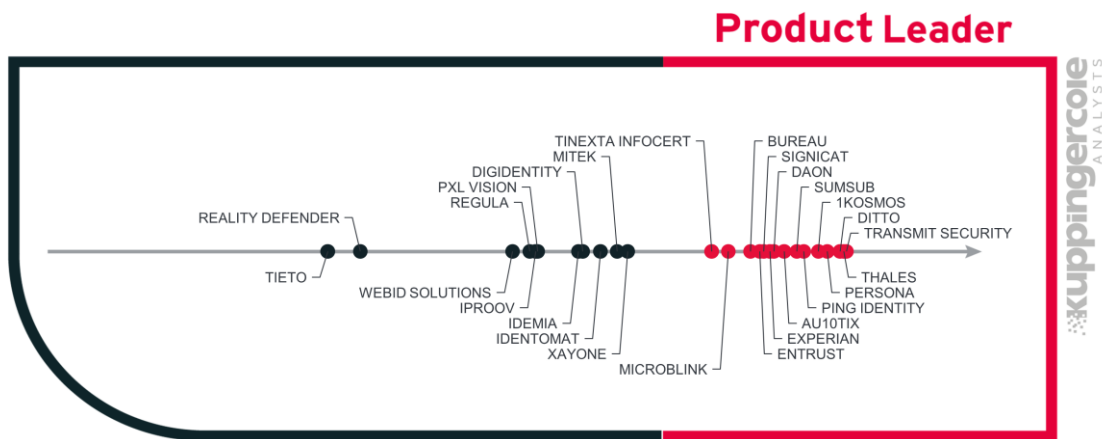
platforms at enterprise scale. Thales, Entrust, Experian, and Tinexta Infocert complete the group, drawing respectively on citizen-identity and government-credential work, a well-rounded offering built around a document-verification acquisition, bureau-grade data checks and fraud analytics with global reach, and European qualified trust services. Their delivery models and regional anchoring differ, but their reliability, scale, partner networks, and market reach are consistent across the group.

Several vendors demonstrate clear leadership in individual dimensions but do not reach Overall Leadership due to imbalances across product, innovation, and market execution. IDEMIA and Mitek perform strongly in Innovation Leadership, advancing document and biometric technology of a depth that also places parts of their portfolios inside competing services, but without the same cross-dimensional balance in this segment. Bureau, Ditto, Microblink, and Signicat perform strongly in Product Leadership, offering compelling capabilities within defined scopes. Signicat offers European eID coverage and orchestration, Bureau and Ditto offer differentiated fraud intelligence and orchestration, and Microblink offers strong extraction and verification technology. However, they lack the combined scale or cross-dimensional balance required for Overall Leadership positioning.

The remaining vendors are positioned as Challengers, reflecting varying stages of development and market traction. These vendors provide focused and technically credible identity verification offerings, several with specialist depth in biometric liveness, deepfake detection, document forensics, or NFC chip verification, but face constraints related to global reach, deployment scale, partner coverage, or completeness across the evaluated dimensions. Many are well suited to specific industries, regions, or national eID schemes, and may progress toward higher leadership positions as their offerings and market presence continue to develop.

Product Leadership

Product leadership is the first specific category examined below. This view is based on the presence and completeness of required features as defined in the required capabilities section above. The chart is horizontal and divided into two areas, the vendors to the right of the chart and colored red are Product Leaders and those to the left and colored black are Product Leadership Challengers.



The Product Leaders in identity verification each combine broad coverage of document, biometric, and data-centric verification, each with a distinct product emphasis.

The Product Leaders are by alphabetical order, 1Kosmos, Au10tix, Bureau, Daon, Ditto, Entrust, Experian, Microblink, Persona, Ping Identity, Signicat, Sumsb, Thales, Tinexta Infocert, and Transmit Security

Ditto is recognized for a full-service offering that combines document verification, face biometrics and liveness, attribute verification, and no-code workflow orchestration, and stands out for deployment flexibility, spanning on-premises to managed cloud, and for binding verification to high-assurance authentication. Sumsb is recognized for completeness, combining global document coverage with KYC, AML, and fraud controls on one platform, while AU10TIX stands out for automation, processing document verification at high volume with layered deepfake and injection defenses. Persona differentiates through configurability, with developer-centric building blocks and orchestration, and Bureau through signal breadth, pairing document and biometric verification with device intelligence, behavioral biometrics, and consortium fraud data. Daon and 1Kosmos are recognized for verification-to-authentication continuity: Daon for biometric onboarding that carries into ongoing authentication across financial services, telecommunications, government, and travel, and 1Kosmos for binding verified identities to reusable, privacy-preserving credentials. Entrust delivers well-rounded document and biometric verification within a wider certificate and payment portfolio, and Experian is differentiated by data strength, bringing bureau-grade record checks and fraud analytics into verification flows. Ping Identity and Transmit Security are positioned for platform integration, embedding verification into wider access management and fraud prevention platforms for customer and workforce scenarios. Microblink is recognized for capture, extraction, and fraud detection technologies whose depth also places it inside competing services. Signicat is differentiated by eID coverage, aggregating European electronic identities alongside document and biometric methods, and Tinexta Infocert by qualified trust, anchoring verification in eIDAS trust services. Thales is positioned for breadth, reflecting citizen-identity heritage and extensive deployment options.

A second group of vendors tops the challengers group and includes Digidentity, Identomat, IDEMIA, Mitek, and XAYONE, each demonstrating strong product capabilities with differing

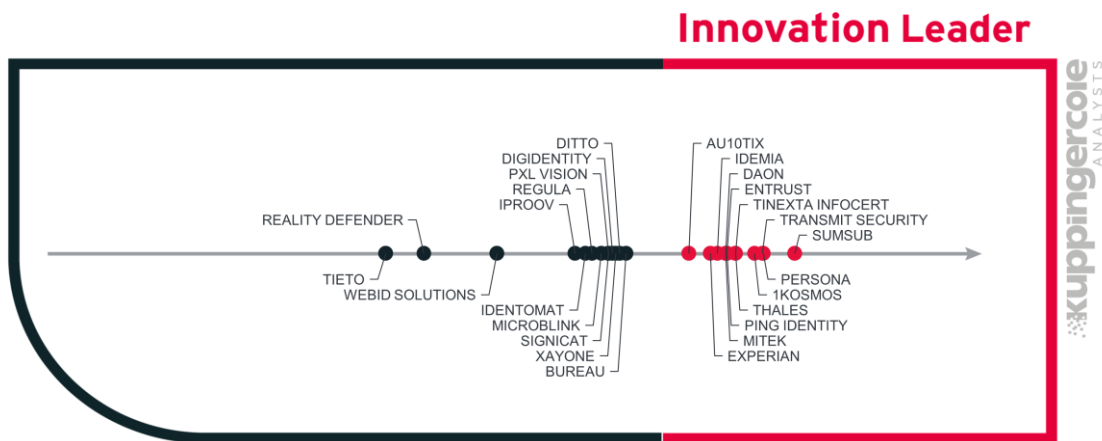
emphasis. Digidentity provides supervisory-approved remote proofing at eIDAS High with reusable wallet identities; Identomat combines an in-house document and biometric stack with an operator-led video channel and deployment flexibility down to on-premises; IDEMIA contributes biometric algorithm depth and government-credential heritage; Mitek brings document-verification technology that is also widely embedded in other vendors' offerings; and XAYONE delivers verification, customer identity management, and electronic signature from a single platform. While these vendors show strong product value, they typically trail the top group in completeness across the full evaluated feature spectrum or in consistency across all sub-domains.

The remaining Challengers in Product Leadership include PXL Vision (automation), iProov (biometric liveness at scale), Regula (document forensics), and WebID (regulated German verification flows). These vendors provide relevant and often specialized verification capabilities but show more pronounced limitations in areas such as orchestration depth, data-source coverage, fraud-signal breadth, or deployment versatility, often reflecting a narrower product scope or target segment. Further behind, Tietoevry and Reality Defender occupy more focused positions: Tietoevry as a Nordic eID broker with partner-delivered biometrics, and Reality Defender as a deepfake-detection specialist whose product addresses only part of the evaluated identity verification spectrum.

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.

The chart is horizontal and divided into two areas: the vendors to the right of the chart, colored red, are Innovation Leaders, and those to the left, colored black, are Innovation Leadership Challengers. Innovation Leaders are those vendors that deliver forward-looking products, not only in response to customers' requests but also because they are driving technical change in the market by anticipating what will be needed in the months and years ahead.



At the forefront of the 2026 Innovation Leadership are vendors shaping how the market responds to GenAI fraud, reusable identity, and the convergence of verification with authentication.

The Innovation Leaders, in alphabetical order, are 1Kosmos, Au10tix, Daon, Entrust, Experian, Idemia, Mitek, Persona, Ping Identity, Sumsb, Thales, Tinexta Infocert, and Transmit Security.

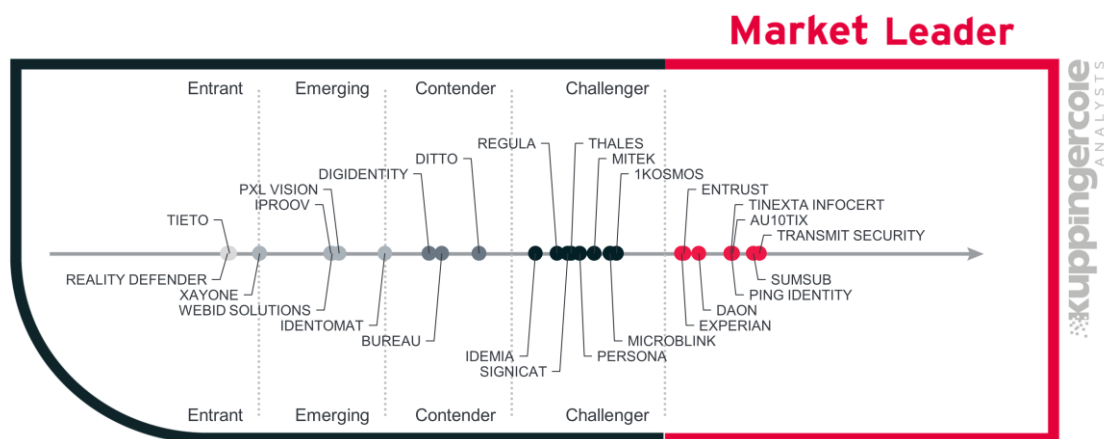
Sumsb (feature velocity) is the highest-placed Innovation Leader, standing out for how quickly new capabilities reach production across all three of these fronts: a continuously retrained deepfake detector, AI applied to verification operations through a copilot that summarizes cases and translates plain-language requirements into workflow configuration and an MCP server that lets customer-operated AI agents work under human approval, and reusable KYC through its proprietary Sumsb ID. AU10TIX (deepfake and injection defense) is likewise advancing the detection of AI-generated documents and faces at production scale, while Persona (developer-led innovation) continues to extend its orchestration and building-block model. 1Kosmos (identity assurance) and Daon (verification-to-authentication convergence) are driving the reuse of verified identities for ongoing authentication, and Ping Identity (privacy-preserving re-verification) and Transmit Security (risk-signal convergence) are bringing verification, fraud detection, and access decisions together on shared platforms. IDEMIA (biometric advancement) and Mitek (document and biometric fraud research) sustain algorithm-level innovation in face matching, liveness, and fraud detection that also reaches the market through other vendors' products. Entrust (AI-assisted document fraud detection), Experian (data-driven fraud intelligence), and Thales (portfolio-level innovation across biometrics, cryptography, and citizen identity) draw innovation from adjacent portfolio strengths, while Tinexta Infocert (qualified trust and wallet readiness) is positioning verification for EUDI Wallet scenarios.

The remaining vendors are positioned as Challengers in Innovation Leadership: Bureau (consortium fraud-graph innovation), Digidentity (wallet-based reusable identity), Ditto (verification bound to high-assurance authentication), Identomat (operator-assisted verification), iProov (biometric liveness research), Microblink (document verification with gen AI detection and capture-layer integrity), PXL Vision (automated verification), Regula

(document forensics), Signicat (eID aggregation), and XAYONE (platform consolidation). These vendors contribute innovative elements within specific contexts or segments, several as notable specialists in their own domains, but show more limited momentum in adopting the broader architectural and conceptual shifts shaping the next phase of identity verification. At the lower end of the spectrum, Tietoevry and WebID show the least recent innovation momentum, reflecting respectively a broker model assembled largely from partner technology and a portfolio still anchored in regulated video identification.

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers and their geographic distribution, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.



The chart divides vendors into five categories: Leaders, Challengers, Contenders, Emerging, and Entrants. The Market Leaders, shown to the right of the chart and colored red, are those with strong market presence and customer reach. Market Challengers, shown to the left of the Leaders and colored black, are strong competitors with solid offerings and room for further market expansion. Contenders, shown in grey, are players with a stable position and reliable offerings but limited market penetration or only regionally. Emerging vendors, with a growing presence and the potential for further market impact, are colored light grey. Entrants, shown to the left of the chart, are newcomers or smaller niche players who are just beginning to establish a market presence.

The Market Leaders in 2026 are Transmit Security (platform-driven adoption), Sumsub (global volume growth), AU10TIX (high-volume enterprise adoption), Ping Identity (installed-base reach), Tinexta Infocert (European trust-services footprint), Experian (North American, Brazilian and UK focus), Daon (long-standing financial-services base), and Entrust (acquisition-strengthened global reach). These vendors demonstrate broad adoption across

regions, large and complex deployments, and well-established partner networks, enabling them to execute consistently at enterprise scale.

The Challenger group includes 1Kosmos (assurance-led growth), Microblink (direct enterprise adoption with OEM volume), Mitek (established document-verification base), Persona (developer-led commercial traction), Signicat (European breadth), Regula (forensic-tooling footprint), IDEMIA (government installed base) and Thales (citizen-identity concentration relative to this segment). These vendors show meaningful market traction and growing visibility but typically operate on a more limited global scale or within more specialized segments compared to the Market Leaders.

The Contenders, Ditto (regional financial-services base), Bureau (APAC momentum), and Digidentity (national-scheme presence), demonstrate credible market execution in defined segments or regions. While these vendors show momentum within their target markets, their overall customer footprint, geographic reach, or partner network in identity verification remains more constrained.

The Emerging vendors, Identomat (regional growth), PXL Vision (Swiss regional base), WebID (presence in regulated industries in Germany), and iProov (specialist biometric deployment at scale), XAYONE (North Africa regional focus) are characterized by limited but focused market presence in this segment. They address specific use cases, geographies, or customer bases and show clear signs of adoption, but have not yet reached the scale or breadth required to compete broadly across the market. Tietoevry, and Reality Defender enter the chart as Entrants, smaller or newly positioned players at an early stage of establishing commercial presence in identity verification.

Product and Vendor Evaluation

This section provides a structured evaluation of each product and vendor included in this KuppingerCole Analysts Leadership Compass. Each profile contains a description of the company and its offering, an analysis of relevant capabilities for this market segment, and an assessment of strengths and challenges. Where applicable, vendors are positioned as leaders in the product, innovation, or market categories.

In addition to these standard Leadership Compass categories, we provide detailed capability ratings for every vendor. These ratings are visualized in a spider chart that reflects performance across the functional and technical criteria defined for this market segment. The spider chart complements the written analysis and enables direct comparison across solutions.

For this Leadership Compass, the capability categories evaluated are described below:

Document Verification: Ability to verify government-issued documents using OCR, scanning the MRZ, and reading embedded chip data via NFC. Forensic checks to detect fraud, counterfeits, and expired documents should also be performed, and should validate the document against authoritative sources.

Biometric Verification: Use of facial analysis for 1:1 matching against the scanned identity document. This typically requires selfie or video of the end-user to compare against the photo used by the identity document. Additional checks for liveness to identify and prevent deepfakes, presentation attacks, injection attacks, etc. are required. Use of 1:N biometric searches to check watchlists of known bad actors or recent applicants looking for duplicate accounts and/or 1:N full database searches to find actors with multiple identities or multiple attempts to register.

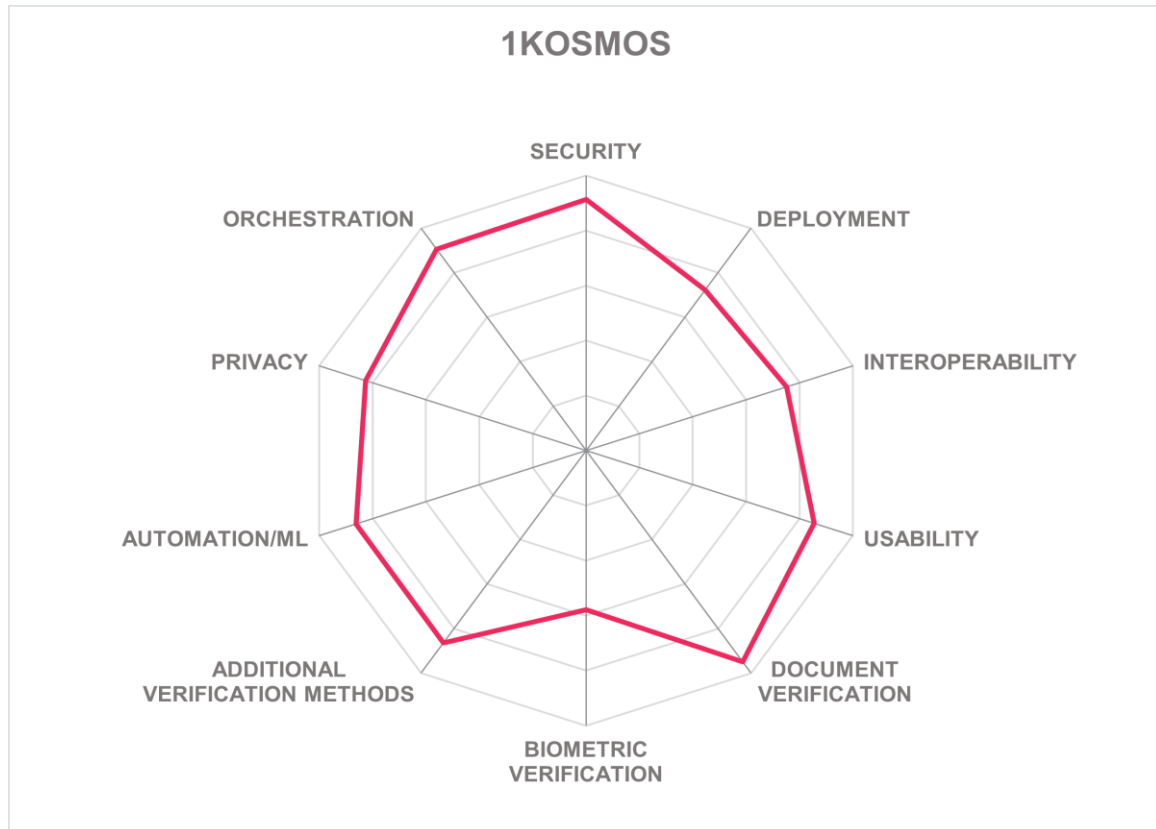
Additional Verification Methods: Use of other verification methods, including federation of an eID, mDL, BankID, trusted government data sources (some governments will allow financial services firms to check a face capture against a face record on file for passports, driver's license or national ID) and other financial information, attribute verification such as name or address, synchronous video verification, or leveraging verifiable credentials to present already verified information.

Automation and ML: Use of automation and ML to improve functionality and user experience, accompanied by appropriate governance of algorithms used for matching, decisioning, and fraud detection.

Privacy: Specific attention to end-user privacy in solution design, information collection, storage, and transactions.

Orchestration: The automated coordination and management of the identity verification components with enterprise systems, services, and processes. The ability to use identity verification to support onboarding, KYC, authentication, and fraud reduction processes is a large value-add which orchestration helps to facilitate.

1Kosmos – 1Kosmos Verify



1Kosmos is a privately held and venture-backed US-based identity company headquartered in New Jersey and founded in 2018. 1Kosmos Verify is the identity verification capability of the 1Kosmos platform that also offers passwordless authentication and a user-held decentralized identity wallet but that can be consumed on its own. It is positioned as full-service identity verification covering consumer onboarding and KYC, workforce onboarding, helpdesk-assisted recovery, workforce re-verification, and government or citizen proofing. Its largest commercial base is in North America, with additional presence in Europe, the Middle East and Africa (EMEA), Asia-Pacific (APAC), and Latin America. The service is priced per

user or per verification, is delivered as vendor-managed Software as a Service (SaaS) with a private-cloud option and is ISO/IEC 27001 certified with a SOC 2 Type 2 attestation. Key industries served include finance, government, healthcare, and manufacturing.

Hosting is available in North America, Latin America, EMEA, and APAC, supporting multi-region deployment and data-residency choices. The platform supports both multi-tenant and dedicated single-tenant operations and is listed on major cloud marketplaces and the Okta Integration Network. On-premises software is not generally available.

Identity verification is based on document, biometric, and attribute checks built and operated in-house. Document capture supports image and video with physical security-feature checks and NFC chip reading. NFC capture is done by a SDK, and the rest of the journey runs as a configurable web flow. 1Kosmos supports more than 4,000 document templates, passports, electronic and physical national identity cards, driver's licenses, and mDLs under ISO/IEC 18013-5, across roughly 190 countries, with fewer for electronic national IDs. Extracted data can be checked against authoritative sources such as American Association of Motor Vehicle Administrators (AAMVA) in the US and Aadhaar in India, among more than 60 other sources of truth. Beyond registry checks, attribute verification can draw on aggregated data from named partners: credit data through Experian across its operating regions, phone intelligence including SIM-swap and number-reputation signals through Telesign, and bank account data through open banking providers such as Plaid, Tink, TrueLayer, Finicity, Yodlee, and MX under frameworks including Payment Services Directive 2 (PSD2), Open Banking UK, and India's Account Aggregator ecosystem. Sanctions and watchlist data, business registries, email intelligence, and breach data extend the aggregated signal set, all partner-sourced rather than native. New templates are, in some regions, built from partner-sourced samples, with OCR training done by 1Kosmos. Facial biometrics offers 1:1 and 1:N matching. Liveness verification is passive only. Presentation attack detection has been tested by iBeta at ISO/IEC 30107-3 Level 2. Biometric templates can be stored on the vendor-side or customer-side.

Fraud controls combine document, biometric, device, and behavioral signals into a single risk score that drives pass, fail, or step-up outcomes. For documents, 1Kosmos describes image forensics, template, and layout validation, MRZ and barcode cross-checking, file-integrity analysis, and detection of AI-edited, composited, and synthetic documents. Biometric anti-spoofing covers masks, AI-generated selfie images and video, face-swap, screen and video replay, virtual-camera and emulator capture, SDK- and API-level injection, and session-integrity checks. Capture, liveness, virtual-camera, session-integrity, and injection controls are native; secondary deepfake analysis can be augmented through partner services such as Reality Defender. Device and behavioral signals include Internet Protocol (IP) reputation, geolocation, geo-velocity, device fingerprinting, jailbreak and root checks, login and transaction-pattern analytics, and optional behavioral biometrics. KYC screening for PEPs, beneficial owners, sanctions, and denylists, with AML, US Bank Secrecy Act, and PSD2 support, runs through partner nodes. 1Kosmos supports customer-configurable thresholds, versioned deepfake models, and a separate audit trail for deepfake decisions, and hybrid adjudication routes cases to manual review with an AI-generated case summary, using in-region and European partner review teams.

Privacy controls are built around decentralized architecture. User identity metadata is encrypted with a private key held in the device secure enclave and recorded, in sharded form, on a private, permissioned Ethereum blockchain, so attribute sharing requires user consent through an identity wallet. Consent is captured before biometric capture and data aggregation, and end-user data is not used for model training or shared externally. Data retention is configurable per customer and per jurisdiction for GDPR, CCPA, and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and users can see which attributes were collected and revoke a relying party's access, though they cannot access a record of which organizations have access to their verified identity.

Integration is available through REST, SOAP, and GraphQL APIs and webhooks, with SDKs for Android, iOS, Java, C/C++, .NET, and Python and a developer portal and sandbox. Administrative workflow configuration is not exposed through the API. Workflows are built in a no-code and low-code visual editor or generated from natural-language prompts, with JSON configuration for coded extensions and templates for common use cases. 1Kosmos supports around 150 enterprise connectors for Identity and Access Management (IAM)/Identity Governance and Administration (IGA), privileged access, identity threat detection and response (ITDR), service desk, and Security Information and Event Management (SIEM) export. Named connectors include Microsoft Entra ID, Okta, Saviynt, CyberArk, and ServiceNow. Verification results can be returned as verified attributes, assurance level, risk score, reason codes, and verifiable credentials, and fraud events can be pushed to customer SIEM pipelines.

1Kosmos is suited for buyers that want one platform to verify identity and then reuse it across onboarding, passwordless authentication, helpdesk-assisted recovery, and step-up re-verification, particularly for workforce and in-store or frontline verification alongside consumer onboarding. Its independent assurance credentials are strong for US public-sector use: Federal Risk and Authorization Management Program (FedRAMP) High with US Department of Defense (DoD) Impact Level 4, and Kantara certification as a full-service credential service provider conformant with NIST SP 800-63-3 at IAL2 and Authentication Assurance Level 2 (AAL2), complemented by UK DIATF certification as an identity and attribute service provider.

Strengths

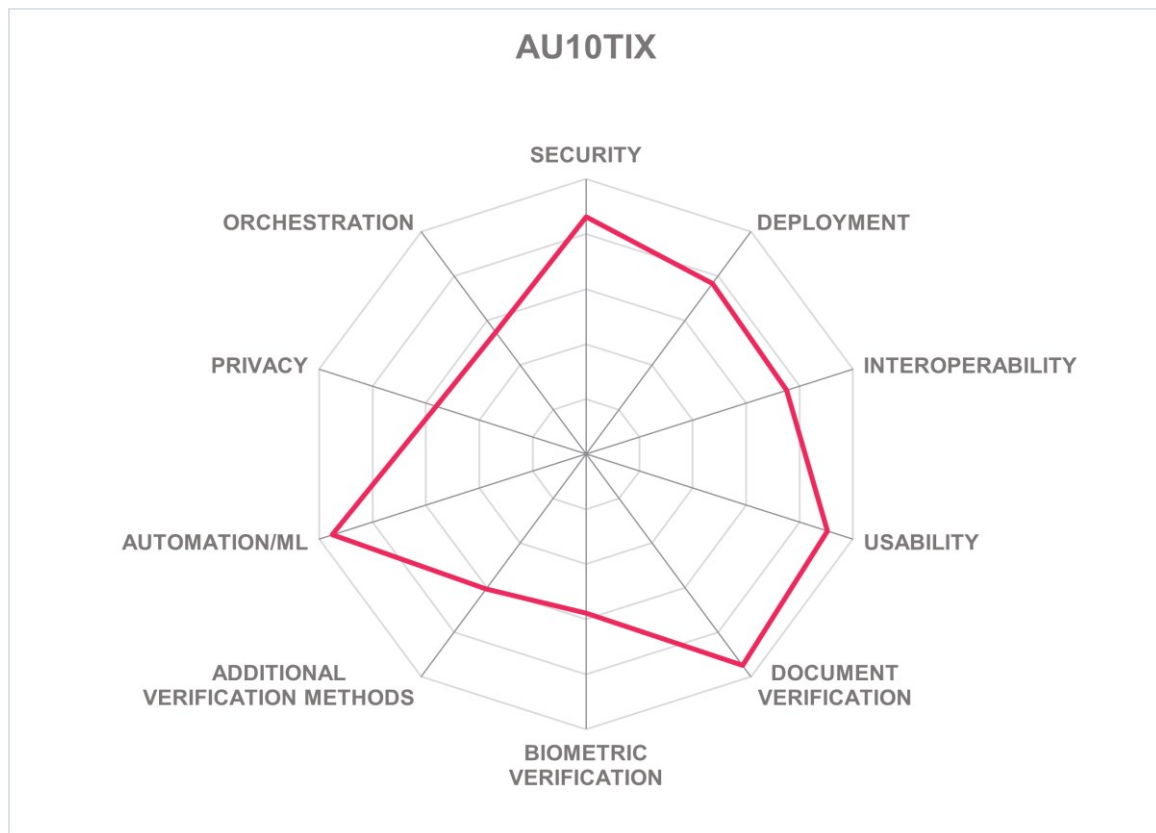
- Independent, high-assurance certifications: FedRAMP High with DoD Impact Level 4 and Kantara certification as a full-service credential service provider at NIST SP 800-63-3 IAL2/AAL2
- Combined identity verification and passwordless authentication on one platform lets buyers reuse a biometrically bound identity for account recovery and step-up
- Flexible biometric template storage, vendor-managed, customer-managed can matter for buyers that want to limit vendor-held biometric data or meet data-residency and privacy constraints
- No-code, low-code, and natural-language workflow generation with real-time branching lets teams adapt verification journeys by use case, geography, or risk without hard-coding each fallback path

- Configurable thresholds, versioned models, and a distinct audit trail for deepfake-related decisions give fraud teams a way to tune and review AI-assisted fraud handling rather than treating all failures uniformly.
- Approximately 150 enterprise connectors covering IAM, IGA, PAM, service desk, and SIEM

Challenges

- Standard delivery is vendor-managed SaaS; a private-cloud option covers a small share of the installed base and on-premises software is not generally available.
- Authoritative data checks and AML/PEP screening are partner-delivered, and secondary deepfake analysis uses partner services,
- Liveness is passive-only, buyers whose policies or regulators expect active liveness, should validate that passive detection meet their requirements
- Evidenced source of truth strength is concentrated in North America and parts of APAC; buyers with large European or Latin American volumes should validate local document coverage, source-of-truth checks, and in-region support
- Users cannot retrieve a full record of organizations that have accessed their identity

AU10TIX – AU10TIX Identity Verification Platform



Leadership



AU10TIX was founded in 2002 as a spin-off from airport-security and border-control specialist ICTS International and is privately held, with corporate headquarters in the Netherlands. AU10TIX Identity Verification Platform, a full-service identity verification platform combines document verification, facial biometrics and passive liveness, consortium fraud intelligence, and no-code orchestration. Core verification and fraud capabilities are native, while proof of address, external identity-data checks, and sanctions/PEP and KYB

registry lookups are delivered through partner integrations. It serves consumer, workforce, and B2B verification, with use cases including digital onboarding, account recovery, re-verification, age assurance, KYC/AML, and KYB/UBO checks in selected regions. The customer base is strongest in North America and EMEA, with additional presence in APAC and Latin America. Per-verification pricing is the primary commercial model, complemented by annual subscription commitments and fixed-price arrangements for high volumes; the service is delivered as vendor-managed SaaS or managed service with no on-premises option, and is ISO/IEC 27001 certified with a SOC 2 Type 2 attestation.

Hosting runs on Amazon Web Services (AWS) and Microsoft Azure across data centers in the EU, US, UK, and APAC, with regional or sovereign deployments on request for data residency. The platform supports multi-tenant and single-tenant operation.

Verification is based on optical document capture, NFC chip reading for International Civil Aviation Organization (ICAO) 9303 documents with PKI validation, facial biometrics, attribute checks, across more than 190 countries and 5,000-plus document templates covering passports, national IDs, driver's licenses, residence permits, and visas. Capture is done through browser or mobile app, though NFC requires the mobile SDK rather than a browser journey. Document authentication uses template and font comparison as well as physical security-feature checks and is performed by in-house technology, with partner adjudication only as an edge-case fallback. Authoritative source-of-truth checks against issuer, or government repositories are selective, available only for specific regulations and customers, with no AAMVA connection so most verifications rely on document authenticity, biometric binding, and risk signals. Facial biometrics are native, with 1:1 and 1:N matching; liveness is passive, based on texture and motion analysis and tested to iBeta PAD Levels 1 and 2.

Fraud controls are layered. An authenticity layer applies to around 180 document forgery tests and detects AI-generated or AI-edited document images, compositing, and tampering, template-based or synthetic documents, and document-to-biometric inconsistencies. An integrity layer verifies capture provenance and session integrity and detects injection attacks, virtual cameras, emulators, and jailbroken, rooted, or connected devices. An intelligence layer, the Serial Fraud Monitor, compares salted-hash representations across an opt-in customer consortium to detect fraud rings and coordinated attacks without exposing personal data between customers. Device intelligence covers IP reputation, geolocation and geo-velocity, device ID and fingerprinting, device reputation, and jailbreak or root checks; KYC screening covers PEP, UBO, denylists, and sanctions. Identity verification decisions are returned as pass, refer, or fail with structured reason codes rather than a numeric risk score. AU10TIX's Risk Intelligence can complement the core IDV workflow by generating additional fraud and risk scores. AI-fraud governance is evidenced through independent deepfake testing, customer-configurable thresholds, versioned and auditable models, a formal update process, false-positive and false-negative reporting, a separate deepfake audit trail, and an internal fraud lab tracking darknet toolkits.

Privacy controls include consent captured before document, biometric, and liveness processing, typically implemented by the customer, and user notice for active and passive liveness. Sensitive data is encrypted at rest and in transit, subject to regional residency configuration, with retention and deletion configurable per customer and per jurisdiction. End

users can, through the customer, see which attributes were collected, revoke access, and obtain a record of organizations holding their data. Mobile SDKs use Apple Secure Enclave and Android Trusted Execution Environment (TEE), with keys held in the device Secure Element where hardware supports it. Anonymized verification data may be used to improve detection models, with no personal data shared externally.

Integration is done through REST APIs and webhooks under an API-first design with full functional parity, supported by API key management, rate limiting, sandbox/production separation, and a developer portal; SDKs cover Android, iOS, C/C++, React Native and Flutter. Orchestration uses a no-code, drag-and-drop workflow builder in the AU10TIX Console with policy-driven branching, step-up, fallback routing, and workflow testing, plus an AI-assist authoring option. Hybrid manual adjudication runs through a rule engine and can be performed by AU10TIX or the customer. Downstream, the platform returns verification results, verified attributes, reason codes to the console and API and integrates with multiple Consumer/CIAM, workforce IAM, IGA solutions including Microsoft Entra ID, Okta, Ping Identity, ForgeRock; the Microsoft Entra integration is native and supports issuing a digital ID into Microsoft Authenticator. External Personally Identifiable Information (PII) and identity-data checks are brokered through partners such as LexisNexis and Asia Verify.

AU10TIX is suited for high-volume, fraud-intensive, multi-region verification programs across financial services, fintech, crypto, marketplaces, gaming, and workforce onboarding, where document and biometric verification must be paired with deepfake, injection, and coordinated-fraud defenses and adapted through no-code workflows. IAL2 certification through Kantara and UK DIATF certification covering Disclosure and Barring Service, Right to Work and Right to Rent checks, make it a defensible option for NIST-aligned and UK-regulated use cases.

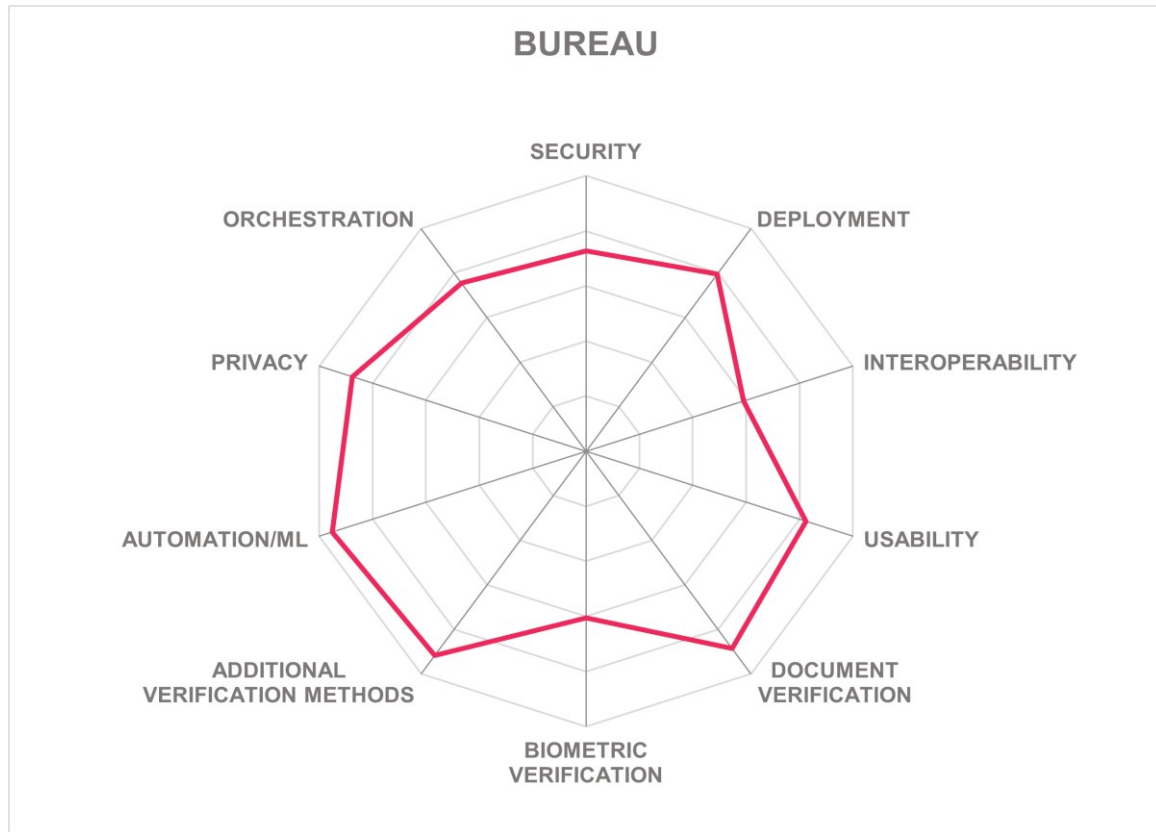
Strengths

- Layered fraud defense detects coordinated, cross-customer attacks that single-transaction verification would miss using document forgery tests, injection and capture-integrity checks and a consortium-based serial fraud monitoring
- Documented AI-fraud governance based on independent deepfake testing, versioned models with a formal update process, false-positive/negative reporting, a dedicated deepfake audit trail, and an internal fraud lab. Certification to NIST SP 800-63A IAL2 (Kantara) and UK DIATF as a Digital Identity Service Provider gives buyers independent validation for NIST-aligned onboarding and for UK Right to Work and Right to Rent, where a certified provider is required
- A native Microsoft Entra integration that issues a digital ID into Microsoft Authenticator and supports no-code onboarding and account-recovery flows can shorten deployment for Microsoft-centric workforce and CIAM buyers, including identity-verification-based account recovery
- A no-code, drag-and-drop orchestration builder with policy-driven branching, step-up, fallback, and workflow simulation lets buyers adapt verification journeys by risk, geography, and use case without engineering effort for each change
- Consortium fraud intelligence built on salted-hash matching lets buyers join cross-customer fraud-ring detection without exposing personal data to other participants

Challenges

- Source-of-truth validation against issuer or government repositories is selective rather than default, with no AAMVA; buyers that need authoritative database matching, not just document authenticity and biometric binding, should validate country-level coverage
- Delivery is limited to vendor-managed SaaS and managed service, with no on-premises option; buyers with customer-managed hosting or on-premises processing requirements should confirm whether regional or sovereign hosting satisfies their control needs
- Identity Verification decisioning currently return pass/refer/fail with reason codes rather than a numeric, weighable risk score, and risk-score-driven policy actions are not evidenced; fraud teams that tune thresholds against a composite score should validate how AU10TIX's reason-code model fits their workflows
- Liveness is passive only and the demonstrated biometric modality is face; buyers that require active liveness, for higher-assurance scenarios should validate against their control requirements

BUREAU – IDENTITY VERIFICATION



Leadership



Bureau Inc is an identity verification vendor privately held and venture-backed founded in 2020, headquartered in San Francisco with engineering and operations in India and Singapore. Identity Verification is one pillar of a wider platform that also covers device intelligence, behavioral biometrics, phone, and email intelligence, KYB, and AML monitoring, unified through a no-code orchestration layer called Flow Studio. Bureau positions the offering as full-service identity verification, combining document and biometric verification with authoritative-source checks, device and behavioral fraud signals, and a consortium graph, applied to onboarding, merchant verification, re-verification, step-up, and account-takeover decisions. The customer base is concentrated in financial services and in APAC, with India the largest market and growth in the Middle East, Europe, and North America. The solution targets consumer and business (merchant) verification scenarios rather than

workforce IAM. Licensing includes per-user, per-transaction, subscription, and fixed-cost terms.

The service is delivered primarily as vendor-managed SaaS on AWS, with region-specific hosting for data residency in Mumbai, Singapore, Bahrain, London, Frankfurt, and Northern Virginia. Private cloud, customer VPC, and on-premises deployment are supported for regulated customers. The default SaaS tier is multi-tenant, with single-tenant clusters and a dedicated Key Management Service (KMS) available for regulated customers. Bureau is ISO 27001 certified and holds a SOC 2 Type 2 attestation.

Identity verification is based on native document, biometric, and authoritative-data methods. Document classification, OCR, MRZ parsing, tampering detection, and face matching are performed with Bureau's own technology across more than 2000 document templates from more than 195 countries, covering ePassports, passports, electronic and physical national IDs, driver's licenses, and residence permits. Capture runs through native mobile and web SDKs with auto-capture, glare, and blur detection. NFC chip reading is also available. Authoritative checks reach more than 200 source-of-truth endpoints across 100-plus countries, roughly half through direct issuer connections and half through licensed data partners. Registry checks operate in three modes depending on what the issuing source returns: a registry-supplied photo matched biometrically against the captured selfie, attribute enrichment where the registry returns identity data and Bureau perform its own face match, or field-level match and no-match flags for the submitted attributes. Aggregated data extends to credit bureaus, telecom operators, and bank account verification rails selected per jurisdiction, with direct integrations in India complemented by licensed regional partners elsewhere. The only biometric modality is face, compared 1:1 by default and 1:N for deduplication. Active and passive liveness are offered, passive by default. The face liveness solution does not have ISO/IEC 30107-3 PAD certification. The face verification algorithm was not submitted to the NIST FRVT.

Fraud controls cover document and biometric attack surfaces. Document analysis applies error-level analysis, copy-move detection, font, and kerning checks, MRZ parity, and security-feature and template-integrity inspection, with separate reason codes and confidence scores for AI-generated or AI-edited documents distinct from traditional tampering. Biometric controls include presentation-attack detection for print, mask, and replay, plus deepfake, face-swap, virtual-camera, emulator, and SDK or API injection detection, backed by capture-provenance and session-integrity checks; when capture runs through the SDK, device intelligence is bound to the session to block injection and man-in-the-middle attempts. Device signals such as emulator, root or jailbreak, GPS spoofing, VPN and proxy, and agentic-browser detection, plus passive behavioral biometrics like keystroke, swipe, and gyroscope patterns, feed bot, and synthetic-identity detection before verification. Bureau's Graph Identity Network, a consortium graph of more than a billion identity records built from public and leaked data, supports stolen-identity, money-mule, and link analysis, and PEP, sanctions, UBO, adverse-media, denylist, and Legal Entity Identifier (LEI) screening with ongoing and transaction monitoring are integrated. Outputs are numeric risk scores with reason codes, configurable thresholds and policies, and actions from auto-approve to manual review and step-up.

Privacy controls include consent capture for document, biometric, device, aggregation, and cross-border processing, recorded in the verification audit trail, and end-user notice of active liveness, passive liveness, and data aggregation through customer-configurable disclosure. Data encryption keys are managed through AWS KMS rather than a customer-controlled Hardware Security Model (HSM), and mobile SDKs use the iOS Secure Enclave and Android TEE or StrongBox for cryptographic operations. Retention is configurable per customer and jurisdiction. End-user data is not used for third-party model training or external sharing without explicit contractual consent. End users can exercise access, revocation, and a record of accessing organizations through Bureau's APIs.

Integration is done through REST APIs, webhooks; SOAP, GraphQL, and gRPC are not supported. SDKs cover Android, iOS, React Native and Flutter. Flow Studio provides a no-code visual designer with conditional branching, parallel execution, version control, rollback, A/B testing, per-geography rule packs, jurisdiction-specific templates, and a bring-your-own-API framework that adds third-party or customer signals as journey nodes. A unified analyst console covers all nodes with maker-checker review, manual override with full audit trail, and drop-off analytics. A managed human-in-the-loop review service is offered selectively to tier-1 customers. Verification results are returned as verified attributes, assurance level, risk score, reason code, and status via webhook, OpenID Connect (OIDC) claims enrichment, or attribute write-back. Bureau integrates with IAM platforms including Okta, Auth0, AWS Cognito, Ping Identity, and Microsoft Entra External ID.

Bureau is suited for financial-services, lending, and marketplace buyers that want document and biometric verification combined with device intelligence, behavioral biometrics, KYB, AML, and a consortium fraud graph in one no-code platform, particularly across India, Southeast Asia, and the Middle East. The assurance posture aligns with eIDAS Substantial and NIST IAL2.

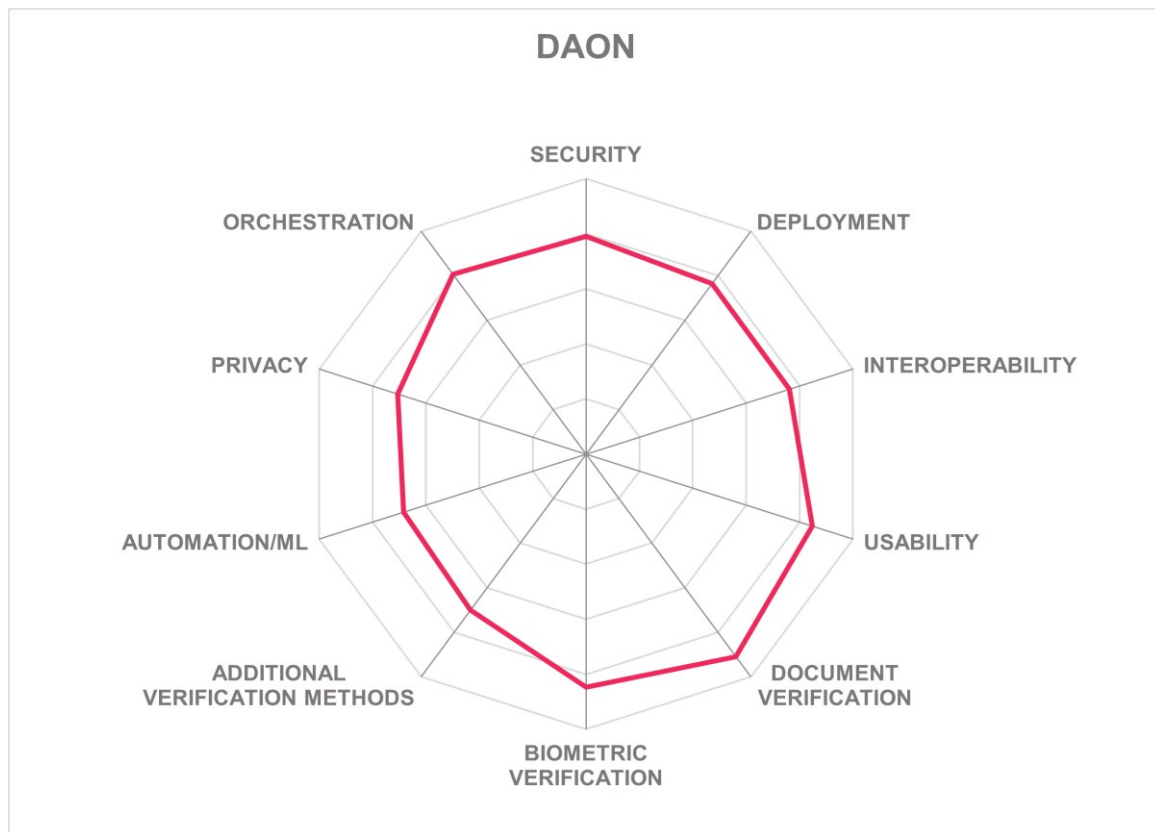
Strengths

- Device intelligence and passive behavioral biometrics are captured through the same SDK and bound to the capture session, which strengthens resistance to injection and man-in-the-middle attacks and lets buyers screen for bots and synthetic identities before verification begins
- Separate reason codes and confidence scores for AI-generated and AI-edited documents and selfies, distinct from traditional fraud, let fraud teams apply different thresholds, analyst routing, and audit trails for AI-assisted attacks instead of treating every failure as the same event
- Flow Studio provides no-code orchestration with per-geography rule packs, version control, A/B testing, a bring-your-own-API framework, and a unified analyst console, which can help compliance and fraud teams adapt journeys by risk, region, and document type without hard-coding fallback paths
- Region-specific AWS hosting plus private-cloud and on-premises options, can help buyers with data-residency or operational-control obligations, provided the deployment scope is confirmed
- The Graph Identity Network adds consortium-level stolen-identity, mule, and link-analysis signals natively as a journey node, which can benefit financial-services buyers that need network-level fraud context beyond a single onboarding event

Challenges

- Many authoritative registry and database checks are delivered through partners, so buyers dependent on authoritative verification should confirm checks providers, since this affects coverage depth, data handling, and support escalation
- The face-matching algorithm has not been submitted to NIST FRVT, and accuracy and demographic-bias figures are self-reported internal benchmarks, which may matter for buyers that must document independent validation of matching performance and fairness
- The face liveness solution does not have ISO/IEC 30107-3 PAD certification
- No standard 24x7 offering may not fit buyers that require follow-the-sun support commitments

Daon – xProof



Leadership



Daon, headquartered in Fairfax, Virginia, was founded in Ireland in 2000, is privately held and provides xProof, an identity verification offering within a platform that also covers ongoing authentication. xProof runs on TrustX for SaaS and IdentityX for self-managed and managed-service deployments and is sold as an integrated full-service offering combining document verification, biometric face matching, liveness detection, data checks, orchestration, and manual review. Its main use cases are KYC proofing at account opening and re-verification at higher-risk moments such as credential changes and new-device access; with a customer base strongest in EMEA, followed by APAC and North America, serving consumer and workforce user groups in financial services alongside telecommunications, government, and travel. A distinguishing element is identity continuity: factors registered during proofing, including face, a device-bound app key, OTP, push, and

FIDO2/Passkeys, are reused for later authentication and step-up on the same platform. Daon develops its own face, voice, and document algorithms in-house and blends OEM components where they improve results, so capability mixes native and partner technology. Verification is licensed per transaction on annual terms, with per-user pricing applying to ongoing authentication.

The service is delivered as vendor-managed SaaS on AWS, as a customer-dedicated managed service, or as customer-managed software on private cloud or on-premises. SaaS runs in the EU (Dublin, with Frankfurt for disaster recovery), the US, and Australia, with managed-service hosting in further regions across Asia, Europe, and Africa, and supports multi-tenancy, single-tenancy, dedicated processing, and bring-your-own-key (BYOK). A hybrid model runs orchestration in SaaS while keeping data storage in the customer's environment for data sovereignty. Data encryption keys are held in AWS KMS or a customer HSM. Daon holds ISO/IEC 27001, 27701, 27017, and 27018, a SOC 2 Type 2 attestation scoped to Security, HIPAA/HITRUST (Health Information Trust Alliance), Cloud Security Alliance Security, Trust, Assurance, and Risk registry (CSA STAR) Level 2, and ISO/IEC 42001 for AI management.

Verification is based on documents, biometrics, and data checks. Document verification uses optical image and video capture, NFC chip reading with passive and active authentication, and physical security-feature checks, covering electronic passport chip reading for roughly 180 countries, 233 driver's licenses templates, and more than 15,000 document types across in-house and partner technology. Data checks run against more than 100 sources through Cloud Functions and External Data Check Adaptors, some direct, some via partners. Aggregated attribute data covers credit-reference, telecom, postal, and government sources, consumed through multiple data rather than direct bureau relationships; bank account verification is planned rather than currently available. Biometric verification uses Daon's native DaonFace v7 algorithm with 2D face capture, 1:1 matching and 1:N for watchlist and duplicate checks; liveness is primarily passive with no separate step and is iBeta-tested to ISO/IEC 30107-3 PAD Level 1 and Level 2. Voice and fingerprint serve authentication rather than core proofing. ISO/IEC 18013-5 and 18013-7 mobile driving licenses are supported and tested with US and Australian issuers but not yet in production, national-ID eID is in production, EU digital wallet support is in preview, and verifiable-credential and reusable identity are supported with specialist partners. Face algorithms were submitted to NIST Face Recognition Technology Evaluation (FRTE)/ Face Recognition Vendor Test (FRVT) 1:1 , 1:N, quality, and age estimation testing.

Fraud controls use pre-trained, locked ML models with no dynamic retraining and no GenAI in the product, reducing model drift and AI-governance overhead. Document controls include tampering, compositing, template-based, synthetic, and AI-generated or AI-edited image detection. Face and injection controls run through the xFace injection-attack module covering spoofing, masks, AI-manipulated selfie images and video, face-swap, replay, virtual-camera and emulator capture, SDK and API injection, and capture-provenance checks. Separate reason codes and risk scores are returned for AI-assisted document and deepfake fraud, alongside versioned models, a formal update process, and false-positive and false-negative reporting. Device intelligence covers IP, geo-location, device fingerprint, and jailbreak/root checks with velocity limits; user-behavior analytics and behavioral

biometrics are not part of core proofing. PEP, UBO, sanctions, and adverse-media screening, with AML and PSD2 checks, run through integrated third parties, and watchlists are native for photos and extended to IP, document number, and device ID. Risk scores can be weighted within policies to trigger step-up authentication, verification, or additional checks, and manual adjudication is offered as a service from an EU team or by the customer's reviewers.

Privacy controls include user notice for active liveness, passive liveness, and data aggregation, with consent captured before verification or by the customer's system. Sensitive data is encrypted before storage and, for SaaS, held in the region closest to the customer; managed-service data is typically in the customer's country, and self-managed keeps data under customer control. Biometric templates are encrypted and non-reversible, and mobile apps use the Secure Enclave, TEE, or Secure Element for key protection, signing, and on-device biometrics. Retention is customizable per customer and per jurisdiction, from 1 to 90 days. End users are not given direct tools to view or revoke attributes; the customer receives APIs to build GDPR controls, and end-user data is not used for model training by default.

Integration is exposed through REST APIs and webhooks, with client SDKs for Android and iOS, SDKs for Java and .NET, and web integration by redirect or iframe. Orchestration is configured in the TrustX process designer, a BPMN-based graphical tool where workflows and activities are versioned for controlled upgrades and A/B testing. The flows adapt to context such as country or device to change documents requested or fall back from an eID to a physical document, and external checks and custom interfaces are added through Cloud Functions without app-developer involvement. The interface provides per-transaction forensic timelines, statistics, watchlist management, and a manual-review queue with a Reviewer role. Downstream, the platform returns OIDC for Identity Assurance claims, custom claims, and metadata via API, with assurance mapped to eIDAS Low, Substantial, and High, NIST IAL1 and IAL2 (not IAL3), UK DIATF, and Spain's CCN-STIC-140. Named integrations include Ping Identity, Oracle, Broadcom, WSO2, banking platforms such as Backbase and Thought Machine, the ConnectID exchange in Australia, and eID Easy.

Daon is suited for multinational enterprises, particularly in financial services, telecommunications, government, and travel, which need broad document and NFC coverage, deployment flexibility for data residency, independently tested native algorithms, and one platform spanning proofing and ongoing authentication. Daon is less focused on buyers needing mobile driving license or participation to EU digital wallet acceptance today, and buyers requiring FedRAMP, SecNumCloud, C5, or PCI-DSS, or built-in user-behavior analytics should validate fit. Because document processing, liveness, screening, and some data sources can be partner-delivered, buyers should confirm which parts of a flow are native for support, assurance, and data handling.

Strengths

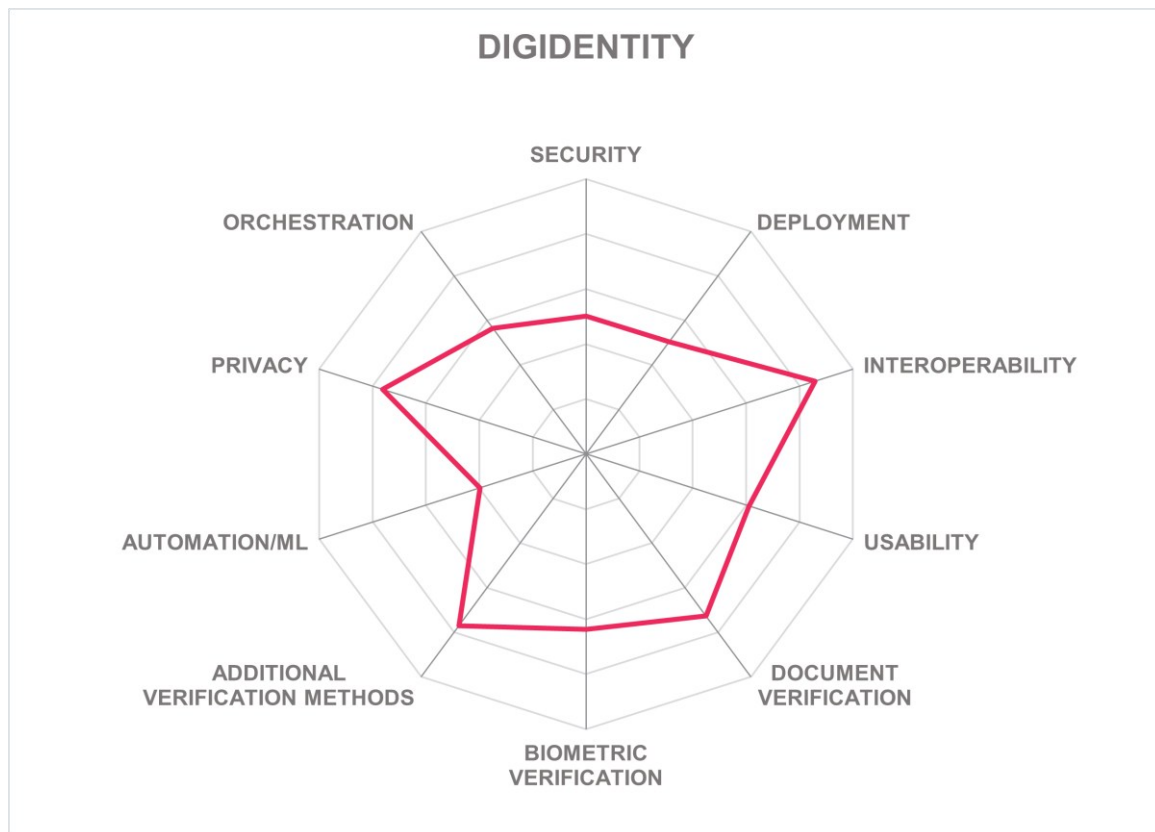
- Deployment flexibility across vendor-managed SaaS on AWS, a customer-dedicated managed service, self-managed software, and a hybrid model that keeps data storage in the customer's environment

- In-house face, voice, and document algorithms combined with independent testing (iBeta PAD Level 1 and Level 2, NIST FRTE/FRVT 1:1 and 1:N participation) reduce reliance on rented algorithms and give procurement teams third-party evidence rather than vendor assertions alone
- Versioned orchestration in the TrustX process designer, where workflows can be A/B tested and adapted to context help buyers maintain many verification flows across jurisdictions
- Identity continuity, where factors registered during proofing are reused for later authentication and step-up on the same platform, can suit buyers that want to cover onboarding and ongoing re-verification without integrating a second vendor
- Layered AI-fraud detection with separate reason codes and separate risk scores for document fraud and for deepfake fraud, built on locked, pre-trained models with no generative AI in the product, can help fraud teams tune thresholds and reduce AI-governance and EU AI Act exposure

Challenges

- Mobile driving license and EU digital wallet support is early: ISO/IEC 18013-5 and 18013-7 are supported and tested with several US and Australian issuers but not deployed in production yet
- Because some components can be partner-delivered rather than native, buyers that require one vendor to own algorithm testing, updates, support escalation, and data handling across the whole flow should confirm which components are native for their specific configuration
- Certification scope has gaps for some regulated buyers: there is no FedRAMP, SecNumCloud, C5, or PCI-DSS certification and the SOC 2 Type 2 attestation is scoped to Security only
- The core proofing flow does not include user-behaviour analytics or behavioral biometrics which may matter for buyers that want transaction-pattern risk signals

Digidentity – Digidentity Identity Wallet and eHerkenning



Digidentity is a Netherlands-based and privately held, qualified trust service provider, founded in 2008 and headquartered in The Hague, which offers identity verification as a standalone proofing service and as the entry point to reusable digital identities. Proofing sits at the center of the portfolio because the company operates as a Quality Trust Service Provider (QTSP) and must establish each subject's real-world identity before issuing qualified electronic signatures, qualified seals, PKI certificates, or an eHerkenning business identity. Buyers can consume the service as one-time proofing, as federated reusable identity, or as a device-held wallet credential, placing Digidentity across the full-service identity verification and reusable verified identity segments. Digidentity's customers are almost entirely in EMEA, and the solution serves consumer, workforce, and citizen identity scenarios, including long-running work for the Dutch and UK governments. Licensing is per identity, per signature, or through annual subscriptions and bundles.

The service is delivered as vendor-managed SaaS. Public-cloud components run on AWS in Dublin and Frankfurt, while security-sensitive elements, the hardware security modules and certificate authority under Digidentity's sole control in the company's own Netherlands data centers in Rotterdam and Delft. A separate in-country platform serves Australia and New Zealand with data held in Australia, so residency follows the operating region. End users

interact mainly through the mobile wallet on iOS and Android, also offered as an SDK. The platform supports multi-tenant and single-tenant operation. It is certified to ISO/IEC 27001:2022 (with 27701, 27017, and 27018) by DNV, audited annually against ETSI EN 319 401, 319 411-1, and 319 411-2 by Attestic, listed as a QTSP on the EU Trust List, and certified under the UK Digital Identity and Attributes Trust Framework through Kantara.

Verification is based on NFC chip reading as the preferred route, developed in-house, and applied to roughly 80 to 85 percent of documents, with ReadID/Innovalor as a fallback. Documents without a readable chip route to optical verification from partners, including DataChecker, Onfido, and Mitek, configured per product and assurance level, with Mitek used for lost or stolen checks. Reported coverage includes chipped passports from around 180 countries and electronic national IDs from about 80, with physical national IDs and driver's licenses also supported, and the wallet handles ISO/IEC 18013-5 mDL where issuers exist. Facial comparison is delivered entirely by the partner BioID, which performs 1:1 matching the wallet holder to the captured document image, with 1:N supported by the engine. Liveness is active only, prompting head movements matched to on-screen prompts. Templates are held centrally in the federated model and on-device in the wallet model, encrypted, and transformed. BioID's engine is the NIST FRTE participant and holds the ISO/IEC 30107-3 PAD results. Attribute aggregation is deliberately narrow and named: credit-reference data through TransUnion, telecom data through Vodafone, and international business identity data through Kyckr, with no bank data aggregation offered, consistent with an architecture that treats the NFC chip, rather than third-party data, as the primary source of truth.

Because capture is app-based rather than browser-based, injection resistance covers screen and video replay, virtual camera, emulator-based capture, and SDK or API image injection, alongside spoofing, mask, face-swap, capture-provenance, and dynamic challenge-response checks. Document fraud handling covers stolen-identity detection by comparing the chip or document image with the selfie and against Interpol or police lost/stolen feedback where a government or financial-services client provides access, plus tamper, compositing, AI-edited-image, and template or synthetic-document indicators. KYC screening covers PEP, UBO, denylist, sanctions, and LEI checks, with AML and PSD2 support including strong customer authentication, and device intelligence includes IP reputation, geo-location, device health, IMEI/SIM, and jailbreak or root checks. The platform returns per-attribute pass, fail, or intermediate results with analyst-visible reason codes rather than an aggregate risk score; it does not weight risk factors or trigger automated policy actions, leaving the decision to the client, with manual override recorded in a full audit trail. Passive behavioral biometrics and broader user-behavior analytics are not offered, and although face-swap and AI-edited-image indicators are covered, suspected deepfake fraud is not separated into its own reason codes, risk score, or false-positive and false-negative reporting.

Privacy controls include consent collected before a persistent identity is created and user notice for active liveness. Sensitive data is stored in AWS Dublin and in the private cloud in the Netherlands, with retention customizable by jurisdictions. End users can see which attributes were collected and verified and can revoke access, though a record of which organizations hold their identity is available only in the EUDI wallet path, not the federated

one. End-user data is not used for model training and is shared only with named sub-processors. Mobile apps use the device Secure Enclave or TEE with keys in the Secure Element, the wallet is cryptographically bound to a single device with no cross-device synchronization, and it supports SD-JWT selective disclosure and immediate self-service account deletion.

Integration is exposed through REST and SOAP APIs and webhooks, secured with OAuth 2.0, OIDC, Security Assertion Markup Language (SAML), and JSON Web Token (JWT), with SDKs for Android and iOS and a developer portal using Swagger and Postman.

Orchestration is evidence-driven: the platform assembles a profile to the required assurance level from configurable evidence sources per product, though extending workflows requires coding in Ruby and no data-mapping workflows are provided. Outcomes are delivered as JSON over API or as a signed PDF proofing report through a self-service portal used by smaller UK right-to-work clients, and identities can be returned as a federated credential over OIDC, as a decentralized wallet credential, or as proofing only. SCIM 2.0 connectors integrate with identity governance tools including Microsoft Entra, One Identity, SailPoint, Omada, and Ping Identity, and with the Thales OneWelcome CIAM platform. A distinguishing capability is chain authorization, which binds a natural person to a legal person through mandates and extends authorizations across company boundaries, applied in a European automotive right-to-repair scheme. Digidentity also issues verifiable credentials through OpenID for Verifiable Credential Issuance (OpenID4VCI) and OpenID for Verifiable Presentations (OpenID4VP) and has begun issuing qualified electronic attestations of attributes.

Digidentity is suited for buyers that need high-assurance remote onboarding, particularly organizations issuing workforce or organizational identities with authorizations, buyers combining KYC with qualified signing, and organizations onboarding users to EUDI wallets. Its remote proofing at eIDAS High has been scrutinized and approved by the Dutch supervisory authority, and its QTSP status, ISO/IEC 27001 certification, and UK DIATF conformance reduce procurement uncertainty for regulated European and UK use. Deployment is SaaS-only and mobile-first, centered on NFC and its app or SDK; buyers requiring browser or desktop-webcam capture, offline verification, or customer-managed hosting should validate fit, as should those whose populations rely on non-chipped documents. Face matching and liveness are partner-delivered, and there is no native risk-scoring or policy engine, so buyers needing single-vendor biometric accountability or configurable risk-based orchestration should confirm the split. Evidenced strength is concentrated in EMEA, with the Benelux and UK as core markets and an automotive-driven presence in Australia; buyers elsewhere should validate document, registry, and support coverage.

Strengths

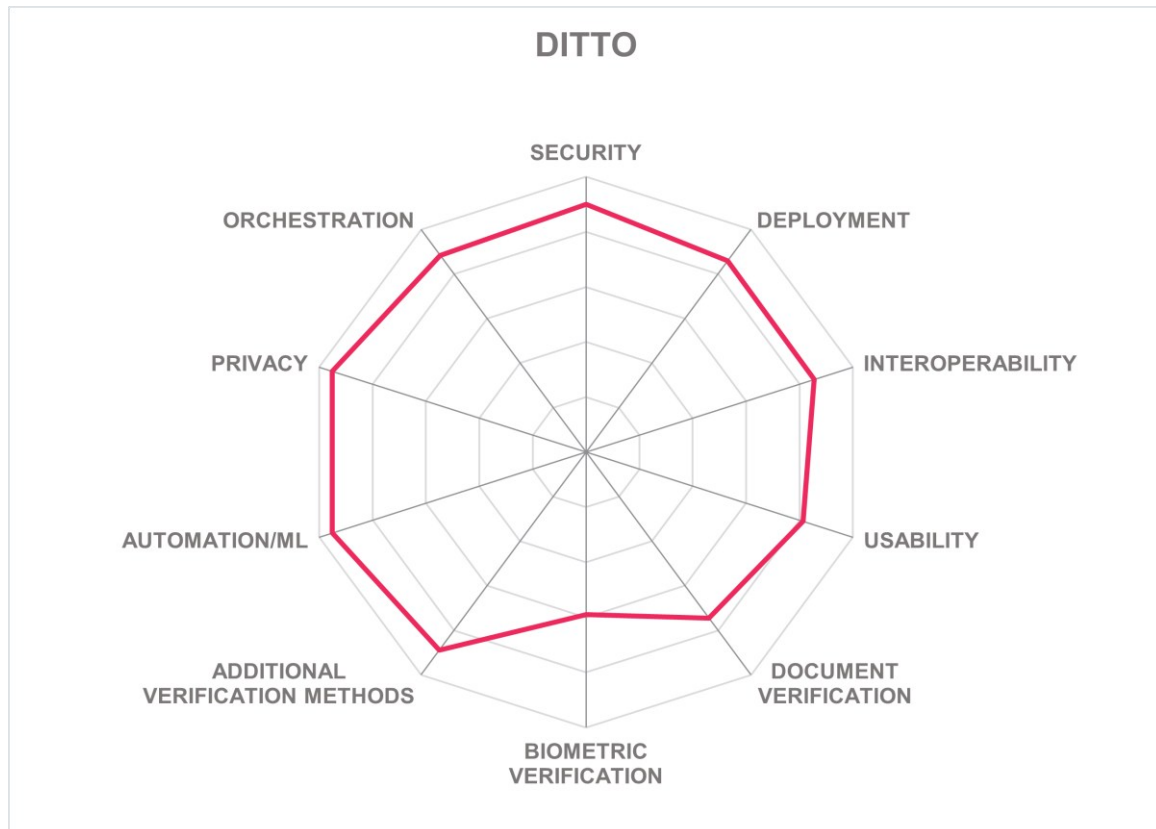
- Native NFC-first document verification developed in-house and used for the large majority of checks, with an NFC fallback engine, gives buyers cryptographic validation of chipped passports and national IDs and reduces dependence on optical fraud detection for higher-assurance onboarding

- Regulator-approved remote proofing at eIDAS High, combined with QTSP status, ISO/IEC 27001 certification, and UK DIATF conformance through Kantara, lowers procurement risk for high-assurance and regulated onboarding in the Netherlands, wider EU, and UK, and lets buyers bundle KYC with qualified signing from a single proofing event
- Organizational identity with chain authorizations that bind natural persons to legal persons through mandates and extend authorizations across company boundaries is a differentiated capability for sector schemes such as automotive right-to-repair, maritime, and healthcare workforce access
- Reusable identity across federated and decentralized models from the same proofing foundation lets buyers consume proofing-only, federated, or wallet-based identity without re-onboarding
- Issuance of verifiable credentials through OpenID for Verifiable Credential Issuance (OpenID4VCI) and OpenID for Verifiable Presentations (OpenID4VP)

Challenges

- Face matching and liveness are entirely partner-delivered (BioID), and optical verification depends on DataChecker, Onfido, and Mitek; buyers that require one vendor should validate how that responsibility is split
- No native risk-scoring or policy engine; buyers that need risk-based orchestration, step-up triggers, or jurisdiction-specific fraud policies should validate whether this must be built in their own systems
- Mobile-first, SaaS-only delivery centered on NFC and its app or SDK. Browser or desktop-webcam capture is not offered, and verification is not available offline, which may limit fit for omnichannel onboarding or for populations reliant on non-chipped documents, where the partner-supplied optical route carries more of the work
- Face-swap and AI-edited-image detection sits inside the partner-delivered biometric fraud-led buyers facing GenAI attack patterns should validate whether the per-attribute pass/fail model gives their fraud teams enough signal

Ditto – Ditto Verify



Leadership



Ditto, headquartered in Barcelona, Spain, is the operating brand of Uniken, Inc., founded in 2013, which has supplied identity and security technology to regulated sectors for over a decade and rebranded to Ditto in early 2026. Built on its REL-ID heritage, the platform offers three modules: Ditto Verify for identity verification, Ditto Authenticate for authentication, and Ditto Protect for mobile threat defense. Ditto Verify is a full-service offering combining document verification, face biometrics and liveness, KYC and AML screening, device and behavioral signals, and a no-code orchestration hub. Verification is sold within a bundle rather than in isolation, and its distinguishing intent is to bind a verified identity to Ditto's split-key authentication for reuse across recovery, step-up, and transaction approval. Primary use

cases are onboarding and KYC, account recovery and re-enrolment, re-verification, high-risk transaction signing, call-center proofing, and KYB. The customer base is concentrated in financial services and in EMEA, APAC (notably India), and Latin America. The same platform serves consumer, workforce, and B2B scenarios. Licensing is subscription-based per active user, with per-verification pricing and enterprise agreements available.

The service is delivered as on-premises software, as a vendor-managed cloud service and as a Ditto- or partner-managed service, in single- or multi-tenant form. SaaS hosting defaults to AWS in Europe (Ireland, Frankfurt); data residency can be pinned to a region, and customer-managed keys and HSMs are supported. Ditto holds ISO/IEC 27001 certification and SOC 2 Type 2 attestation across all five Trust Services Criteria.

Verification is based on a document library licensed from an OEM partner, covering more than 16,000 templates across roughly 195 countries. Capture uses optical image and video, MRZ and barcode reading, and NFC chip reading, while US driver's license data is cross-checked against AAMVA where available. Supported documents include biometric and physical passports, electronic and physical national ID cards, physical and mobile driver's licenses (ISO/IEC 18013-5), and residence permits. Face matching relies on OEM algorithms from a third-party who is a NIST FRTE participant, in both 1:1 and 1:N modes. Liveness detection is passive, analyzing skin texture, lighting, compression artifacts, and micro-movements in video, and returns a liveness score; an optional active challenge-response mode (head turn, blink, voice phrase) is available for step-up flows; the underlying OEM engine passed iBeta presentation attack detection testing at ISO/IEC 30107-3 Levels 1 and 2 in 2020. Attribute verification can additionally draw on aggregated credit-bureau, telecom, banking, utility, and employment data, configured per jurisdiction through the orchestration hub. As with the document library, these data connections are partner-delivered, so buyers should confirm which sources are active for their target markets.

Fraud controls cover document tampering and compositing through pixel-level and lighting analysis, template-anomaly and synthetic-document detection, and detection of AI-generated or AI-edited document images using vision-language models, with cross-modal checks comparing the document portrait against the selfie. Biometric attack coverage includes spoofing, masks, face-swap, AI-generated selfies, screen and video replay, virtual-camera and emulator capture, and SDK- or API-level injection, with capture-provenance and session-integrity checks. Separate reason codes and a dedicated AI-fraud and deepfake confidence score accompany the standard risk score, with versioned models and a deepfake-specific audit trail that let fraud teams tune thresholds and review those decisions independently. KYC and AML screening uses OEM-sourced feeds of more than 3,300 PEP, AML, and sanctions watchlists, with UBO, LEI, and adverse-media checks, transaction screening, and case management. Device intelligence and behavioral biometrics are delivered through the adjacent Ditto Protect module, while graph identity intelligence links users across phone numbers, devices, emails, and IPs to flag stolen and synthetic identities. Policy actions range from allow and step-up to split-key Multifactor Authentication (MFA) through added evidence, manual adjudication, deny, and account freeze.

Privacy controls include notice and consent before document capture, liveness, data aggregation, watchlist screening, and device-signal collection, with consent receipts retained

in the audit trail. Sensitive data can reside in the Ditto-managed cloud with regional residency or in the customer's own on-premises or private-cloud deployment with customer-managed keys. The mobile SDK uses the iOS Secure Enclave and Android TEE or StrongBox for key storage. Retention is configurable per tenant and per jurisdiction and end users can review collected attributes, revoke access, see which organizations hold their verified identity, and exercise data-subject and right-to-be-forgotten requests.

Integration is exposed through REST and webhooks, with OpenAPI specifications, a developer portal, and SDKs for iOS and Android, cross-platform frameworks (React Native, Cordova, Flutter, Xamarin), and server languages (Java, C/C++). Orchestration is handled by an AI-assisted, no-code drag-and-drop journey designer with more than 100 KYC and journey templates, conditional logic, risk-aware routing on document, device, and identity risk, and fallback flows that re-prompt for capture, switch path, step up to active liveness, or route to manual adjudication or a call center. The builder can also output a mobile application scaffold, an Android or iOS project and React Native asset pack with configurable backend URLs, rather than only an API result. Downstream, the platform returns verified attributes, an assurance level, a risk score, reason codes, and verification status, and can trigger policy-driven step-up into Ditto Authenticate. Named integrations include Microsoft Entra and Active Directory, core-banking platforms (Temenos, InfoSys Finance), and SIEM tools such as Splunk and Microsoft Sentinel.

Ditto Verify is suited for regulated financial services buyers that want identity verification bound to a device-bound, high-assurance authentication and mobile-protection stack from a single vendor, and for buyers that need on-premises or region-specific hosting rather than SaaS alone. Because the document library and the face-matching algorithm are OEM-delivered, buyers that require one vendor to own biometric testing, liveness updates, and match-rate data should validate ownership and request test reports. A small customer base concentrated outside North America means buyers elsewhere should validate local document coverage, source-of-truth checks, and support. The differentiation lies in orchestration and in binding verification to authentication rather than in natively owned document and biometric engines.

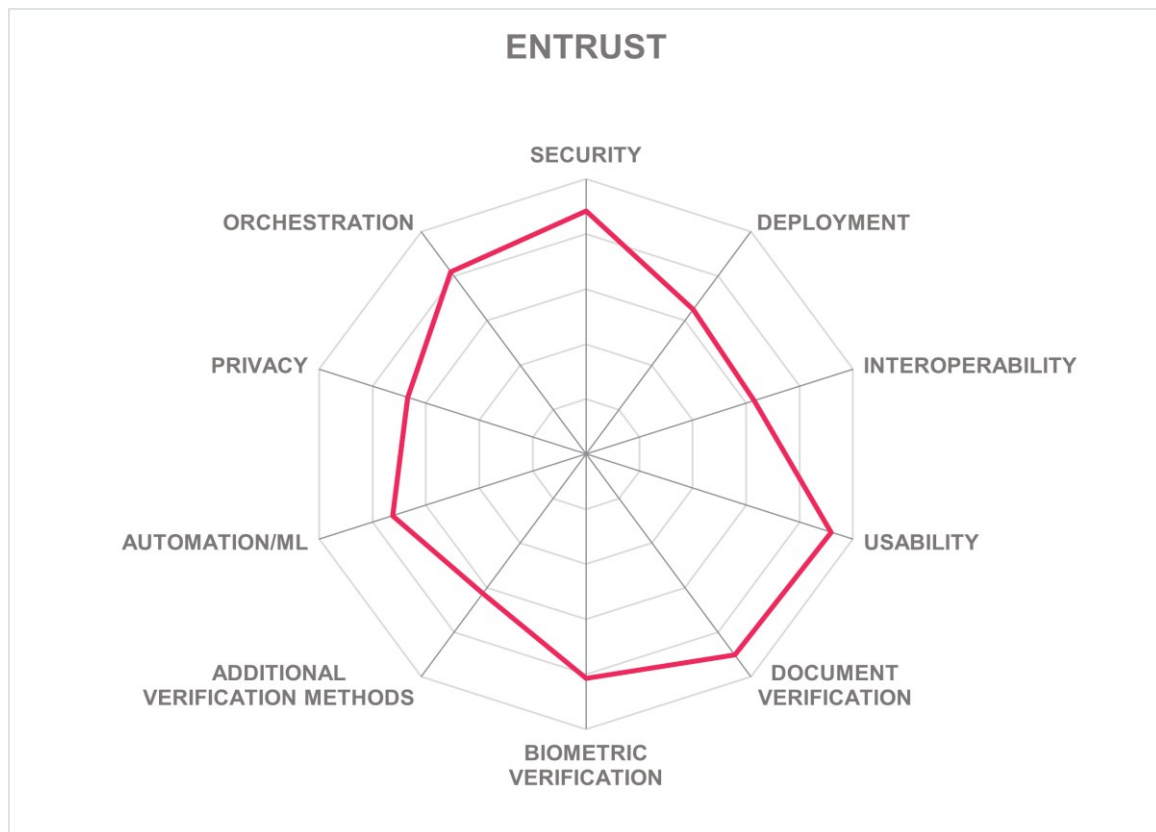
Strengths

- Flexible deployment across on-premises software, vendor-managed AWS and Azure, and managed service can help regulated buyers with data-residency and operational-control requirements
- Verified identity optional binding to MFA and passkeys help buyers maintain continuity from onboarding through recovery, without re-establishing trust
- Separate reason codes and a dedicated deepfake and AI-fraud confidence score are produced alongside the standard risk score; lets fraud teams tune AI-fraud thresholds independently rather than treating all failed verifications alike
- No-code and low-code orchestration with risk-aware routing and configurable fallback paths can adapt verification by document, device, and identity risk without hard-coding each path
- Ability to output a mobile app scaffold plus REST, webhooks, and broad SDKs can shorten build effort for buyers embedding verification into a new mobile onboarding app

Challenges

- Identity verification can be sold standalone but much of the differentiation sits in the adjacent authentication and mobile-protection modules, while the IDV layer itself is orchestration- and OEM-led; buyers seeking a standalone specialist document or biometric engine should weigh this against buyers seeking an integrated verify-authenticate-protect offering
- The customer base is regionalized, so there is limited global-scale production evidence for performance and feature claims. Buyers should validate matching accuracy, liveness performance, and feature maturity against their own volumes rather than relying on vendor-reported results
- Customers are concentrated in financial services across EMEA, APAC (notably India), and Latin America, with no evidenced North American production deployments. Buyers in North America and other markets should validate local document coverage, source-of-truth connectivity, and support before relying on the platform at volume
- Reusable and wallet-based identity support is on the roadmap. EUDI Wallet and verifiable-credential capabilities are planned rather than generally available. Buyers preparing for EUDI wallet acceptance should confirm delivery timelines before committing

Entrust – Entrust Identity Security Platform



Entrust Corporation, headquartered in Minneapolis, Minnesota, privately held and founded in 1969, provides identity, payments, and data-protection products, within which identity verification is delivered through the Entrust Identity Security platform. The identity verification capability originates largely from the 2024 acquisition of Onfido, with government and travel functionality added through WorldReach. Entrust positions verification as a workflow-driven service that establishes trust at onboarding and KYC checks and then reuses it across later for account-takeover prevention, re-authentication, and workforce or know-your-employee (KYE) verification. The platform combines document, authoritative-data, and biometric

signals to return risk-based identity decisions, and its customer base is concentrated in financial services, with additional presence in gaming, gambling, government, border travel, marketplace, and gig-economy verticals. The customer base is concentrated in EMEA, followed by North America. IDV licensing is predominantly per verification with contract-level volume commitments.

The service is delivered as vendor-managed SaaS with managed-service options, hosted on public cloud in three AWS regions: US (us-east-1), EU (eu-west-1), and Canada (ca-central-1), which provide data-residency choices for those markets. All components run full multi-tenancy; no on-premises, single-tenant, or customer-managed hosting is offered. The IDV service is certified as ISO/IEC 27001, holds SOC 2 Type 1 and Type 2 attestations.

Verification is based on native in-house document processing. Capture methods include image and video capture, MRZ extraction, PDF417 barcode reading on driving licenses, and NFC chip reading, alongside checks of physical document security features. Coverage includes passports across 146 countries, driving licenses across 172, national identity cards, and residence permits and travel documents. Source-of-truth checks are partner-delivered, including AAMVA coverage for 43 US states, India PAN, and UK lost-or-stolen document checks. Attribute and data verification, legal name, date of birth, address, and identification numbers, plus proof-of-address documents relies on OEM data providers such as Experian and Equifax. Biometric verification is native and face-only, offering selfie capture with passive liveness or active-liveness check based on a guided head turn, with 1:1 comparison and 1:N matching. Entrust Motion algorithm is certified to iBeta ISO/IEC 30107-3 Presentation Attack Detection (PAD) Level 2 on iOS and Android, and Selfie algorithm to Level 1; a partner algorithm (Paravision) is used only for some government engagements. The platform also verifies some eID schemes and verifiable credentials through Microsoft Entra Verified ID but does not support ISO/IEC 18013-5 mDLs.

Document fraud detection covers tampering, compositing, template-based or synthetic generation, and AI-edited document images, with grid-based anomaly analysis and separate reason codes for suspected AI-assisted document fraud. On the biometric side, the platform detects spoofing, masks, deepfake images and videos, face-swap, screen and video replay, virtual-camera, and emulator capture. It also supports SDK- or API-level injection detection, verifies capture provenance, and supports dynamic challenge-response. Deepfake decisions carry both separate reason codes and a separate confidence score. Device intelligence such as IP reputation, geolocation, impossible-journey checks, and device fingerprinting and reputation, is provided through a partner. KYC and AML screening for PEPs, ultimate beneficial owners, denylists, and sanctions, with ongoing monitoring, is provided by partners. Risk signals feed a weighted risk engine that returns Clear, Caution, Consider, or Rejected outcomes with analyst-visible reason codes, configurable thresholds, and override audit trails. An in-house Fraud Lab red team supported by an active-learning retraining loop maintains models against changing attack patterns.

Privacy controls reflect a processor-by-default model in which the enterprise customer is the controller; the platform surfaces in-UX biometric consent where required. Biometric templates can be stored centrally by Entrust, the customer, or on the end-user device as an Encrypted Biometric Token, or purged once the assessment completes, and are held in an

encrypted, hashed proprietary form. Retention is customizable per customer and per jurisdiction to a maximum of three years after last interaction, customers can download their data at any time, and model training is opt-in.

Integration is exposed through REST APIs and webhooks, capture SDKs for iOS, Android, web, Flutter, and React Native, and backend SDKs for Java, Python, Ruby, PHP. Liveness, orchestration, and e-signature steps are available only through the SDKs. Orchestration is handled natively in Workflow Studio, a no- and low-code engine with more than 30 geography and use-case templates, a patented policy validator that flags when configuration changes drift out of compliance, workflow versioning, A/B testing and gradual rollout, audit logging, and drop-off analytics. Manual review is configurable, run either by the customer or by an Entrust partner located in APAC or the EU. Prebuilt integrations cover Microsoft Entra ID and Entra Verified ID, Okta, Salesforce, Workday, and Entrust Identity as a Service, with API authentication via OAuth2, SAML, OIDC, and JWT.

Entrust is suited for regulated financial-services buyers, and secondarily gaming, government or travel, and marketplace buyers, in EMEA and North America that want high-assurance onboarding and lifecycle re-authentication on one platform, particularly where ETSI TS 119 461 (v1.1.1) and ETSI EN 319 401 identity-proofing certification, UK DIATF, eIDAS Substantial, or NIST IAL2 are procurement requirements, and where Entrust can act as an identity-proofing service provider for QTSPs. Because the offering is SaaS-only, multi-tenant, and public-cloud, buyers with on-premises, private-cloud, or customer-managed hosting requirements should validate fit. eIDAS High and NIST IAL3 are not supported and mDLs are not verified. APAC and Latin America are addressed as country-by-country expansion markets, and data-source and attribute coverage, while broad for documents and biometrics, relies on partners for authoritative data and screening; buyers should confirm source-of-truth and attribute coverage for their specific geographies.

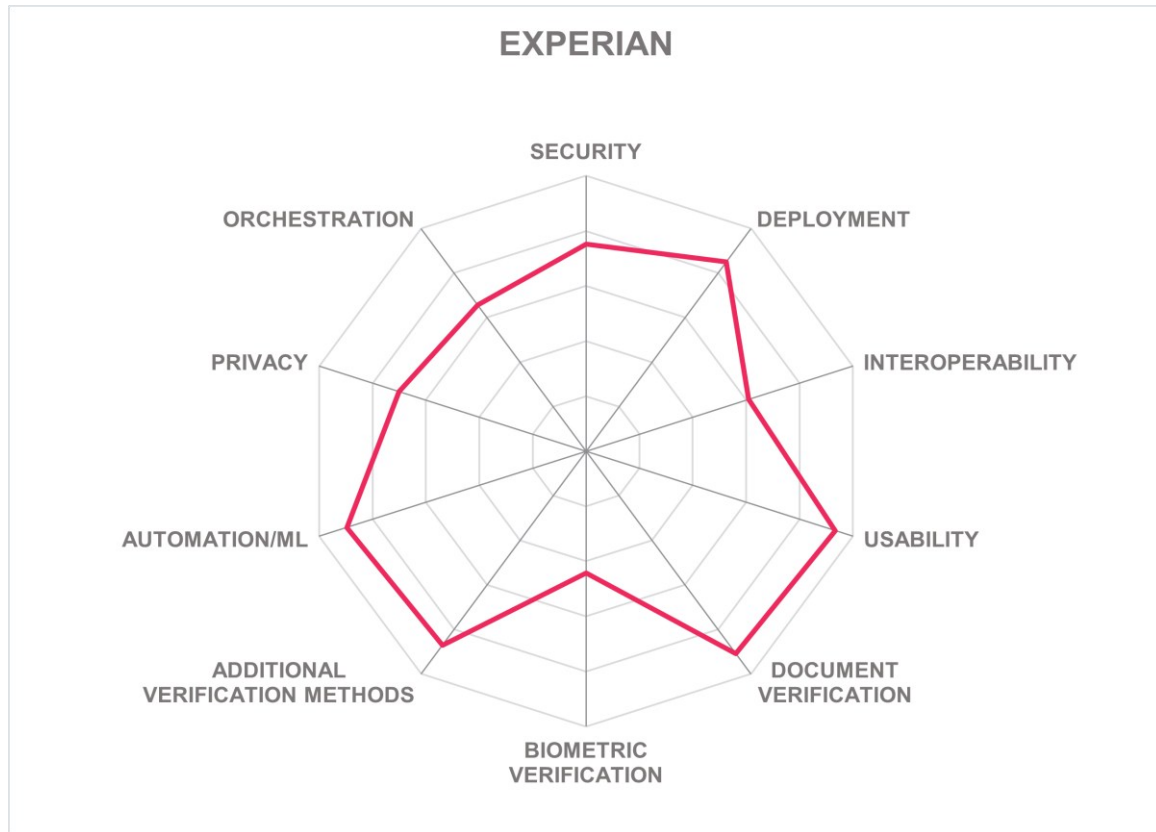
Strengths

- Native, in-house document and face-biometric processing across the core verification path reduces dependence on third parties for the primary onboarding flow and gives buyers a single owner of algorithm testing and updates for documents and biometrics
- Identity-proofing assurance is backed by named certifications: ETSI TS 119 461 (v1.1.1) and ETSI EN 319 401 identity-proofing certification, UK DIATF, and iBeta ISO/IEC 30107-3 PAD Level 2 for Motion, which matters for regulated EU and UK onboarding and for acting as an identity-proofing provider to qualified trust service providers
- Flexible biometric template handling customer storage, or purge-after-assessment, together with jurisdiction-level retention limits, can help buyers that need to minimize vendor-held biometric data under GDPR, Biometric Information Privacy Act (BIPA), or similar regimes
- Patented policy validator flagging workflow configuration drift out of compliance which helps buyers operating across multiple jurisdictions
- Lifecycle coverage that reuses a day-one verified identity for later re-authentication and know-your-employee flows suits organizations consolidating onboarding, account-takeover prevention, and workforce verification on one platform

Challenges

- The service is SaaS-only, multi-tenant, and public-cloud on AWS, with no on-premises, private-cloud, or single-tenant option; buyers with customer-managed hosting or strict processing-location requirements beyond the three AWS regions should validate fit
- Authoritative-data and screening coverage depends on partners
- APAC and Latin America are addressed as country-by-country expansion rather than established coverage, so buyers with large volumes in those regions should confirm document, data-source, and support depth for their markets
- Behavioural and passive biometric signals are collected but not used automatically for decisioning, so buyers wanting continuous behavioural risk as part of the verification decision should validate current capability rather than assume it from the collected data

Experian – CrossCore on Experian Ascend Platform



Leadership



Experian, headquartered in Dublin, Ireland, is a publicly listed data and analytics company, formed in its current structure in 1996, operating across North America, Latin America, EMEA, and APAC. Its identity verification offering, CrossCore on the Experian Ascend Platform, is a full-service verification and orchestration solution positioned within a broader portfolio covering credit risk, fraud prevention, and decisioning, with financial services as the largest client segment. The solution combines Experian-native capabilities with integrated, Experian partner services behind a single API and a common commercial framework: Experian's Data Hub. Primary use cases are consumer onboarding, KYC-related identity proofing, account recovery, step-up verification, age verification, re-verification, call-center verification, and high-risk transaction checks. However, workforce verification is out of scope. Acquisitions shape the capability set: BrScan and AllowMe (document verification

and fraud prevention, Brazil), NeuroID (behavioral analytics), illion (identity data, Australia and New Zealand), KYC360 (compliance workflows), and AtData (email intelligence covering more than 10 billion addresses). Licensing is offered per user, per transaction, or per time period, varying by use case.

The service is delivered predominantly as vendor-managed SaaS in public cloud: more than 90 percent of new deployments follow this model, fewer than 10 percent run on-premises, and private cloud is limited to customers with data-residency or sovereignty requirements. AWS is the primary hosting stack, with Azure used in multi-region environments and Oracle Cloud in limited contexts; data centers operate in the US, UK, Germany, Spain, Brazil, Singapore, India, South Africa, and Australia, with both multi-tenant and single-tenant operation. Covered services are certified against ISO/IEC 27001 and attested under SOC 2 Type 2 across all five trust service principles.

Verification is anchored in attribute checks: legal name, date of birth, address, phone number, national identification numbers, and email are verified against Experian's credit bureau records, telecom intelligence, Open Banking data, public records, electoral rolls, watchlists, and email intelligence. Data depth is strongest in Experian's bureau markets, the US, UK, Brazil, parts of Europe, and Australia and New Zealand, with partner sources closing gaps elsewhere. A distinguishing point is that much of the aggregated data is Experian's own: credit header and trade line attributes and contributed demographic records come from its bureau assets, while telecom, Open Banking, and additional public-record sources are configured per geography and client from partner providers. Bank-sourced checks extend beyond account ownership to statement-based income verification through Open Banking APIs, and electoral roll, postal, and, where permissible, driver's license data are also included among configurable sources. Document verification covers ePassports and physical passports, national identity cards, driver's licenses, and stated support for ISO/IEC 18013-5 mDLs, captured via browser, Android and iOS SDKs, or APIs, using OCR, MRZ and barcode parsing, NFC chip reading, physical security feature checks, consistency validation, real-time authoritative-source matching, and manual review. Document technology mixes Experian-owned capability from its Brazilian acquisitions with partner services such as Mitek and Incode, selected by region or client preference. Biometric verification is limited to face, using 1:1 selfie-to-document matching and both active liveness (guided prompts) and passive liveness (facial texture, depth, micro-movement, ambient light); it is delivered through in-house technology for Brazilian market and through partners in other markets.

Document checks detect AI-generated or AI-edited document images, compositing, and tampering, template-based or synthetic documents, stolen identities, and inconsistencies between document and biometric evidence, with separate reason codes and separate risk scores for suspected AI-assisted document fraud. Face verification detects spoofing, masks, AI-generated or manipulated selfie images and videos, face-swaps, screen and video replay, and SDK- or API-level injection attacks, and verifies capture provenance and session integrity, with distinct reason codes and scores for suspected deepfakes returned partly through partner detection services. Virtual camera and emulator-based capture detection are not supported. Device intelligence contributes to IP reputation, geolocation and geo-velocity, device fingerprinting, device health, jailbreak and root checks, and on-device malware

indicators, while NeuroID-based behavioral analytics evaluate keystroke, mouse, swipe, and touchscreen dynamics to detect bots, remote-access-trojan patterns, and social-engineering behavior early in the journey. Because Experian holds longitudinal credit data, it also runs synthetic identity and first-party fraud models, including bust-out prediction, that document-centric providers cannot derive from a single session. Screening covers PEP, sanctions, denylist, and UBO checks with Global Legal Entity Identifier Foundation (GLEIF) LEI validation and supports AML, US Bank Secrecy Act, and PSD2 workflows. Policies weight risk factors and trigger step-up, continue, refer, or stop actions, with analyst-visible reason codes, manual override under full audit trail, and a separate audit trail for deepfake-related decisions. Model governance includes bias and drift monitoring, and explainability tooling. A GenAI assistant supports strategy design, investigation guidance, case summarization, and governance documentation, with final decisions retained by humans. A MCP server allows agents to submit transactions to detect fraudulent activities.

Consent is collected before verification, including for PII processing, fraud checks, and eCBSV-based social security number (SSN) verification in the US; active liveness is explicitly user-facing, while notice for passive liveness and data aggregation is handled through consent workflows and disclosures rather than always appearing as distinct steps. Retention is configurable per customer and jurisdiction (GDPR, CCPA), regional data remains under regional authority, and end-user data is not used for model training or shared externally. End users can learn which attributes were collected and verified and can revoke a customer's access to their verified identity.

Integration is exposed through a single REST/JSON API with OAuth2, JWT bearer tokens, and HMAC-signed requests; SOAP is also supported, outbound webhooks push workflow notifications, and native SDKs are limited to Android and iOS with browser-based web capture, documented through a developer portal and client implementation kits rather than publicly. Orchestration combines a drag-and-drop strategy designer, rule engine, and no-code configuration with Groovy scripting at defined extension points and built-in workflow templates; a fraud sandbox lets clients build attributes and models on combined Experian, client, and partner data, run champion/challenger tests, and deploy to a monitored model-ops environment under an approval workflow. Enterprise integrations include ServiceNow, Pega, Camunda, MuleSoft, Salesforce, and Microsoft Dynamics, plus CIAM, access management, and MFA platforms. Administrative access uses Okta-integrated SSO (SAML2, OIDC, LDAP) with role-based access control and privileged-access controls; policy changes, administrator activity, and failed access are logged in protected audit trails, exported via REST APIs and webhooks rather than syslog SIEM feeds.

Experian is suited for consumer-facing enterprises, particularly in financial services, e-commerce, telecommunications, healthcare, and the public sector, who want identity verification embedded in a wider fraud and credit decisioning platform rather than a standalone document-and-selfie check. Buyers with verification volumes concentrated outside Experian's bureau markets should test coverage per country. Delivery is SaaS-first with only limited private cloud and on-premises options, and document and biometric technology is a mix of native and partner components, so buyers should validate which provider delivers each check in each region, along with the absence of vendor-held ISO/IEC 30107-3 PAD testing, published NIST FRVT results, and FedRAMP or C5 attestations where

procurement requires them. For organizations that value data breadth, behavioral intelligence, and orchestration depth over single-vendor biometric ownership, CrossCore on Ascend is a credible platform-level choice.

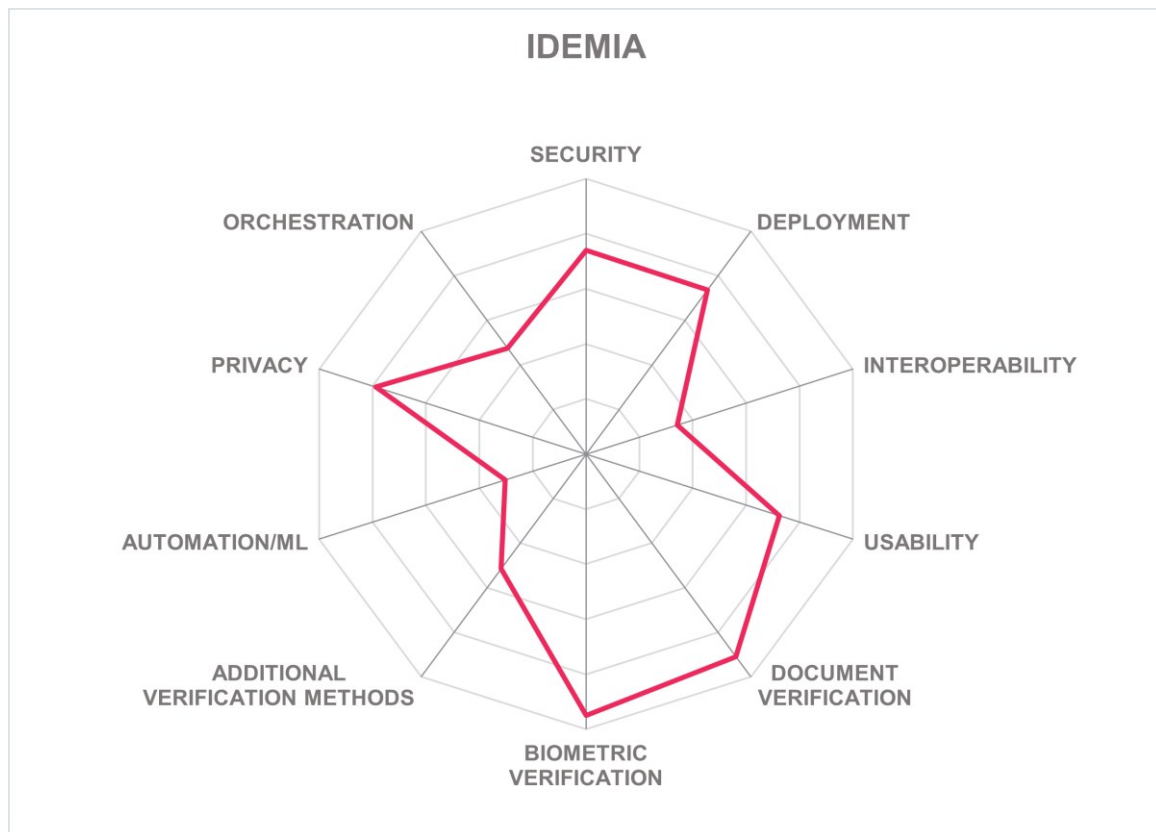
Strengths

- Extensive Cross-domain data assets and attribute verification plus synthetic identity and first-party fraud detection compared to document-centric vendors, especially in Experian's bureau markets
- Native behavioral analytics from the NeuroID acquisition evaluate keystroke, mouse, swipe, and touchscreen dynamics with bot and remote-access-trojan detection inside real-time orchestration, giving fraud teams risk signals before document or biometric steps are triggered
- A fraud sandbox connected to monitored model deployment, and assistant-guided strategy changes under human approval, can shorten iteration cycles from days to minutes for fraud and risk teams that tune policies frequently
- Separate reason codes and risk or confidence scores for AI-assisted document fraud and suspected deepfakes, analyst-visible adjudication evidence, and override audit trails help fraud teams tune thresholds and defend contested decisions
- Hosting across nine countries, jurisdiction-configurable retention, no central vendor biometric database, and no secondary use of end-user data support multinational rollouts with differing privacy regimes

Challenges

- Document and biometric verification mix native and partner technology (Mitek, Incode, Veridas), and Experian holds no ISO/IEC 30107-3 PAD testing in its own name and publishes no NIST FRVT error rates; buyers requiring single-vendor algorithm accountability should validate which provider delivers each check per region
- Face is the only physiological biometric modality and matching is 1:1 only; the absence of 1:N search may matter for buyers that need duplicate-account or fraud-ring detection at the biometric layer
- Verification depth varies with Experian's bureau and data footprint; outside the US, UK, Brazil, and other bureau markets, coverage leans on partner data, which buyers with globally distributed populations should test corridor by corridor
- The offering targets consumer identity flows, so organizations that want to consolidate customer and employee verification on one platform will need to validate the workforce side

IDEMIA – Identity Proofing Platform



Leadership



IDEMIA Public Security is the biometrics and identity division of IDEMIA Group, a privately held French company majority-owned by Advent International. The corporate perimeter is changing: IDEMIA sold its Smart Identity business to IN Groupe in July 2025, and in April 2026 Amadeus announced its intention to acquire IDEMIA Public Security, with closing expected in mid-2027. The Identity Proofing Platform is a full-service identity verification offering combining document verification, biometrics, liveness detection, authoritative data checks, and issuance of reusable digital credentials, serving consumer and workforce onboarding, account recovery, step-up verification, and age verification. The platform shares its core technology with IDEMIA's government business, which issues driver's licenses for US states, giving it direct access to document templates and issuer data that most

competitors obtain indirectly. The customer base is concentrated in North America, weighted toward government and financial services, and predominantly large enterprises. Licensing is per transaction for commercial onboarding flows, per user for government and IAM use cases, and typically priced annually.

The service is delivered primarily as vendor-managed, multi-tenant SaaS on AWS Gov Cloud, with hosting evidenced in US (US West) and EU (Stockholm). Customers can alternatively run the capture SDKs, document verification engine, and liveness engine as Docker containers on their own infrastructure; the administration portal and hosted web journeys are not part of the standard on premises offering and are delivered through managed services partners. IDEMIA holds a SOC 2 Type 2 attestation covering security, availability, and confidentiality. The service is neither ISO/IEC 27001 certified nor FedRAMP certified yet.

Verification is based on natively developed document technology covering more than 4,800 document types, including passports from 171 issuing countries, national identity cards from 105 countries, driver's licenses from 97 countries, and residence permits; gaps remain in parts of Asia, and Chinese documents are not covered. Optical checks combine OCR, document classification, and physical security feature analysis, while NFC chip reading validates ICAO passports and electronic identity cards against country signing certificates from the German BSI master list or directly from issuers. Capture runs through a hosted, brandable web journey or native Android and iOS SDKs, with multispectral desktop scanners for in-person channels, and US mobile driver's licenses conforming to ISO/IEC 18013-5 are accepted as identity evidence. Source-of-truth checks are a differentiator in the US Department of Motor Vehicles (DMV) records in 44 states through AAMVA, live connections to state systems of record where IDEMIA operates its issuance infrastructure, signed-barcode verification keys from some states, Social Security number checks through Experian Precise ID, and phone-number checks against telecom data through Prove; coverage elsewhere depends on partnerships still being established. Biometric verification is also native, with 1:1 matching and 1:N search; templates are stored in a customer-controlled database and not retained beyond the transaction. Liveness is primarily passive video analysis; the earlier active method is deprecated, and a multidimensional liveness check adding a smile prompt and a randomized color-flash challenge is being rolled out against replayed synthetic video. Passive liveness was tested by iBeta at ISO/IEC 30107-3 PAD Levels 1 and 2, the face matching algorithms participate in NIST FRTE with low measured demographic differentials, US Department of Homeland Security (DHS) S&T's Remote Identity Validation Technology Demonstration (RIVTD) evaluation placed IDEMIA first in its liveness detection track, and the proofing flow is certified by Kantara as a NIST 800-63-3 IAL2 component service.

Fraud controls cover both evidence channels. ML models detect AI-generated or AI-edited document images, compositing and tampering, template-based synthetic documents, and inconsistencies between document and biometric evidence. On the biometric side, the platform detects masks, AI-manipulated selfie images and videos, face swaps, and screen replays, plus virtual cameras, emulators, and image or video injection at SDK or API level, supported by capture provenance and session integrity checks. Per-tenant velocity checks flag reuse of the same document within a short window using hashed identifiers, and device

intelligence is limited to IP address, device identifier and type, device fingerprinting, and software signatures. Document verification returns a risk score, negative decisions carry per-check results through the API, and if a target confidence score is not met the flow requests further evidence such as another document or a data-source check. There is no manual review or hybrid adjudication, and no PEP, sanctions, denylist, or AML screening yet. Deepfake defenses are independently tested, with versioned models, a formal update process, and false positive and false negative reporting; there is no separate audit trail for deepfake decisions, and deepfake-specific reason codes are internal only.

Privacy controls rest on data minimization. Users consent at the start of each journey to what is captured, where it is processed, and post-transaction deletion; personal data is retained at most 30 days, customers can reduce retention to zero. Data at rest is encrypted with AES-256 using per-tenant keys in AWS KMS, document-signer keys reside in a cloud HSM. Production data is not used for model training or shared externally; new training data comes from explicitly consented campaigns or synthetic generation. Mobile SDKs use the Apple Secure Enclave or Android TEE, with keys stored in the Secure Element.

Integration is exposed through REST APIs with JSON payloads, webhooks, native Android and iOS SDKs, and a web SDK. Most customers consume the hosted web journey, configured in the portal: accepted document types and countries, optional phone, Social Security number, and address checks, liveness type, branding, and a target assurance level that determines how much evidence the flow collects. IAM integration works through OIDC: an identity provider such as Microsoft Entra, Ping Identity, or Okta triggers verification for recovery or step-up and receives verified attributes in the ID token; this is configuration work rather than a marketplace listing, except for Microsoft, where IDEMIA is pre-integrated with Entra Verified ID, issues verifiable credentials into Microsoft Authenticator for Face Check-based account recovery and is listed in the Azure security marketplace. As a reusable-identity issuer, IDEMIA delivers ISO mDoc-based digital credentials through its SDKs and a white-label ID Wallet app, while W3C-style verifiable credentials are issued exclusively through Microsoft Entra. The portal provides transaction history with event-level session timelines and predefined reports; there is no custom report builder and no case management, and IDEMIA deliberately does not position the platform as an orchestration engine: predefined workflows cover most common flows and extending them requires coding.

IDEMIA is suited for North American enterprises and public-sector organizations that need high-assurance remote verification anchored in authoritative US data sources, and for organizations invested in Microsoft Entra that want verified-identity onboarding and recovery. Organizations that require KYC and AML screening, manual adjudication, or fine-grained fraud policy control should plan for complementary tooling, and prospective customers should account for the pending Amadeus acquisition when assessing support continuity and roadmap items like Fedramp certification and PEP, sanctions, denylist, or AML screening support.

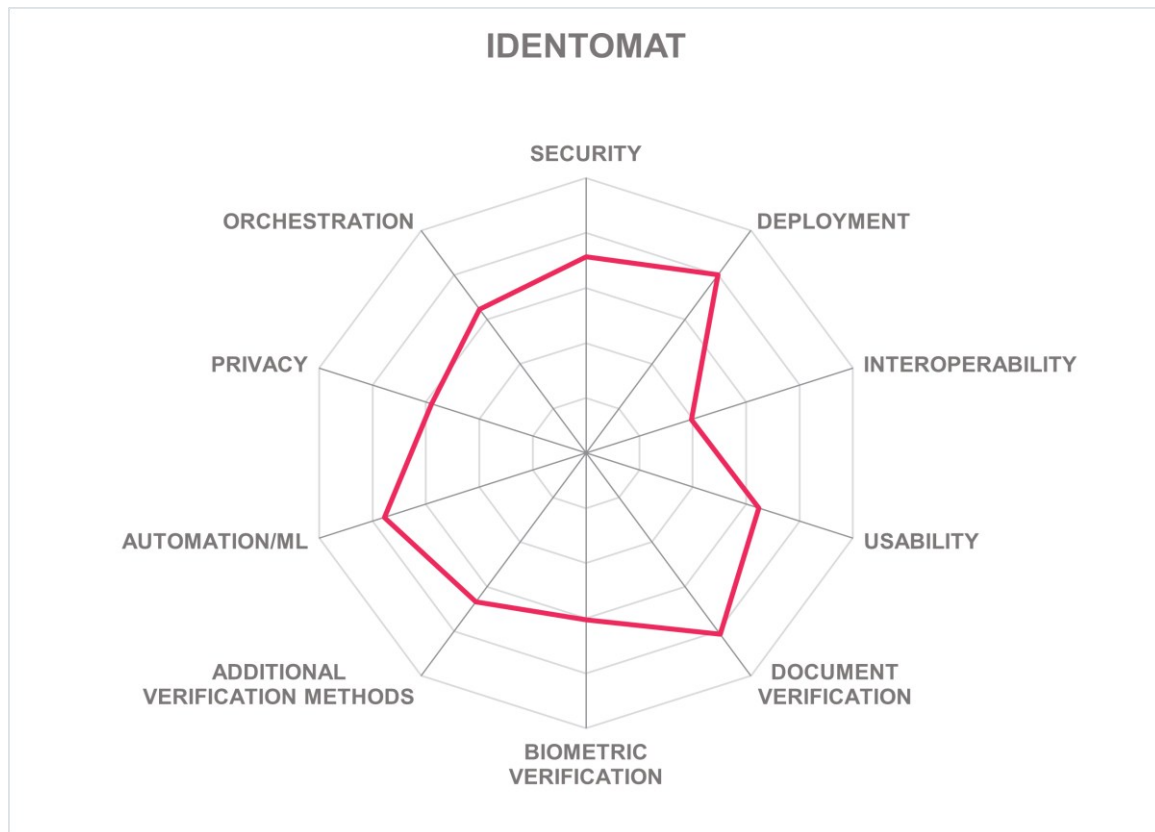
Strengths

- Fully native technology stack across document verification, face matching, liveness, and mDoc credential issuance, validated by independent benchmarks which matter for buyers that want one vendor accountable for algorithm quality, updates, and support
- Authoritative US source-of-truth depth AAMVA checks in 44 states, live DMV system-of-record connections, and signed-barcode keys from some states derived from its own driver's license issuance business that competitors without an issuance footprint cannot easily replicate for high-assurance US onboarding
- Early, standards-based reusable identity position: issues mobile IDs for US states into Apple, Google, and Samsung wallets, accepts ISO/IEC 18013-5 mDLs as verification evidence, and issues verifiable credentials through Microsoft Entra, giving buyers a low-friction path as wallet adoption grows
- Data-minimizing architecture maximum 30-day retention configurable to zero, per-tenant encryption keys, no vendor-held biometric database, and no model training on production data which reduces vendor-concentration and privacy risk for regulated buyers

Challenges

- Customer base, sources of truth, and evidenced hosting are concentrated in the US; Chinese documents are not covered, and gaps remain in parts of APAC, so EMEA and APAC buyers should validate document coverage, data-source availability, and data residency before committing
- Service-level certifications are thin for a vendor of this profile: no ISO/IEC 27001 or FedRAMP for the SaaS service, which may lengthen procurement in regulated environments
- No KYC or AML screening (PEP, sanctions, denylists) is available today, so financial services buyers must pair the platform with a separate screening provider
- No manual review or adjudication tooling and limited fraud-policy configurability, no risk-factor weighting, no per-jurisdiction policies short of separate tenants, no manual override audit trail, and deepfake reason codes that are not exposed to customers, which may matter for fraud teams that need analyst workflows and explainable overrides

Identomat – Identomat



Identomat, headquartered in London, UK, is a venture-backed identity verification vendor founded in 2019, operating as Identomat Inc., with engineering roots in Tbilisi, Georgia. The Identomat platform combines document verification, facial biometrics and liveness detection, AML, PEP, and sanctions screening, operator-led video verification, business verification (KYB), and transaction monitoring (KYT) on one proprietary stack with shared orchestration. Document and biometric technology are developed in-house; watchlist and other compliance data and the audio/video communication layer are partner sourced. Primary use cases are remote customer onboarding, account recovery, step-up verification for high-risk transactions, age assurance, and video KYC. The customer base is concentrated in EMEA, above all Eastern Europe and the Caucasus, with financial services, fintech, telecom, online gaming, and government as the most active verticals. Licensing is per verification, per screening, or per event, with volume-tiered bundles.

The service is delivered primarily as vendor-managed SaaS on AWS in Germany and the US, backed by Google Cloud Platform (GCP) capacity in Germany; most new installations run in the public cloud. On-premises and bring-your-own-cloud deployments are also delivered through managed services partners, with production on-premises installations reported in Georgia, Ukraine, and Uzbekistan where data residency requirements exclude

the default cloud regions. The service has ISO/IEC 27001 certification and SOC 2 Type 2 attestations covering all five trust service criteria.

Verification is based on optical document capture by image or video, file upload, and NFC chip. Coverage includes passports from 193 issuing countries, ePassports from 138, electronic and physical national identity cards from respectively 75 and 168 countries, and driver's licenses from 165. However, ISO/IEC 18013-5 mDLs are not supported. Authenticity checks combine MRZ and visual-zone consistency, physical security feature checks, and template-based document recognition, and extracted attributes can be cross-checked against a small set of issuing-authority sources in Georgia and Ukraine and against the US Social Security Administration. Attribute checks cover name, date of birth, address, phone, email, and identification numbers through credit-reference, telecom, and aggregation sources concentrated in Georgia and Ukraine, plus proof-of-address documents, OTP checks, and geolocation. Biometric verification is native 1:1 face matching, with an optional 1:N deduplication. Passive liveness analyzes a three-second selfie video, active liveness uses a randomized smile prompt, and an adaptive mode in the native mobile SDKs starts passive and steps up to active on low confidence. A video verification module supports operator-led calls with up to ten participants, per-participant verification steps, and in-call document signing, and is in production with public-sector and banking customers.

Fraud detection relies on in-house ML and computer vision models. Document checks target AI-generated or AI-edited images and template-based synthetic documents through document liveness, screen, photocopy, and edge detection, plus tamper indicators such as font consistency, MRZ checksums, face-photo tampering, and visual-zone-to-barcode matching. Biometric defenses cover masks, face swaps, screen and video replay, virtual cameras, emulators, and SDK- or API-level stream injection, with capture provenance and session integrity checks; the liveness component holds iBeta confirmation letters for ISO/IEC 30107-3 presentation attack detection at Levels 1 and 2. Recurring-face recognition and opt-in denylist APIs flag reuse of the same face or document, and device signals include IP address and reputation, geolocation, VPN detection, device fingerprinting, and jailbreak or root checks. A rule engine assigns weighted risk scores, including country scores, and drives accept, hold, reject, step-up to NFC or liveness, enhanced due diligence, or manual-review actions. Analyst-visible reason codes flag suspected AI-assisted document fraud and deepfake suspicion, and reporting separates document, biometric, deepfake, and synthetic identity cases.

Privacy handling follows the deployment model: sensitive data and biometric templates are stored centrally in Identomat's cloud or in the customer's environment, role-based and privileged access controls, and a tamper-protected audit trail. Encryption keys can be customer-managed, on-premises or in cloud. Consent steps are configurable per flow, and retention policies can be set per customer and per jurisdiction. Customer data is not used for model training unless both the business customer and the end user opt in. End users are informed of active and passive liveness and data aggregation, but the platform provides no end-user self-service controls to view, revoke, or track access to verified attributes; the mobile SDKs do not use the device Secure Enclave or TEE.

Integration is exposed through REST/JSON APIs, webhooks, an iFrame web flow, and SDKs for Android, iOS, Web/React, React Native, and Flutter, with a developer portal and sandbox. A no-code, drag-and-drop workflow builder defines configurations invocable by URL, embedded widget, or SDK; workflows can layer step-up requests within one session, documents, then liveness, proof of address, or proof of funds, and fall back to alternative configurations on risk triggers. Verification can run fully automated end-to-end, with hybrid adjudication where customers require it; manual review runs through pending queues, case management with analyst comments and justifications, and manual override with a full audit trail, while administrator access is role-based and can federate through SAML, OIDC, or Microsoft Azure AD. Connections to issuing databases are backend custom integrations rather than workflow-builder components. The platform returns verification status, extracted attributes, match scores, and device details downstream, but no prebuilt CIAM or IAM connectors.

Identomat is suited for small to mid-market financial services, fintech, gaming, telecom, and public-sector buyers, particularly in Eastern Europe, the Caucasus, and Central Asia, who want configurable onboarding, screening, and monitoring from one vendor with deployment flexibility that extends to on-premises operation for data residency. The combination of in-house liveness with iBeta-tested presentation attack detection and an operator-led video channel differentiates it in regulated scenarios where automated flows need a human escalation path. Buyers should weigh Identomat's small-size against enterprise support and roadmap expectations, validate document performance and data-source coverage outside the core region, and note that assurance rests on ISO/IEC 27001, SOC 2 Type 2, and PAD testing rather than NIST FRVT participation.

Strengths

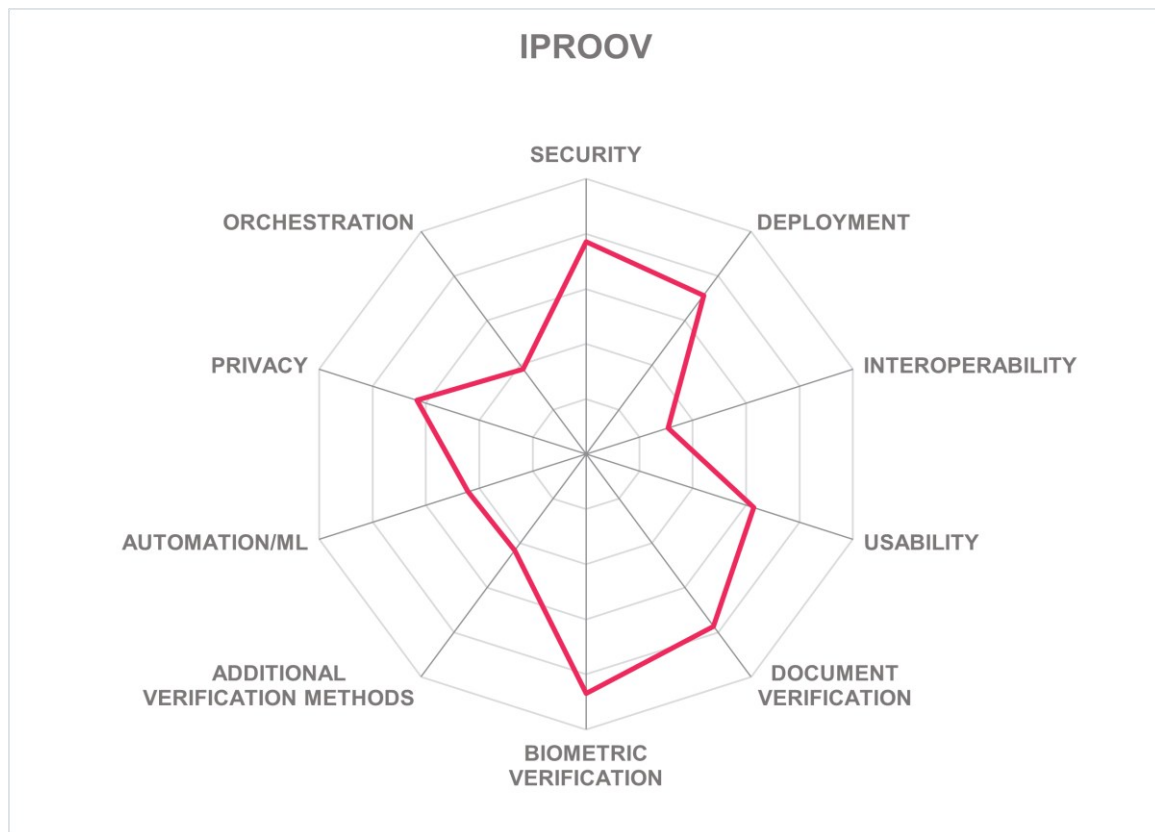
- A single proprietary stack covering document verification, face matching, liveness, video verification, and orchestration simplifies due diligence for buyers
- The liveness detection is certified ISO/IEC 30107-3 presentation attack detection at Levels 1 and 2
- The solution is connected to issuing-authority sources in eastern Europe that are not covered by other vendors
- Deployment flexibility across public cloud (AWS and GCP in Germany and the US), on-premises, local cloud, and bring-your-own-cloud, help buyers in markets where data residency rules exclude the major cloud regions
- Layered liveness, passive, active with randomized prompts, and adaptive step-up in the mobile SDKs which matters for buyers facing replay and injection attacks in remote capture flows
- The operator-led video verification module, with up to ten participants, per-participant verification steps, and in-call document signing, can serve notarial, multi-party, and regulated escalation scenarios that fully automated flows do not cover

Challenges

- The company remains small, with revenue concentrated on one product line
- The customer base and data-source coverage are heavily concentrated in Eastern Europe and the Caucasus

- Authoritative source-of-truth coverage is limited to a small number of issuing-authority connections, and AML, KYB, and watchlist data are partner-sourced
- Independent validation is partial: the face matching algorithm has not been through NIST FRVT
- There are no prebuilt CIAM or IAM connectors; embedding verification into onboarding, account recovery, or step-up flows requires custom integration through REST APIs, webhooks, and SDKs

iProov – iProov



iProov, privately held, founded in 2011, and headquartered in London, UK, is a biometric verification vendor whose portfolio has expanded from liveness detection into a multi-product company. Its identity verification portfolio covers remote onboarding, authentication, and a Workforce Solution Suite, all built on the company's Express and Dynamic Liveness face verification. iProov is a biometric-first provider rather than a full-service identity verification provider: biometric capture, liveness detection, and the service platform are native, while optical document verification, attribute checks, and face-matching algorithms are delivered through partners, under a single iProov contract and support line. Its customer base is strongest in EMEA, with additional presence in North America, APAC, and Latin America and is concentrated in government and large financial institutions, with use cases covering consumer and workforce onboarding, step-up and privileged-access verification, shared-device authentication, and account recovery. Licensing is per user for the workforce suite and per transaction for the IDV solutions.

The service is delivered as vendor-managed SaaS operated as a managed service, running entirely in public cloud with GCP as the primary environment and data centers in the US, Brazil, the Netherlands, Singapore, Indonesia, and Australia. Multi-tenant delivery is standard, with single-tenant clusters for customers with stricter isolation requirements. Customer-managed software is not offered; on-premises or private-cloud hosting is possible

only as a locked-down installation that iProov installs, operates, and updates, offered case by case rather than as a standard delivery model. The service is audited against ISO/IEC 27001 and SOC 2 Type 2 and holds CSA STAR Level 2 and UK Cyber Essentials.

Verification is fully automated, with no hybrid adjudication: by agreement with the customer, Security Operations Center (SOC) analysts review a sample of passed and failed transactions to track attack patterns and retrain models, this review never changes a transaction result, and the liveness check completes in under two seconds. NFC chip reading is native and covers any NFC-enabled document, while optical verification of non-chipped passports, identity cards, and driver's licenses is partner-delivered, giving broad but partner-dependent country coverage. The solution supports mobile driver's licenses according to ISO/IEC 18013-5, eID verification, and presentation of verifiable credentials; iProov built the California DMV Wallet and holds a direct connection to that issuing database, other authoritative checks run through partners or connections the customer already holds. Document fraud controls cover physical security features, tampering and compositing, and template-based, synthetic, or AI-edited document images. Biometric verification is face-first with 1:1 matching; the matching algorithms come from partners ranked in NIST FRTE evaluations, while passive liveness is iProov's own patented Flashmark mechanism, which illuminates the user's face with a one-time screen-color sequence that cannot be replayed.

Attack detection is layered: imagery-based algorithms address presentation attacks, masks, AI-generated or AI-manipulated selfie images and videos, and face swaps, while metadata-based algorithms evaluate timing, operating-system, and screen properties, jailbroken or rooted devices, emulators, virtual cameras, and image or video injection at SDK or API level, including capture-provenance checks. Each attack type is covered by at least three independent tests, and all tests must pass before a result is issued. The customer receives a binary pass or fail: risk scores are generated internally but not exposed, and iProov positions the fixed threshold as an assurance feature rather than a configuration option, with reason codes for suspected deepfake or AI-assisted fraud and separate reporting for document, biometric, deepfake, and synthetic-identity fraud; the result is a digitally signed JSON response collected out of band from the iProov server, so the outcome does not depend on the integrity of the end-user device.. The iProov Security Operations Center monitors production traffic for attack patterns and biometric performance, runs a red team that researches fraud methods on dark-web forums, and feeds a formal model-update process with versioned, auditable models and a separate audit trail for deepfake-related decisions. iBeta confirmed ISO/IEC 30107-3 PAD Levels 1 and 2, the UK National Physical Laboratory assessed performance under ISO/IEC 19795-1, the FIDO Alliance certified Dynamic Liveness under its Face Verification program through Ingenium Biometrics, and injection attack detection was tested against CEN/TS 18099 at Ingenium Level 4. Verified Meetings, announced as generally available in May 2026, extend the same deepfake and virtual-camera checks to live video calls. Device intelligence includes IP addresses, device identifiers and fingerprints, device health and reputation, and jailbreak checks; user behavior analytics, behavioral biometrics, and KYC screening are not provided.

iProov acts as a processor under GDPR. Consent is collected before verification, users are informed of the passive liveness check, and the default retention period of 30 days is

configurable per customer and per jurisdiction. Captured imagery is used to retrain defense models under controls defined in the data processing agreement, and customers can opt out of cross-customer threat analysis. Data is encrypted at rest and pseudonymized, keys are held in HSMs managed by the cloud provider, and mobile apps use the device Secure Enclave or TEE.

Integration is exposed through REST APIs secured with OAuth2 and OIDC, Android and iOS SDKs, and a web capture flow, supported by a developer portal with a sandbox. OIDC federation allows configuration inside IAM platforms without custom code, with Microsoft Entra and PingOne as the evidenced product integrations, and a Windows credential provider brings face verification to shared-device Windows logon. Built-in workflow templates, data-mapping workflows, and low-code enablement inside IAM platforms are available, while extending workflows requires coding; logging covers policy changes, administrator activity, and failed access, with tamper-protected audit logs and syslog export for SIEM consumption. Administration of the workforce products is currently API-driven, without a management console.

iProov is suited for governments, banks, and other regulated enterprises that need high-assurance remote face verification at national or enterprise scale, and for identity platforms that embed a certified liveness layer alongside their own document and data checks. Its published certification listing covers ETSI TS 119 461 remote identity proofing at substantial and high levels under eIDAS, UK Digital Identity and Attributes Trust Framework (DIATF) certification via Kantara, and an Australian IRAP assessment at Identity Proofing Level 3; buyers should still validate the certificate scope for their specific use case. The trade-offs are structural: delivery is vendor-managed with public-cloud SaaS as the standard model, document and attribute verification depend on partners, decisioning is a fixed binary result governed by iProov rather than by the customer, and KYC screening and case management are absent. Buyers seeking one vendor to own the full verification, screening, and review chain should validate the operating model; buyers prioritizing independently tested resistance to presentation, injection, and deepfake attacks will find one of the more extensive evidence sets in this market.

Strengths

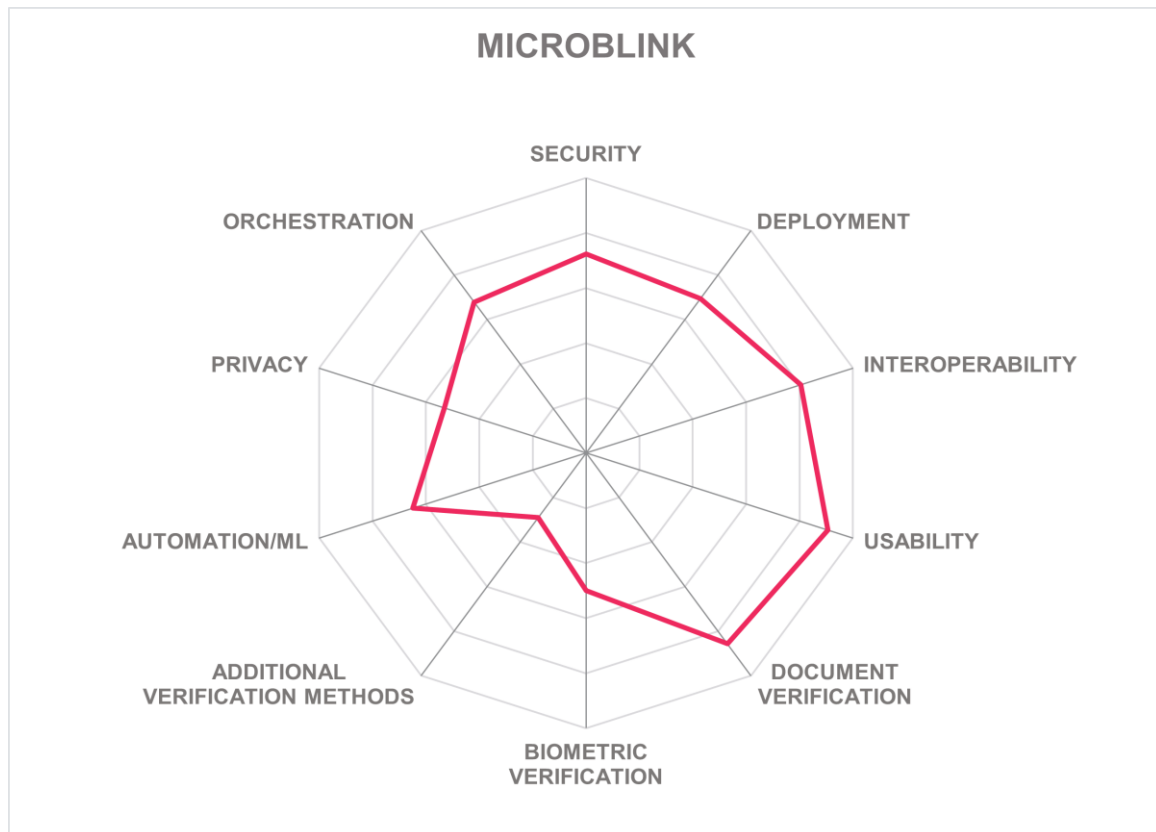
- Extensive third-party certifications and independent testing reduce procurement risk for organizations requiring validated biometric controls. Advanced deepfake and injection attack protection, combining multiple anti-tampering and capture-integrity techniques, helps organizations defend against sophisticated AI-assisted identity fraud
- A biometric-specific SOC with a red team, dark-web threat research, versioned models, and a formal patch process give buyers an operational defense that adapts to novel attack types between certification cycles — relevant for national-scale and financial-sector deployments
- Delivery of a digitally signed verification result directly from the iProov server allows relying parties to trust outcomes from untrusted devices and networks, supporting zero-trust architectures in onboarding, account recovery, and privileged-access flows

- The Workforce Solution Suite, including Verified Meetings for real-time deepfake checks in video calls, addresses remote-hiring and employee-lifecycle fraud scenarios that few identity verification vendors cover as packaged product

Challenges

- Optical document verification, attribute checks, and face-matching algorithms are partner components; iProov contracts and supports the assembled service as a single vendor, but buyers should confirm which partner algorithm is in production for their contract.
- Decisioning is a fixed binary pass or fail set with each customer: internally generated risk scores are not exposed, thresholds and fraud policies cannot be changed by the customers-, and there is no manual adjudication or override, which limits fit for fraud teams that tune verification outcomes by risk appetite, geography, or channel
- Delivery is a vendor-managed service: public-cloud SaaS in the listed hosting regions is the standard model, and on-premises or private-cloud hosting is available only as a locked-down installation that iProov operates and updates, offered case by case
- No native KYC screening (PEP, sanctions, denylists), data aggregation, user behavior analytics, or case management is provided, so buyers needing full-service onboarding compliance must assemble those functions from partners or their own stack
- Enterprise administration is still thin: workforce lifecycle management is API-driven without a management console today, evidenced IAM product integrations are limited to Microsoft Entra and PingOne

Microblink – Identity Intelligence OS



Leadership



Founded in Croatia in 2013, Microblink is a privately held identity verification vendor with offices in the United States and Croatia, employing about 150 people. The company began as a supplier of document capture and OCR technology embedded by other identity verification providers and now sells its own platform, Identity Intelligence OS, directly to enterprises. The platform combines document capture and verification, face biometrics with liveness detection, watchlist screening, payment card capture, and non-identity document extraction; a full-service identity verification offering that combines native technology with OEM components and that is licensed per transaction. Primary use cases are consumer onboarding and KYC, fraud prevention, re-authentication and step-up verification, and payment card verification, with a customer base concentrated in North America and EMEA.

The service is delivered as vendor-managed SaaS on GCP, with data encryption keys managed through Google KMS. Hosting is primarily in EU and US regions, with in-country deployments available for data sovereignty requirements. Customers can instead self-host the services as Docker images on infrastructure or cloud of their choice; a managed service is not offered, and most installations run in the public cloud. Microblink is certified against ISO/IEC 27001:2022 and ISO/IEC 27701:2019, holds a SOC 2 Type 2 attestation covering the Security and Availability criteria.

Verification is based on document verification built in-house, covering more than 6,500 document types from 195 countries and territories, including passports, national identity cards, driver's licenses, and other government-issued documents. Capture runs through mobile and web SDKs or hosted web links, with on-device real-time image quality analysis, automatic capture without frames, end-user real-time cues or manual shutter input, and desktop-to-mobile handoff. Embedding-based classification lets the engine extract data from document types it has not been trained on, and over-the-air updates add new document support without SDK upgrades or app-store resubmission. Document checks evaluate around 60 data points covering GenAI detection, physical security features, photo tampering, data and barcode consistency, document liveness against screen and photocopy presentation, and validity. NFC chip reading, mobile driver's licenses according to ISO/IEC 18013-5, national eID schemes are not supported; NFC and mDL support are planned. In the US Department of Homeland Security Remote Identity Validation Rally concluded in 2026, Microblink was the only participant to meet the program's high-performing thresholds across all three document-validation error rates (False Acceptance Rate, False Rejection Rate and System Error Rate), on a corpus of primarily US documents. Face verification performs a 1:1 comparison between the document portrait and a selfie with passive liveness detection; this capability is OEM-delivered and passed the NIST FRTE benchmark and ISO/IEC 30107-3 PAD testing. Attribute checks on name, address, phone number, SSN, and email are sourced from third-party data aggregators and focus on the US market, while partner-sourced PEP, sanctions, and adverse media screening with continuous watchlist monitoring applies globally. The same extraction pipeline processes non-identity documents such as paystubs, tax forms, and proof of address, with an LLM-based fallback for long-tail formats, and payment card capture adds BIN checks and card liveness binding them to a unified user profile.

Fraud controls center on fully automated decisioning without vendor-side human review. A native detection check for AI-generated or AI-edited document images is enabled by default and configurable across ten match levels, alongside photo-forgery and compositing detection and recognition of template-based synthetic documents. On the biometric side, the solution supports detection of AI-manipulated selfie images and videos, face swaps, replays, virtual cameras, emulators, and image or video injection at the SDK or API level, with capture provenance verified through a remote trust service and image metadata checks. Verification returns a recommended outcome with per-check results, scores, and reason codes, including separate reason codes for suspected AI-assisted document fraud; no separate deepfake-specific score is provided for biometric checks. Device intelligence is limited to IP address, geolocation, and device type, and the solution performs no user behavior analytics or behavioral biometrics. Risk factors can be weighted, thresholds tuned per check, and outcomes routed to step-up verification or customer-run manual review.

Model governance is documented in a published framework, with document extraction models typically updated quarterly and verification models every six to eight weeks, each version required to demonstrate measured improvement over the current production model in accuracy, latency, domain coverage, and bias, and production accuracy monitored against expert-established ground truth where a data sharing agreement allows.

Privacy controls include consent collection before verification, covering fraud prevention, sanctions screening, AML obligations, and audit trail creation. By default, Microblink does not retain PII, and customers choose whether biometric templates and verification data are stored on Microblink's platform or on their side, with retention, consent, and data processing agreements configurable per customer and per jurisdiction. End users can learn which attributes were collected and revoke the customer's access to them, and end-user data is used for model training only where consent is given. Administrative activity, policy changes, and failed access attempts are logged in read-only, PII-free form, although syslog or SIEM forwarding is not available.

Integration is exposed through REST APIs, webhooks, and JSON payloads secured with OAuth 2, JWT, and API keys, and through SDKs for iOS, Android, JavaScript and React, React Native, Flutter, .NET, Python, and C/C++, including a headless variant. The Command Center's no-code workflow builder provides templates with four preset policies from permissive to very strict, per-check threshold adjustment, and rules such as age and document expiry. Funnel analytics trace user journeys down to SDK-level events such as camera permission denials, retries, instructional messages, demographics (cohorts per devices/platforms, document type, country/ region) and an activity view exposes per-transaction evidence that can also be retrieved through a single API request. Unified user profiles allow returning users to be recognized without a full re-check. Administrator access is managed through a bundled third-party IAM service with OIDC, passkeys, enterprise single sign-on including Google and GitHub, and role-based access control. SAML based enterprise identity providers, including Microsoft Entra ID, can be enabled through the same service.

Microblink is suited for organizations that need high-volume, fully automated, document-centric verification across web, mobile, kiosk, and assisted in-person channels, particularly in the US and Europe, and for buyers that value configurable thresholds and capture-level telemetry over vendor-run adjudication. Flows requiring chip-based document verification or national eID integration cannot be served today. Buyers should validate the announced transition of biometric verification from the current OEM partner to an in-house stack, the depth of authoritative data sources outside the US, and their own capacity to operate manual review where regulation demands it.

Strengths

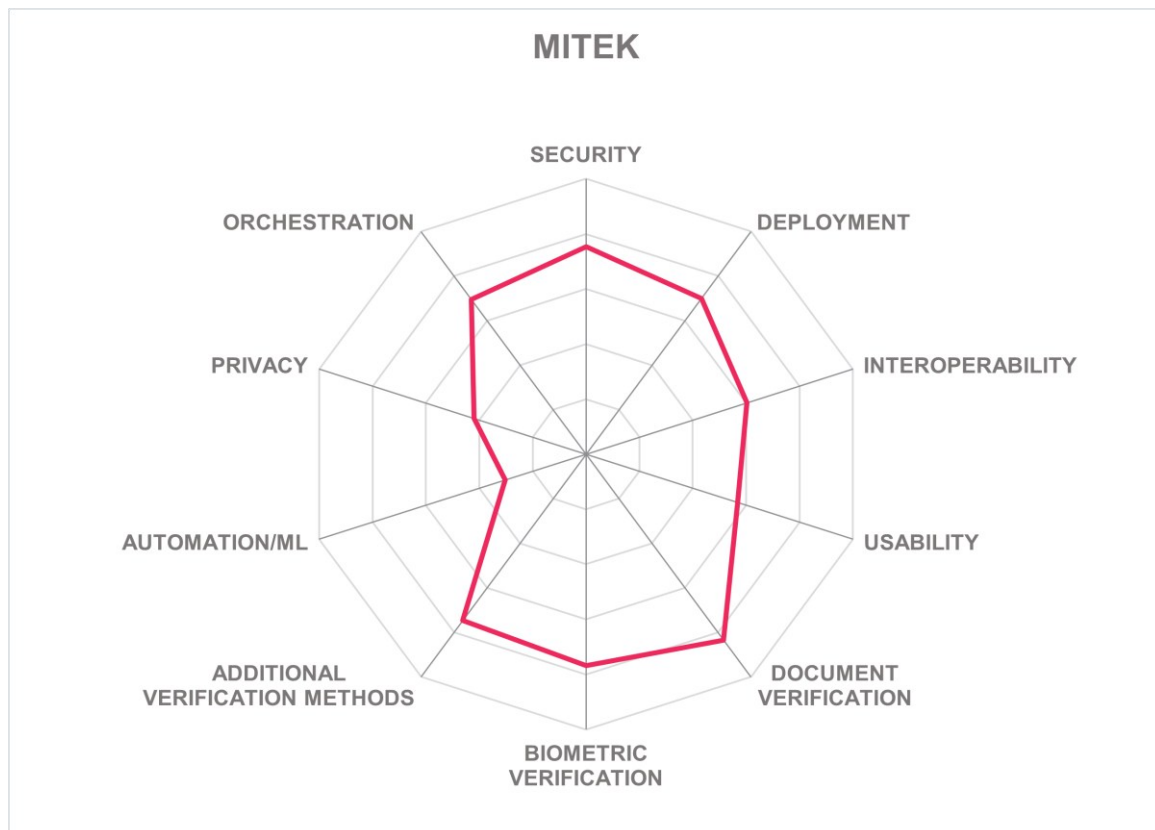
- Met all high performing thresholds in the DHS Remote Identity Validation Rally, giving buyers third party evidence on validation accuracy particularly for US document portfolios

- Extensive library of supported documents combined with embedding-based extraction of previously unseen documents, and over-the-air document updates shortening time-to-support for new documents
- Signal-level transparency and configurability, with per-check thresholds, four preset policy levels, reason codes, and funnel analytics down to SDK events, can help fraud and product teams tune false accept and false reject trade-offs instead of consuming an opaque vendor decision
- Payment cards capture with BIN checks and non-identity document extraction in the same workflow extend verification beyond ID-plus-selfie journeys, which suits lenders, marketplaces, and gig platforms with proof-of-income or card-binding needs
- Documented model governance covering update cadence, mandatory measured improvement before release, in-production accuracy monitoring, and a maintained risk register, giving buyers an auditable basis for AI governance diligence

Challenges

- Face matching and liveness are currently OEM-delivered, and the cited NIST FRTE and PAD test results belong to the partner algorithm; with an in-house biometric stack announced as a replacement, buyers should validate algorithm continuity, independent testing plans, and support ownership through the transition
- NFC chip reading, ISO/IEC 18013-5 mDL, and national eID schemes, are not supported today, which rules out chip-based assurance and limits fit for European high-assurance onboarding
- Authoritative attribute and personal database checks concentrate on US data sources through third-party aggregators, so buyers with verification volumes outside the US should validate data-source depth in their markets
- Microblink provides no hybrid verification with human adjudication, so regulated buyers that require documented manual review must build and staff that process themselves on top of the platform's routing and evidence views
- Device intelligence is limited to IP address, geolocation, and device type, without device fingerprinting, reputation, or behavioural analytics, so buyers seeking layered device risk signals will need a complementary fraud tool
- No prebuilt CIAM or IAM connectors, buyers embedding verification into IAM-driven onboarding, recovery, or step-up flows should plan for custom API and webhook integration

Mitek – Mitek Verified Identity Platform (MiVIP)



Leadership



Mitek Systems, founded in 1986 and headquartered in San Diego, California, is a publicly traded software company (NASDAQ: MITK) with roots in check imaging and mobile deposit for banks. The Mitek Verified Identity Platform (MiVIP) is a full-service identity verification offering that combines document verification, face and voice biometrics, passive liveness detection, partner-delivered data checks, and configurable verification journeys. The platform builds on two acquisitions: ID R&D (2021) for in-house voice and face biometrics and liveness, and HooYu (2022) for journey configuration and KYC workflows. MiVIP serves consumer onboarding, KYC and AML-related identity checks, age verification, and re-verification, and the MiPass module reuses biometrics captured at onboarding for later step-up verification and account recovery. Licensing is per transaction, with per-user pricing for

the MiPass biometric authentication module. The customer base is concentrated in financial services across North America and EMEA, with particular depth in the UK and Spain, and several other identity verification vendors also OEM Mitek's liveness technology.

The service is delivered as vendor-managed, multi-tenant SaaS on AWS, with hosting in the US East and West regions, Canada, and the EU; the full platform is not available on-premises. The IDLive face and document liveness components can instead be deployed on-premises or in private cloud without public-cloud dependency, typically through system integrators. Mitek is ISO/IEC 27001 certified and holds a SOC 2 Type 2 attestation covering security, availability, processing integrity, and confidentiality, though not the privacy criterion, plus UK Cyber Essentials.

Verification is based on optical document checks with OCR, MRZ, and barcode reading, NFC chip reading, and physical security feature analysis, with document models developed in-house and barcode scanning sourced from an OEM partner. Coverage includes passports from 265 ISO country codes, national identity cards from 176 countries, driver's licenses from 62 countries, and residence permits, visas, and other government-issued documents. Capture runs in the browser with real-time guidance and no app installation; NFC reading requires a customer app embedding Mitek SDK. Extracted attributes, name, date of birth, address, phone number, and national identifiers, can be checked against nine source-of-truth connections, including US AAMVA driver's license validation, the Dutch Basisregistratie Personen (BRP) population register and Rijksdienst voor het Wegverkeer (Dutch vehicle authority), and the UK Credit Industry Fraud Avoidance System (CIFAS) fraud database, plus aggregated identity data from about 45 countries through partners such as LSEG, Equifax, and Experian. Face verification compares the document portrait with a selfie in 1:1 mode, with 1:N search within a tenant; voice is a second modality, enrolled actively by repeating a statement three times. Passive liveness detection is native ID R&D technology, while biometric comparison incorporates partner technology. Templates are stored centrally by Mitek and scoped to a single tenant. The Spanish mobile national identity document (MiDNI) digital identity is accepted, but not ISO/IEC 18013-5 mDL.

Injection attack detection analyzes both content and transmission channel to flag virtual cameras, emulators, and SDK- or API-level injection; template attack detection identifies fraudulent document templates reused with varying personal data; and deepfake detection examines images, video, and audio for generation artifacts. Document-side checks cover tampering and compositing, AI-generated or AI-edited document images, synthetic documents, and inconsistencies between document and biometric evidence, with separate reason codes and confidence scores for suspected AI-assisted fraud. Face velocity rules search templates across the tenant for repeated attempts, and an internal face-block list flags known fraudsters. PEP, sanctions, denylist, and UBO screening and a UK-specific AML check are partner-delivered; device signals are limited to IP address, geolocation, device ID, and device type. Risk scores support configurable factor weighting, and policies can end a journey, trigger additional checks, or route to review, either in the customer's case management view, with evidence, match scores, and overrides recorded in an audit trail; or through Mitek's opt-in agent step-up service of trained forensic reviewers with a typical two-to-three-minute turnaround. Liveness has been tested under ISO/IEC 30107-3 PAD Levels 1 and 2 through iBeta and was one of two passive systems among 21 to detect all attacks in

the 2025 DHS S&T remote identity validation evaluation; while the face matcher participated in NIST FRTE 1:1 testing with a 2024 submission. Deepfake models are versioned and auditable with a formal update process and false-positive and false-negative reporting, although detection thresholds are not customer-configurable.

Privacy controls reflect a processor model: consent is obtained by Mitek's clients, passive liveness is disclosed to end-users, and MiPass template storage requires an explicit opt-in during the journey. Data is stored in AWS production and encryption keys held in the cloud provider's HSM-backed KMS. Retention is configurable per customer with automatic purging, though not per jurisdiction, and end-users can learn which attributes were collected and revoke access through the client. End-user data feeds model training only with client consent and is not sold or shared externally. Administrators authenticate through a built-in directory or a customer Identity Provider (IdP) over SAML or OIDC with role- and attribute-based access control; administrative activity logs sit on a separate network and cannot be deleted, but no customer-facing SIEM export exists.

Integration is exposed through REST APIs and webhooks using JSON and OAuth 2.0, with callbacks over webhook or SFTP whose payloads can include or exclude captured images. SDKs cover Android, iOS, and web JavaScript/TypeScript. A no-code/low-code hosted portal supports branded journey design, separate environments per business unit, and conditional rules across document types, biometric outputs, IP data, and third-party signals, so journeys adapt dynamically, for example requiring NFC or an additional voice step for higher-risk users. Advanced Attachment Processing applies OCR and configurable validation rules to arbitrary supporting documents such as proof of address or articles of incorporation, and the platform can re-engage users who abandoned verification. The API covers journey configuration and execution but not portal-only functions such as branding. Named integrations include Ping Identity, Mitek's primary IAM partner including account recovery flows, plus Experian, Equifax, Nice Actimize, and the FICO Marketplace.

Mitek is suited for fraud-exposed and regulated buyers, particularly banks, telecommunications providers, and marketplaces with age or high-risk checks, verifying users mainly across North America and Europe. SaaS-only delivery of the full platform with AWS hosting in the US, Canada, and the EU sets the architectural boundary: buyers requiring customer-managed processing can deploy only the IDLive liveness components on-premises. Buyers planning around mDL acceptance, requiring single-vendor ownership of biometric comparison, or operating large volumes in APAC or Latin America should validate current capability and support before committing.

Strengths

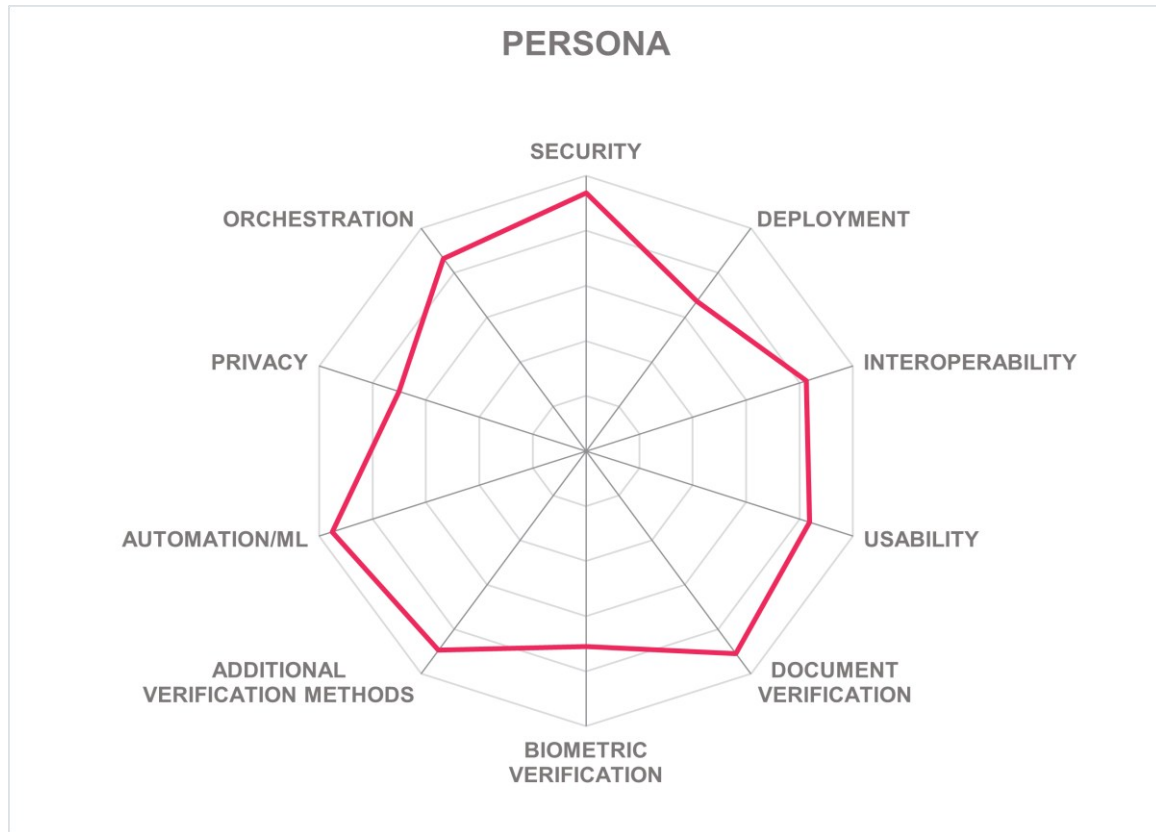
- Layered digital-fraud detection covering injections, template, and deepfake attacks with separate reason codes and confidence scores per fraud type can help fraud teams tune thresholds and investigate decisions instead of treating all failures alike
- Native passive liveness from the ID R&D acquisition is OEMed by other identity verification vendors, which supports both assurance documentation and model improvement at scale

- MiPass extends onboarding biometrics into cloud-based, device-independent face and voice re-authentication, giving buyers one vendor for verification, step-up, and account recovery scenarios, including through the Ping Identity integration
- Hybrid adjudication combines customer-side case management, business rules with operations-only caution flags, and an opt-in forensic agent review service with a typical two-to-three-minute turnaround, useful for regulated buyers that cannot fully automate borderline decisions
- The no-code/low-code journey builder applies conditional rules across document, biometric, device, and third-party data signals so verification friction scales with risk, and abandoned journeys can be re-engaged to protect conversion
- Advanced Attachment Processing automates extraction and validation from arbitrary supporting documents, closing a common manual-review gap in enhanced due diligence and right-to-work style flows

Challenges

- The full MiVIP platform is SaaS-only on AWS in the US, Canada, and the EU, which may not fit buyers with strict data-residency or customer-managed hosting requirements outside those regions; only liveness components are deployable on-premises
- Operational control gaps may matter at enterprise scale: console and administrative activity logs cannot be exported to a customer SIEM, and retention policies are configurable per customer but not per jurisdiction
- Deepfake detection thresholds are not customer-configurable
- ISO/IEC 18013-5 mDL is not supported yet but in the roadmap

Persona – Persona Identity Platform



Leadership



Persona was founded in 2018, is headquartered in San Francisco, and is venture-backed with a Series D round closed in 2025. The Persona Identity Platform is a full-service identity verification offering built from modular products that customers combine per use case: government ID document verification, facial biometric verification with liveness detection, verification against authoritative and commercial data sources, acceptance of eID schemes, mobile driver's licenses, and verifiable credentials, AML screening, workflow orchestration, and case management. Licensing combines per-verification pricing with monthly platform subscription fees. Evidenced use cases include consumer onboarding and KYC, age assurance, marketplace trust and safety, workforce identity verification integrated with IAM platforms, account recovery and re-verification, US public-sector identity proofing, and identity proofing for qualified electronic signatures delivered with the QTSP Infocert. The customer base is concentrated in North America, with a smaller EMEA presence.

The service is delivered as vendor-managed SaaS on GCP; no on-premises deployment is offered. Multi-tenant hosting is available in the US and in Germany, and dedicated single-tenant deployments are available in the US, Germany, Australia, Brazil, Canada, India, and Singapore, with customer-selectable colocation or separation of processing and storage for data-residency requirements. The service is ISO/IEC 27001 certified, holds a SOC 2 Type 2 attestation covering security, availability, confidentiality, and privacy, and reports PCI-DSS attestation and US Health Insurance Portability and Accountability Act (HIPAA) support. Persona achieved FedRAMP Moderate authorization in April 2026 through the FedRAMP 20x pilot and is a Kantara-approved credential service provider at NIST SP 800-63 IAL2, including use as an approved provider under the US Trusted Exchange Framework and Common Agreement (TEFCA), the US health data exchange framework.

Verification starts with document evidence covering 195 countries, including ePassports, national identity cards, driver's licenses, residence permits, and supplementary documents. Capture runs in the browser or through native SDKs on a user's own device, with OCR, MRZ parsing, PDF417 barcode reading, and NFC chip reading validated through passive and active authentication against issuing-country Signing Certificate Authority (CSCA) certificate chains; NFC requires an app context, delivered through an iOS App Clip or the Android app rather than a pure web session. Document verification is native technology, with document auto-capture licensed from Microblink for a limited set of countries and LLM-based extraction handling non-standard layouts. Extracted attributes can be corroborated against more than 400 authoritative and commercial sources across more than 75 countries, including issuing registries such as AAMVA in the US, SERPRO in Brazil, and the Australian Document Verification Service (DVS), with configurable fuzzy-matching thresholds per field. Persona also accepts national eID schemes, among them Swedish BankID, MitID, iDIN, itsme, France Identité, and ConnectID, partly through an OEM integration with eID Easy, verifies ISO/IEC 18013-5 mDLs from wallets, issues and verifies W3C Verifiable Credentials including through Microsoft Entra Verified ID, and offers silent network authentication across major US carriers using CAMARA-standard APIs. Biometric verification is face-only: 1:1 selfie-to-document-portrait comparison using an ensemble of in-house models and licensed algorithms from Paravision and IDRND, processed inside Persona's infrastructure, plus 1:N search for duplicate and velocity checks. Active liveness uses randomized multi-gesture challenges; passive liveness analyzes facial texture, depth inference, optical flow, and blink distribution, and passed iBeta ISO/IEC 30107-3 PAD Level 1 and Level 2 testing on iOS and Android. ML-based facial age estimation supports age assurance without a document.

Fraud controls are layered across evidence, device, and population signals. Document checks cover tamper and compositing detection, image metadata analysis, electronic replica detection, and cross-checks between visual, barcode, MRZ, and chip data; AI-generated documents are targeted with classifiers for known generative model families, and clustering of visually linked submissions. On the biometric side, dedicated models detect deepfakes, face swaps, AI-generated faces, and replays, while injection attacks are addressed through virtual camera and emulator detection, JavaScript integrity checks, and a signed proof-of-capture with a pixel-level hash on every photo, supported by Apple App Attestation and Google Play Integrity. Device intelligence covers IP reputation, geolocation and geo-velocity, device fingerprinting, and jailbreak and root checks, and behavioral biometrics such as keystroke, mouse, swipe, and gyroscope analysis feed a bot score with population-level p-

values. Each attack type surfaces separate reason codes and uses confidence scores with independent threshold, with configurable policies by geography, manual override under an immutable audit trail, and versioned deepfake-detection models. An opt-in cross-customer graph links faces, devices, and attributes to expose fraud rings, and sanctions, PEP, and adverse media screening with ongoing monitoring rounds out the AML layer.

Privacy controls include explicit, immutably logged consent before biometric processing and data aggregation, with Persona acting as processor in standard deployments and as controller for its wallet product. Retention is configurable per field and per jurisdiction, with a three-year default for biometric data, permanent redaction via dashboard or API, a zero-retention mode, and no storage of data from US users under 13. Data is encrypted with keys in Google Cloud KMS backed by HSMs, field-level tokenization, and role-based masking of sensitive fields. Customer data is not used for model training without consent.

Integration is exposed through REST APIs with JSON, webhooks, a CLI, and SDKs for JavaScript frameworks, iOS, Android, and React Native. A no-code workflow engine provides conditional branching, step-up routing, waiting steps for external callbacks, HTTP calls to third-party services, and simulation against historical data before publishing, and configuration can also be managed as code in git. The Cases product supplies manual-review queues, assignment policies, and audit logs, while analytics include funnel diagrams, check-level reporting, and direct SQL queries over tenant-isolated data. Verification results, reason codes, and signals hand off to IAM platforms including Okta, Microsoft Entra, Cisco Duo, and OneLogin, with SCIM write-back and post-verification OIDC token issuance, and identity events export to Splunk, Datadog, and Elastic Security.

Persona is suited for organizations that need configurable, high-volume verification across consumer onboarding, age assurance, marketplaces, workforce, and US public-sector scenarios, and that want orchestration and fraud tooling operated by their own teams. SaaS-only delivery bounds fit for buyers requiring customer-managed hosting, and manual review is tooling rather than a vendor-operated service. US assurance is anchored in FedRAMP and Kantara IAL2 certification; and EU assurance in ETSI TS 119 461 and ETSI EN 319 401 certification.

Strengths

- Workflow orchestration is unusually deep: a no-code engine with real-time conditional branching, reusable modules, simulation, and configuration-as-code in git can help operations teams run many verification programs and policy variants without vendor involvement or redeployment
- Separable fraud signals, distinct reason codes, and independent confidence scores let fraud teams tune responses per threat instead of treating all failures alike, supported by capture-provenance signing and device attestation
- A US-centric assurance portfolio of FedRAMP Moderate authorization, Kantara-approved IAL2 proofing usable under TEFCA, iBeta ISO/IEC 30107-3 PAD Level 1 and 2 test results, SOC 2 Type 2, and ISO/IEC 27001 reduce procurement friction for US government, healthcare, and regulated buyers
- Breadth of corroborating checks, more than 400 data sources across more than 75 countries including issuing registries, eID scheme acceptance, mDL and verifiable

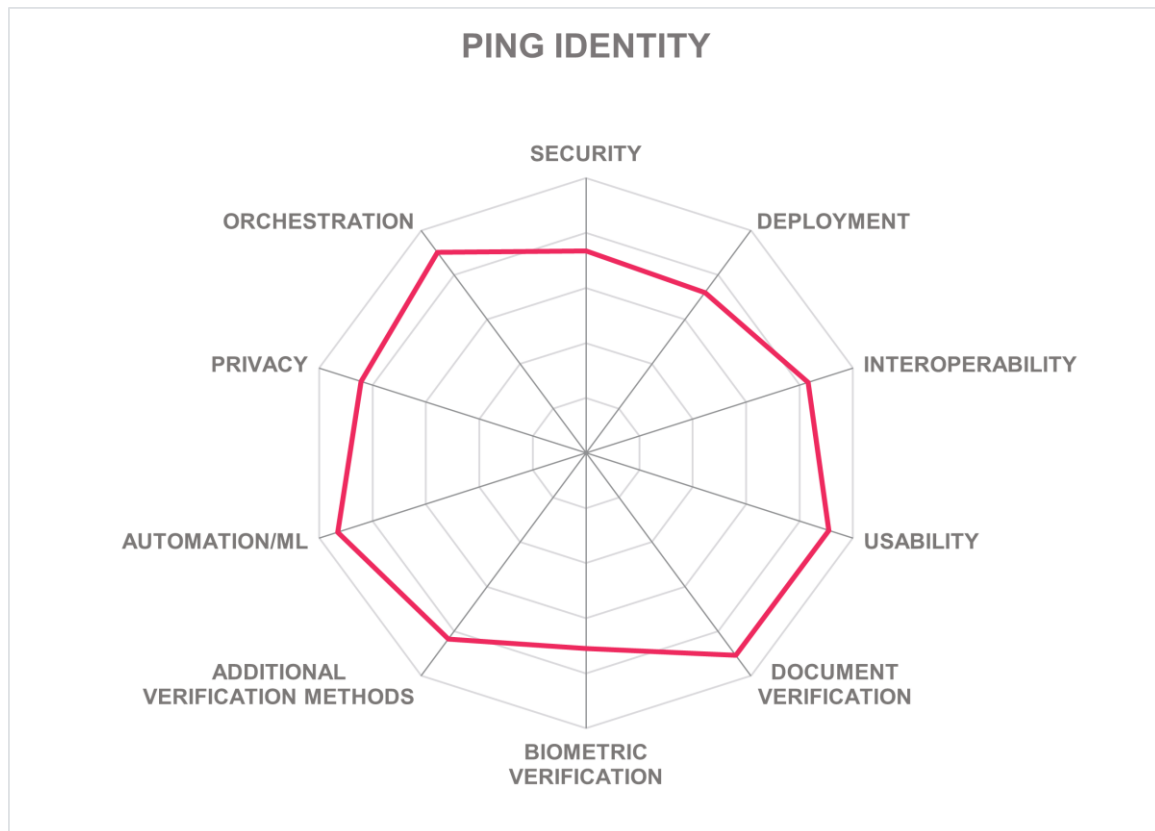
credential support, and CAMARA silent network authentication across US carriers reduces dependence on optical document capture alone

- Privacy tooling is granular: per-field and per-jurisdiction retention, permanent redaction via API, zero-retention modes, and consent logging can help buyers align one deployment with GDPR, CCPA, and US biometric statutes such as BIPA
- Single-tenant deployments in seven regions with isolated scaling and surge-queueing infrastructure suit buyers with data-residency needs or launch-driven traffic spikes

Challenges

- The platform is SaaS-only on GCP; buyers requiring on-premises processing, customer-managed hosting, or sovereign-cloud designations such as SecNumCloud or C5 will not find them here and must rely on regional single-tenant deployments
- Face matching depends partly on licensed algorithms from Paravision and IDRND, and NIST FRTE participation is through the licensed Paravision algorithm rather than a Persona submission
- Persona does not operate a manual-review service; customers need their own review teams or third parties, with vendor-arranged review limited to QTSP-run adjudication in Qualified Electronic Signature (QES) flows

Ping Identity – PingOne Verify and PingOne Recognize



Leadership



Ping Identity, founded in 2002 and headquartered in Denver, Colorado, is privately held under private-equity ownership. PingOne Verify and Ping One Recognize are services embedded in the Ping Identity Platform that can also be used alongside third-party identity environments: PingOne Verify provides document, biometric, verifiable credentials and data-based verification; PingOne Recognize, based on the Keyless technology acquired in a transaction announced in October 2025, adds privacy-preserving biometric re-verification; PingOne Credentials covers verifiable credentials; PingOne Protect contributes device and behavioral risk signals; and the DaVinci engine provides orchestration. Ping frames these components as a verified trust model: a single proofing event at onboarding is bound to a reusable authenticator, a zero-knowledge biometric enrollment, or a wallet-held verifiable credential; so later interactions re-verify against that origin event instead of repeating document checks. Use cases include consumer onboarding with progressive verification,

workforce and contractor hiring, account recovery, step-up verification, high-risk transaction approval, and age verification. The verification services do not require Ping's own IAM products and can be used alongside third-party identity providers. Ping Identity targets consumer and workforce customers in North America, with EMEA the second region. Licensing is per user or per transaction.

The verification and fraud services are delivered as vendor-managed, multi-tenant SaaS hosted on AWS, with data center locations in the US, Canada, Brazil, Ireland, Germany, Australia, and Singapore. Single-tenant or customer-hosted deployment is not offered for the verification services. The service is certified against ISO/IEC 27001, with a certificate scope that also covers ISO/IEC 27017 and 27018.

Physical document verification is OEM-delivered: capture SDKs and two document verification suppliers operate behind Ping's own API and policy layer and cover 214 passports, 209 national identity cards, 230 driver's licenses, visas, and residence permits, with image and video capture, automatic document type detection, and physical security feature checks. NFC chip reading is not yet available. Face verification is a 1:1 comparison of a selfie against the document portrait with passive, single-frame liveness detection; this component is also OEM-supplied, and the underlying technology has been tested at ISO/IEC 30107-3 PAD Levels 1 and 2 by iBeta, with the confirmation letters issued to the supplier rather than to Ping. Native capability is concentrated on digital identity: the platform verifies mDLs and digital passports presented from Apple and Google device wallets through the Digital Credentials API and OpenID for Verifiable Presentations (OID4VP) in SD-JWT and mDoc formats, demonstrated against the EU Digital Identity Wallet reference implementation, and it issues and verifies its own verifiable credentials. Data-based verification covers credit bureau, telecom, and bank sources through integrated data partners, AAMVA driver-record checks in the US, SSN-based synthetic identity checks, and email, phone possession, and device ownership checks. Failed document checks can be routed to a human reviewer who inspects the captured document and selfie images.

Fraud controls on the document side cover tamper and compositing detection, template-based and synthetic document detection, and detection of AI-generated or AI-edited document images. On the selfie side, a server-side deep neural network performs passive liveness detection, and the platform detects deepfake images and video, 3D masks, face swaps, replay attacks, virtual cameras, emulators, and SDK- or API-level injection, with capture provenance and session integrity checks; injection detection for the document capture channel is not supported. The PingOne Recognize matcher participates in NIST FRTE 1:1 verification under the Keyless name, with a November 2024 submission that placed in the top 50 of the mugshot category at its January 2025 debut, and its injection attack detection was the first certified at the high level against CEN/TS 18099, tested by CLR Labs. Verification outcomes return risk and confidence scores with reason codes that separate suspected AI-assisted fraud, backed by versioned, auditable detection models with a formal update process. PingOne Protect adds IP reputation, geolocation and geo-velocity, device fingerprinting, jailbreak and root detection, bot detection, and user-behavior risk models. These signals can be used alongside PingOne Verify's identity verification capabilities in orchestrated journeys. Sanctions, watchlist, and adverse media screening are

available through the integrated data providers with coverage varying by country; PEP, UBO, denylist, and LEI screening and AML-specific tooling are not provided.

PII and biometric images captured during verification are retained for a maximum of 30 minutes and then purged, with an API to delete them sooner, and retention policies are configurable per customer and per jurisdiction. PingOne Recognize avoids central biometric storage: the facial image is transformed on the device and matched through secure multi-party computation, so neither selfies nor reversible templates are stored, and a secondary key held in the device's secure element adds a possession factor to each face authentication. Mobile SDKs use the Secure Enclave or TEE where available. Consent collection with versioned terms and privacy notices is configurable. Customer images are used for model training only on an opt-in basis, and data passed to verification sub-processors is contractually restricted to processing purposes.

Integration runs through a REST API that streams status events and exposes results and scoring metadata through separate endpoints; webhooks forward audit events to Splunk, New Relic, or generic JSON listeners. Verification behavior is defined in policies in the PingOne admin console, and DaVinci provides low-code and no-code orchestration with importable flow templates and a marketplace of pre-built integrations. The current limitation is that a single verify policy cannot restrict which document combinations are accepted, so multi-document logic requires routing between policies in orchestration. SDKs are available for Android, iOS, JavaScript, Java, .NET, and Flutter, and the hosted capture interface is brandable and multilingual. Verification results can be issued as OIDC for Identity Assurance claims, an early-stage capability, and a demonstrated account recovery flow for a Microsoft Entra ID tenant returned the verified outcome to the third-party IAM system.

Ping Identity is suited for enterprises that want identity verification embedded in wider identity journeys, workforce hiring and helpdesk-driven account recovery under social-engineering pressure, or consumer onboarding with progressive assurance, and particularly for buyers that want re-verification without retaining biometric data. Buyers should note the architectural boundaries: verification services are multi-tenant SaaS only, physical document verification and the associated selfie matching are partner-delivered, NFC reading is not yet available. Buyers should validate the current attestation scope for the verification services, including SOC 2 Type 2 coverage, and the country-level source-of-truth coverage for their target markets.

Strengths

- Zero-knowledge biometric re-verification is native and independently validated: the matcher is listed in NIST FRTE 1:1 under the Keyless name, and its injection attack detection was the first certified at CEN/TS 18099 high level
- The verified-trust binding model turns one proofing event into a reusable authenticator, either a zero-knowledge biometric or a verifiable credential, reducing repeated document verification for workforce access recovery and returning consumers
- Digital ID coverage is ahead of much of the market: mDL verification from device wallets via the Digital Credentials API, and OID4VP demonstrated against the EUDI

wallet reference implementation, useful for buyers preparing for wallet-based verification

- Orchestration depth differentiates the offering. DaVinci low-code flows, marketplace templates, and policy routing combine document, digital ID, data, and risk checks in one journey
- The verification services also work standalone with third-party identity providers such as Microsoft Entra ID
- Short default data retention combined with per-jurisdiction retention policies and opt-in-only model training simplifies privacy assessments for verification workloads
- Separate risk scores and reason codes for suspected AI-assisted fraud, exposed through APIs, webhooks, and dashboards, help fraud teams tune thresholds instead of treating all failed verifications as the same event

Challenges

- Injection detection for the document capture channel is not yet supported
- All physical document verification, and the selfie matching and liveness used with it, are OEM-delivered, and the independent PAD test letters are issued to the supplier
- NFC chip reading is not available; buyers that need cryptographic chip validation of passports or national IDs, or High/IAL3 assurance, cannot achieve it with this solution today
- Verification services are offered only as multi-tenant SaaS on some AWS regions; the absence of customer-managed, single-tenant, or on-premises options may matter for strict data-residency or sovereignty requirements
- KYC screening is limited: sanctions, watchlist, and adverse media checks come through data partners with uneven country coverage, and PEP, UBO, denylist, LEI, and AML-specific tooling are absent

PXL Vision – PXL Ident



PXL Vision AG, privately held, founded in 2017, and headquartered in Zurich, Switzerland, provides remote identity verification and electronic signing. Its core offering, PXL Ident, is a SaaS identity verification platform covering document verification, facial comparison, passive liveness detection, and age verification; the same platform anchors PXL Vision's signing flows from simple through qualified electronic signatures. Licensing is subscription-based per transaction, with per-user pricing for the manual-review application and annual service plans. PXL Pro packages the technology as mobile and server SDKs for on-premises and hybrid use. It builds its document and face technology in-house and positions the offering as full-service identity verification. The solution serves consumer and workforce scenarios, including B2B2C age verification. Its customer base is concentrated in Switzerland and the wider DACH region, with telecommunications as the largest vertical, and it is expanding into financial services and e-government.

The service is delivered as vendor-managed, multi-tenant SaaS hosted with Exoscale, a Swiss private cloud provider, in data centers in Zurich and Geneva. Nearly the entire installed base runs on the SaaS platform, with a small share of on-premises installations through PXL Pro and an optional managed service for manual review. PXL Vision is certified against ETSI TS 119462 for eIDAS/ZertES by KPMG, ISO/IEC 27001:2022 by TÜV Rheinland and holds an ISAE 3402 Type 2 attestation from KPMG.

Document verification is native and combines image and video capture, OCR and MRZ extraction, comparison against document templates, and physical security feature checks, with coverage of documents from about 165 countries, including biometric passports from 105 countries, physical national identity cards from 118, driver's licenses from 124, residence permits, and European health insurance cards. NFC chip reading with validation against country signing certificates is delivered through a partner component and launched as an Android instant app or iOS App Clip inside the web flow, so users verify chipped documents without an app store download. Mobile driver's licenses according to ISO/IEC 18013-5 and national eID schemes are not supported. The product does not connect to government issuing databases; address verification is performed against the Swiss postal registry, with utility bill upload and manual review as a fallback. Biometric verification is native: two-dimensional face capture from a short selfie video, 1:1 comparison against the document portrait, and patented passive liveness detection that requires no user challenges, with 1:N search used only for fraud analysis. Verification runs fully automated or in hybrid mode with adjudication through a 24/7 agent review service operated under PXL Vision's certification for regulated flows or by the customer's own team using the platform review tool.

A deepfake detector developed in an Innosuisse-funded collaboration with the Idiap Research Institute has been generally available in PXL Ident since the beginning of 2026; it classifies face swaps, face reenactment, and fully synthetic faces. The detector is retrained against newly released generator models on a cadence of weeks or days and provides its assessment as a separate output without changing the capture journey. PXL Vision maintains versioned, auditable detection models, a formal update process, and reporting of false positives and false negatives for deepfake decisions. Document fraud controls cover tamper and compositing detection. Screen replay, virtual camera, and emulator-based capture detection are supported, alongside device signals such as IP address, device type, and jailbreak or root checks. However, injection attack detection at the SDK or API level and capture provenance verification are not evidenced as current capabilities. A fraud protection network that shares confirmed fraudster face data with participating customers is being rolled out initially to telecommunications customers. Each check provides its own result and reason codes rather than a single global risk score; policies and thresholds are configured per customer inside the platform, and manual overrides are recorded with an audit trail. KYC screenings such as PEP and sanctions checks are not part of the product but are available through partners.

Personal and biometric data are stored encrypted in the Swiss data centers, with retention policies configurable per customer and per jurisdiction. Users are informed and explicit consent is collected before verification, with responsibilities divided between PXL Vision and its customers according to controller and processor roles. End-users can see which attributes were collected, revoke a customer's access to their verified identity, and access a

record of which organizations used it. End-user data is only used for model training with customer approval and, when necessary, user consent. This data is not shared with external organizations.

Integration is exposed through REST APIs and webhooks, with SDKs for Android, iOS, Java, and C/C++ and a developer portal. Verification journeys are composed of modular steps into white-label flows. Configuration is applied by PXL Vision through an internal configuration API that is not yet exposed to customers; there is no self-service flow builder. Outcomes are provided as per-check results, reason codes, extracted document and chip data, and audit evidence, and can feed electronic signing with QTSPs including Swisscom Trust Services. Enterprise integrations include SAP and Salesforce, while IAM integration is delivered through partners; administrative access supports SAML and OIDC federation, and logs can be forwarded via syslog with tamper protection.

PXL Vision is best suited for organizations in Switzerland and the DACH that need configurable onboarding and identity proofing at qualified-signature grade with Swiss data residency. Buyers should validate document performance and support delivery outside Europe, where PXL Vision may work through partners. Buyers that require government database checks, ISO/IEC 18013-5 mobile driver's license support, or orchestration tooling controlled by their own teams should weigh those boundaries against the depth of regulated Swiss and EU verification flows.

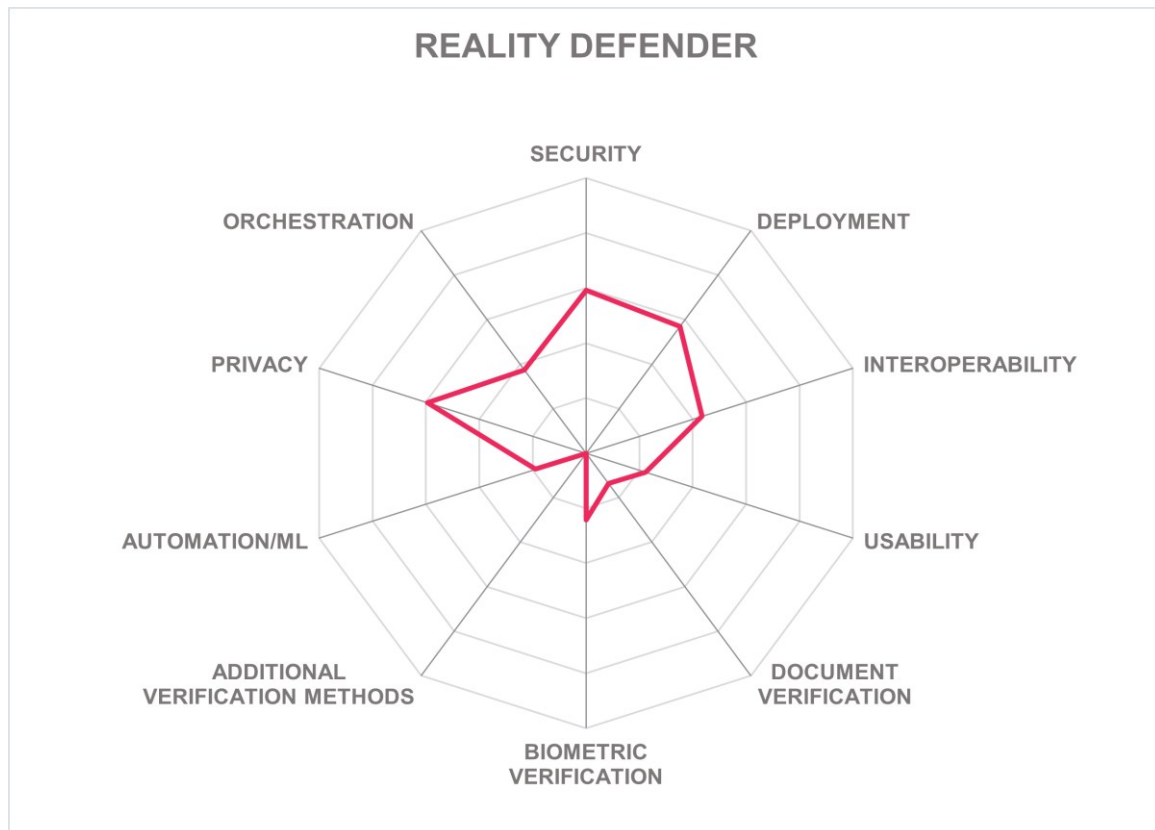
Strengths

- Automated verification and manual checks certified under both eIDAS and Swiss Federal Act on Electronic Signatures (ZertES) reduces procurement work for buyers running QES and other regulated onboarding in Switzerland and the EU
- Swiss data residency by design, vendor-managed SaaS on Exoscale data centers in Zurich and Geneva, combined with ISO/IEC 27001:2022 certification and an ISAE 3402 Type 2 attestation fits buyers in the DACH region with strict data protection requirements
- Browser-first capture with NFC chip reading launched through an instant app or App Clip provides chip-level document assurance without an app store download, which supports conversion in consumer onboarding where app installation causes drop-off
- Deepfake face detection developed with the Idiap Research Institute is generally available as an integrated scoring layer with false positive and false negative reporting
- In-house document and face technology lets PXL Vision prioritize country-specific documents quickly, such as Swiss residence permits, which matters for buyers whose user populations present documents that globally oriented vendors support poorly
- Manual review is available both as a vendor-managed 24/7 agent service certified for regulated flows and as a tool for customer-run adjudication, giving buyers a choice between outsourced and in-house review operating models

Challenges

- The product has no connections to government issuing databases, which is a limitation for buyers that expect registry-level corroboration of identity documents when available
- Mobile driver's licenses according to ISO/IEC 18013-5 and national eID schemes are not supported
- Injection attack detection at the SDK or API level and capture provenance verification are not evidenced as current capabilities yet
- Customer base, hosting, support, and the system integrator network are concentrated in the DACH region; buyers with significant verification volumes elsewhere should validate document performance and support delivery through partners
- Independent biometric testing is limited: ISO/IEC 30107-3 presentation attack detection testing was in preparation for the second half of 2026, and the only NIST FRTE face matching submission dates from 2020
- Workflow configuration is defined inside the platform through a non-public configuration API

Reality Defender – Real Suite (RealScan, RealCall, RealMeeting, RealAPI)



Reality Defender, privately held, founded in 2021, and headquartered in New York, is a specialist vendor of a deepfake detection platform that analyzes audio, video, and images for AI generation or manipulation, in real time for calls and meetings and on demand through its API. The company states explicitly that it is not an identity verification provider: it does not verify documents, match biometrics, or establish identity assurance. Instead, it supplies a media authenticity signal that identity verification, KYC, contact center, video conferencing, and brand-protection platforms embed in their own workflows. The portfolio comprises RealScan, a web application for analyst-driven review of uploaded files; RealCall, real-time voice analysis for contact center and telephony flows; RealMeeting, plugins for Zoom and Microsoft Teams that flag impersonation during live sessions; and RealAPI, the developer interface through which most detection volume is consumed. Within identity verification, the relevant use case is onboarding and KYC augmentation, where partner platforms such as 1Kosmos and Proof send captured imagery, video, or audio to Reality Defender and receive an authenticity score in return. Licensing is per transaction, per time period, or fixed, with volume-based enterprise agreements. The customer base is weighed up toward enterprise

and mid-market organizations in financial services, technology, telecommunication, media, and government, concentrated in North America and APAC with a smaller EMEA presence.

The service is delivered primarily as vendor-managed, multi-tenant SaaS hosted by AWS and Microsoft Azure, with single-tenant and dedicated environments available for enterprise customers. Selected government and enterprise deployments run as customer-managed software on-premises, in containerized form, or fully air-gapped. The company holds SOC 2 Type 1 and Type 2 covering the Security criterion.

The verification methods referred to in this report are outside the scope of the product. Reality Defender does not perform optical document verification, NFC chip reading, attribute or registry checks, biometric enrollment or comparison, or liveness detection. It does not create or store biometric templates, nor does it require any information about the person. What it does provide is native, multimodal analysis of submitted or streamed audio, video, and images for signs of AI generation or manipulation. Each modality is served by an ensemble of proprietary models, including full-frame vision models alongside face-focused ones, and vision models applied to audio spectrograms. Results are delivered in seconds as a probability-based score from 0 to 100 with a classification of Authentic, Suspicious, or Manipulated, scored per detected face and per audio segment. For identity document images, the boundary matters: the platform detects AI generation or manipulation of facial areas, including selfies and portrait photos, but does not detect tampering of non-facial fields such as names or document numbers, template-based synthetic documents, or fraud introduced through print-and-scan workflows.

Fraud controls address a single attack family: media generated or manipulated by AI. The models detect AI-generated and AI-manipulated selfie images and videos, face-swap attacks, virtual camera use, and synthetic or cloned voices, and RealCall additionally identifies autonomous agentic AI callers navigating interactive voice response and contact center flows. Image metadata is checked for provenance signals, including Coalition for Content Provenance and Authenticity (C2PA) data and traces of common generators. Explainability outputs include heat maps of pixel- and spectral-level anomalies and identification of the suspected generation technique. Equally relevant are the capabilities the platform does not provide, including SDK- or API-level injection detection, capture provenance or session integrity checks, replay or emulator detection, challenge-response prompts, and discrete reason codes. There are no customer-configurable thresholds, policies, or override audit trails; customers or partner platforms consume the score and apply their own routing, escalation, step-up, or review logic. The vendor maintains a red team that tests models against emerging generation tools, reports false positive and false negative rates for its detection, and operates a formal update process for new manipulation techniques. Based on the information provided, models do not appear to be versioned or auditable from a customer perspective.

Privacy handling benefits from the narrow data model. Because the platform analyzes media rather than identities, no biometric enrollment takes place, no templates are stored, and no personal identifiable information is required for detection. Media and event data are stored according to the deployment model and contract, with retention configurable per customer and per jurisdiction, and dedicated or customer-controlled environments available. Customer

data is not shared with external organizations, and any use of that data for model improvement is subject to customer agreement. Data encryption is managed through AWS KMS with customer-managed options for enterprise deployments, and administrative access supports SAML, OIDC, FIDO2 passkeys, and role-based access control with logged administrator activity.

The platform integrates through REST APIs and JSON-based webhooks and provides SDKs for Python, Java, TypeScript/JavaScript, Go, and Rust, all documented in a public developer portal. Mobile SDKs are not currently available. Detection events can be forwarded to SIEM tooling, with a Splunk integration available for meeting detection events. Prebuilt integrations cover contact center and telephony platforms including Amazon Connect, Genesys, Twilio, RingCentral, Illuma, Five9, Zoom and Microsoft Teams meeting plugins, and identity verification platforms such as 1Kosmos and Proof. The platform provides no built-in workflow templates, data mapping, or policy engine; orchestration is deliberately left to the surrounding customer or partner systems, and API integration requires engineering effort.

Reality Defender is well suited for enterprises and platform providers seeking an independent, specialized capability to detect AI-generated media within existing identity verification, contact center, or collaboration workflows, particularly where biometric enrollment is not appropriate or no trusted reference ("ground truth") is available. It is not a substitute for document verification, biometric matching, or liveness detection. It must be paired with an identity verification platform for onboarding use cases. Within this report, it should be understood as a specialized detection layer rather than a full-service provider.

Strengths

- Native, multimodal detection across audio, video, and images from a single API, with ensemble models per modality and results in seconds
- Extend deepfake detection from onboarding only to contact center, and meeting-security workflows with the same platform
- The no-enrollment design, no biometric templates, no PII requirement, no ground truth keeps the privacy footprint small and shortens integration, which suits buyers who want deepfake coverage without expanding their biometric data estate
- Deployment covers multi-tenant SaaS, single-tenant, on-premises, containerized, and air-gapped models, which supports government and data-sensitive buyers that most SaaS-only detection vendors cannot serve
- Continuous model maintenance through an in-house research team, red-team testing against emerging generators, and a biweekly update cadence addresses the fast turnover of generation techniques that static detection deployments struggle with

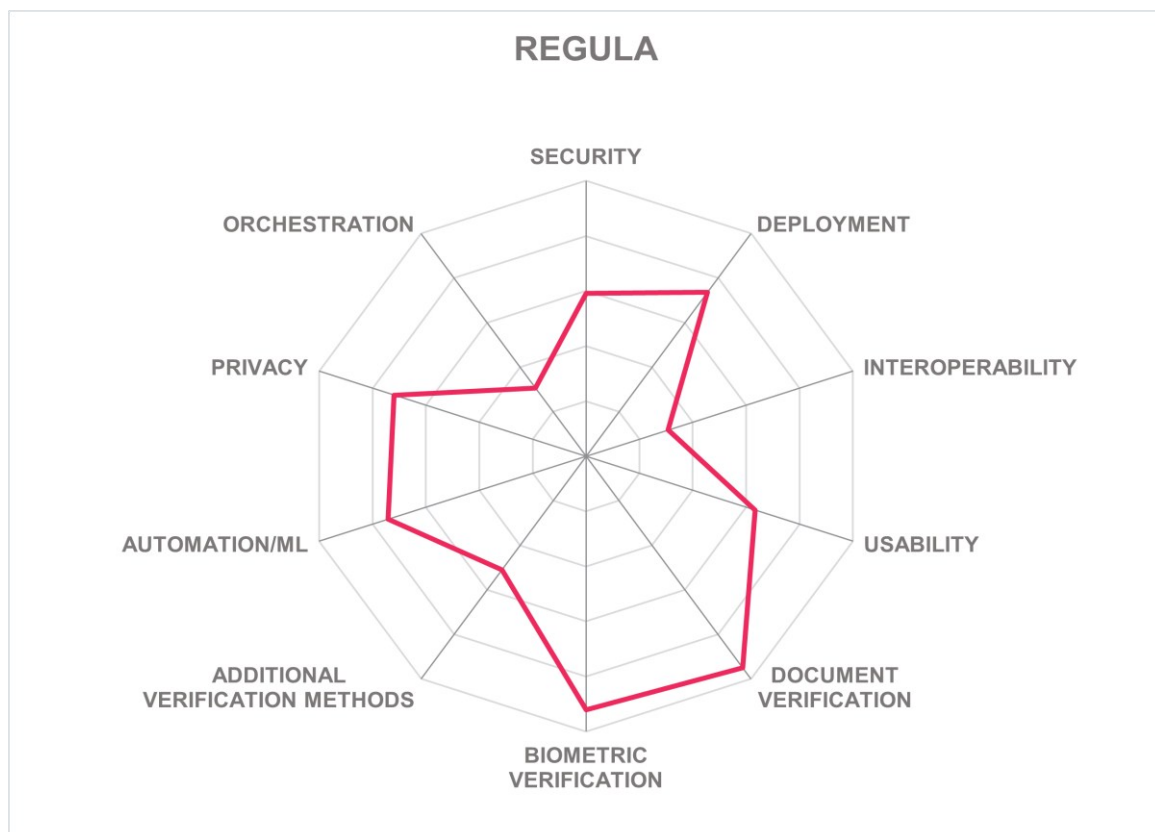
Challenges

- Reality Defender is not an identity verification provider: document verification, biometric comparison, liveness detection, and attribute checks are absent by design, so buyers in this report's core scope always need a separate IDV platform and cannot compare it like-for-like with full-service vendors

- Document fraud coverage is limited to facial regions of an image; tampering of textual fields, template-based synthetic documents, and print-and-scan fraud are out of scope, so the platform cannot replace document forensics in onboarding flows
- The absence of injection detection, capture provenance, and session integrity checks means manipulated media that bypasses the camera can only be judged on content artifacts, and buyers must pair the service with capture-side controls from their IDV or SDK vendor
- Decisioning depth is deliberately thin: no configurable thresholds, no discrete reason codes, no policy actions, no override audit trails, and models are not versioned and auditable

Regula – Regula IDV Platform, Document Reader SDK, Face SDK

Regula



Regula, founded in 1992 and headquartered in Daugavpils, Latvia, with offices in the US, Germany, Poland, the Netherlands, and Brazil, is a privately held, self-funded vendor with a background in forensic document examination equipment and cooperation with international bodies such as ICAO and Interpol. Its software portfolio consists of the Regula Document Reader SDK for identity document reading and authenticity checks, the Regula Face SDK for facial biometrics, and the Regula IDV Platform, introduced in 2025, which combines the document and biometric verification along with identity lifecycle management workflow orchestration, case management, and persistent user profiles into an end-to-end verification and identity lifecycle offering. All core technology is developed in-house, with no OEM or third-party components reported. Primary use cases include customer onboarding, KYC, re-verification, authentication, age assurance, and fraud prevention, with a customer base concentrated in EMEA and strongest in financial services, government, and travel. Licensing is a transaction-based subscription, with per-user-profile pricing available.

The products are delivered as customer-managed software. Deployments run on-premises or in customer-controlled private or public cloud environments, with AWS, Microsoft Azure, GCP, and Oracle Cloud supported as infrastructure options; no vendor-hosted SaaS or managed service is generally available. Regula does not receive, process, or store end-user data in any deployment model. Multi-tenancy is supported, allowing integrators to operate multi-client services on top of the platform. Regula is certified under ISO/IEC 27001 and SOC 2 Type 2 attestation is not currently held.

Verification is anchored in optical document verification against a proprietary template database of more than 16,000 document templates from 254 countries and territories. This database is continuously updated with new specimens. A submitted document is classified automatically without asking the user for type or country, read via OCR, and cross-checked for consistency across MRZ, visual zone, barcode, and NFC chip data, with physical and optical security features validated against the template. Regula does not connect to government issuing registries; the specimen-based template database serves as the source of truth, and chipped documents are additionally validated cryptographically through NFC passive authentication. Dynamic optical security features such as holograms and optically variable ink can be checked remotely on standard smartphones. ISO/IEC 18013-5 mobile driver's licenses are supported with server-side reprocessing of device-collected data., Identity data derived from ePassports can be reprocessed as digital travel credentials or verifiable credentials. Facial biometric verification is native and covers 1:1 matching and 1:N identification against customer-held databases, with active and passive liveness detection selectable per workflow. The Regula Face SDK passed iBeta presentation attack detection testing at ISO/IEC 30107-3 Levels 1 and 2, with confirmation letters issued in 2025 for both iOS and Android configurations, and Regula submits its face matching algorithms to the NIST FRTE evaluations. Facial images are used to estimate age and gender. This estimation is then compared against document data. This comparison also supports age assurance scenarios.

Fraud controls combine document and biometric mechanisms. ML models in the Automatic Authenticity Control function detect tampering, compositing, template-based generation, and AI-generated document images through forensic artefact analysis of compression, noise, and texture. Deepfake and injection attacks are addressed in three layers: SDK-controlled capture that blocks arbitrary photo upload and collects device metadata, encrypted transmission with certificate pinning, and backend neural network analysis of the received imagery, with virtual camera and emulator detection included. All session artefacts are retained on the backend so that suspicious verifications can be re-examined, and devices linked to fraudulent activity can be banned by device identifier. Device signals cover IP address, geolocation, device types, fingerprint, and customers can maintain reference lists, including facial watchlists for 1:N screening. The solution does not produce an aggregated risk score; it returns discrete, interpretable results and reason codes per check, which customers feed into their own decisioning, and manual review is supported with analyst-visible evidence and an audited override trail. PEP and sanctions screening is partner-delivered, with an out-of-the-box connector for LexisNexis Bridger Insight XG and support for Polixis.

Customer-managed architecture determines how privacy is handled. User consent is collected before verification through the client application. All identity and biometric data, which may include images and derived descriptors, remain in the customer's infrastructure. Retention policies are configurable per customer and per jurisdiction, storage encryption is implemented in the customer environment following Regula guidance. End-user data is not used for model training. End-user transparency and revocation controls are left to the implementing organization.

The platform supports integration through REST APIs, webhooks, and a CLI, with SDKs for Android, iOS, Java, .NET, C/C++, Flutter, and React Native, plus web components and Docker images, documented in a public developer portal. The Regula IDV Platform models work as workflows, sessions, and profiles, configured through a wizard and a components library with prebuilt templates, and extended through low-code Jinja expressions or Python scripting. Client-side capture screens can be reconfigured on the server and rendered by SDKs without republishing mobile applications. The back office provides manual review, session artefacts and recorded liveness video, user activity logging, and syslog output for SIEM integration, while administrative access supports SAML and OIDC federation with role-based access control. Verification results, extracted attributes, and reason codes are provided as JSON to downstream systems; a connector for Microsoft Entra ID is available, and other IAM integrations must be customer-built via the APIs.

Regula is suited for security-sensitive organizations that must keep identity and biometric data inside their own infrastructure and want document verification depth backed by a forensic lineage, as well as for integrators and KYC providers embedding verification technology into their own services. Buyers should plan for operating the stack themselves, for building decision logic on top of granular check results, and for sourcing authoritative-database checks from partners. The certification portfolio centers on ISO/IEC 27001 and PAD testing. The organizations integrating verification into wider IAM processes should validate connector availability beyond Microsoft Entra ID.

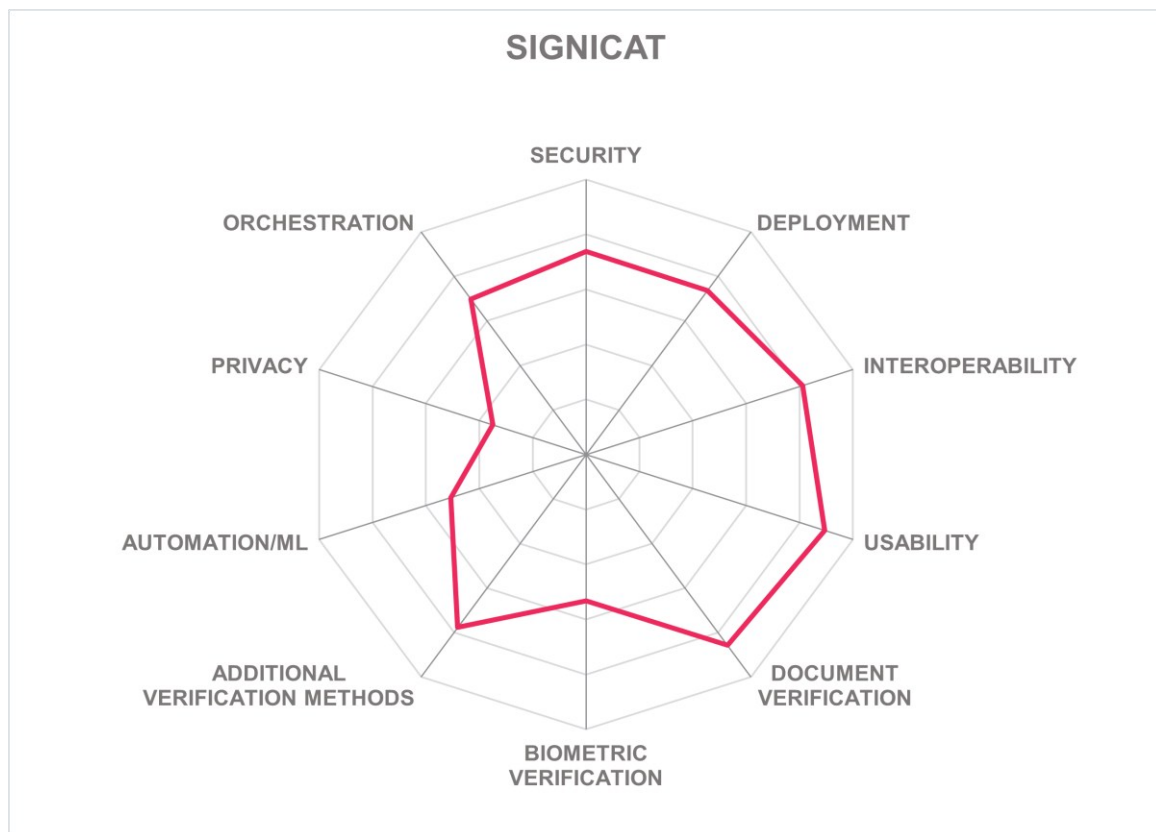
Strengths

- Fully in-house document and biometric technology with no OEM components and licensed by other identity verification providers indicates the depth of the underlying technology
- Document coverage of more than 16,000 templates built from verified specimens and continuously updated, reduces the need for fallback vendors for globally distributed user bases
- Three decades of forensic document expertise and cooperation with ICAO and Interpol
- Customer-managed deployment on-premises or in private cloud keeps all identity and biometric data inside the buyer's environment, which fits data-residency requirements and security-sensitive buyers in finance, government, and border management
- Layered injection and deepfake defense, combining SDK-controlled capture, certificate pinning, and backend neural analysis, with server-side retention of session artefacts that allows re-adjudication of suspicious verifications

Challenges

- No vendor-hosted SaaS or managed service is generally available
- The solution does not produce an aggregated risk score which means decision logic must be built and maintained in the customer's own risk systems
- The certification portfolio is limited to ISO/IEC 27001
- Evidenced IAM connectors are limited to Microsoft Entra ID, so embedding verification outcomes into broader IAM tooling is largely a customer-side integration effort

Signicat – VideoID, ReadID, eID and Wallet Hub, and Signicat Flow



Leadership



Signicat, founded in 2006 in Trondheim, Norway, and owned by the private equity firm Nordic Capital since 2019, provides a digital identity platform covering identity proofing, authentication, electronic signing, and orchestration. The company has grown through eight acquisitions, most recently the July 2025 purchase of Dutch NFC specialist Inverid and its ReadID product. The IDV offering is based on VideoID for optical document and facial biometric verification; ReadID for NFC chip reading, the eID and Wallet Hub for verification through national electronic identity methods and the future EU digital wallet; and Signicat

Flow, which combines orchestration with verification against external data sources. Licensing is per transaction combined with monthly or yearly subscription fees. Identity proofing is sold standalone or as part of the wider platform. Primary use cases are B2C and B2B onboarding under KYC and AML obligations, ongoing due diligence, account recovery, identity proofing for qualified electronic signatures, and police and border-control document inspection. The customer base is concentrated on EMEA, led by the Nordics and Benelux, with financial services being the largest industry segment.

The service is delivered as vendor-managed, multi-tenant SaaS; no on-premises or managed-service options are offered, and private-cloud deployments are rare exceptions. Hosting is on GCP, with AWS, Microsoft Azure for specific cases, with data centers in Europe and Australia. The service is certified against ISO/IEC 27001:2022 and ISO/IEC 27018, holds a SOC 2 Type 2 attestation and UK Cyber Essentials Plus, and operates qualified trust services in Norway, Spain, and Lithuania. VideoID is listed in the Spanish Centro Criptológico Nacional (CCN), Spanish National Cryptologic Centre, Catálogo de Productos y Servicios de Seguridad TIC (Spanish CCN security product catalog) (CPSTIC) catalog with ENS High certification. ISO/IEC 30107-3 presentation attack detection testing is evidenced only for partner-delivered biometrics.

Verification draws on multiple methods, used separately, or combined. VideoID captures documents by image or video and applies OCR extraction, physical security feature, hologram, black-and-white copy, photo tamper checks, presentation attack detection against paper and screen reproductions, and injection detection and deep-fake detection. Coverage includes over 180 issuing countries for ePassports and electronic national identity cards, over 195 countries and more than 6,000 document types for physical documents, and over 155 countries for driver's licenses. However, ISO/IEC 18013-5 mDL verification is not supported. ReadID reads and cryptographically validates the NFC chip of ICAO-compliant documents. Document verification is fully in-house developed; Signicat also resells third-party services (Onfido, iProov, Veriff) separately. Facial biometric verification performs 1:1 comparison with active liveness through guided user actions, and passive liveness analysis, natively through VideoID or optionally through partner technology (Innovatrics), in browser-based or app-based flows. The eID and Wallet Hub connect to 35 European eID schemes and can combine document evidence with eID authentication for holder verification. Attribute verification checks legal name, date of birth, address, phone number, identification numbers against more than 200 public and private sources, including population registers, lost-and-stolen document registers, and credit bureaus. Attribute verification can also check legal entity identities, ownership, and credit risk against business registers. Verification runs fully automated in 5 to 90 seconds, or hybrid with adjudication by Signicat agents, the customer, or a third party. eIDAS Low, Substantial, and High assurance levels can be achieved.

Fraud controls rely on natively developed ML models trained on vendor-built datasets, including internally generated deepfake material. Document checks detect AI-generated or AI-edited images, compositing and tampering, stolen identities, template-based or synthetic documents, and inconsistencies between identity documents and biometric data. The platform also generates a document risk score. Biometric checks detect spoofing, masks, AI-generated or manipulated selfie images and videos, face-swap, replay, virtual camera, and emulator attacks, and SDK- and API-level injection, and verify capture provenance and

session integrity. Deepfake-related decisions lack separate reason codes, risk scores, and configurable thresholds, and no independent testing against AI-generated attacks is evidenced. Risk decisioning in Signicat Flow produces a weighted risk score with customer-configurable thresholds and jurisdiction-specific policies; actions include accept, reject, step-up, manual review, additional-evidence requests, and restricted access. Reason codes and supporting evidence are provided through the API and a case management tool; manual overrides are audit-trailed, with separate reporting for document, biometric, deepfake, and synthetic-identity suspicion. KYC screening covers PEP, UBO, denylists, sanctions, and LEI, with AML, US Bank Secrecy Act, and PSD2 features and ongoing monitoring. Device intelligence covers IP reputation, geolocation and geo-velocity, device fingerprinting, health, reputation, IMEI/SIM, and jailbreak checks, plus login- and transaction-pattern analytics and cellular subscription data.

Signicat acts as data processor, leaving end-user notice to the customer; consent is collected before verification, and end-user data is used for model training only with additional permission. This data is not shared externally. Data is stored in a centralized vendor database. Retention is configurable per customer for document evidence but not per jurisdiction, with standardized event logs; end users can learn which attributes were collected but cannot revoke access or view an access record.

Integration is exposed through REST and SOAP APIs, webhooks, Android and iOS SDKs, and web redirect flows, with OIDC, SAML, or REST connections for the eID Hub and a public developer portal. Signicat Flow provides a no-code builder and low-code extension for front-end and back-end orchestration, workflow templates, and policy routing on signals such as device profile, user country, or screening hits, including fallback paths that accept optical evidence when NFC fails and flag the transaction as higher risk. A case management tool supports human-in-the-loop approvals with audit trails.

Signicat is suited for European organizations, particularly in financial services, insurance, and the public sector, which want to combine national eID reuse, document and NFC verification, data-source checks, and electronic signing under one contract and API. The platform is available only as a Europe-hosted SaaS offering, which may not meet the requirements of organizations seeking customer-managed deployments. Its market presence outside EMEA is also limited. Organizations relying on assurance documentation should verify the scope of ETSI TS 119 461 certification, the PAD coverage of the native biometric pipeline, and the availability of independent face-matching accuracy evidence, as no current NIST FRTE submission is held by the in-house solution. The partner solution, from Innovatrics, has a NIST FRTE public submission.

Strengths

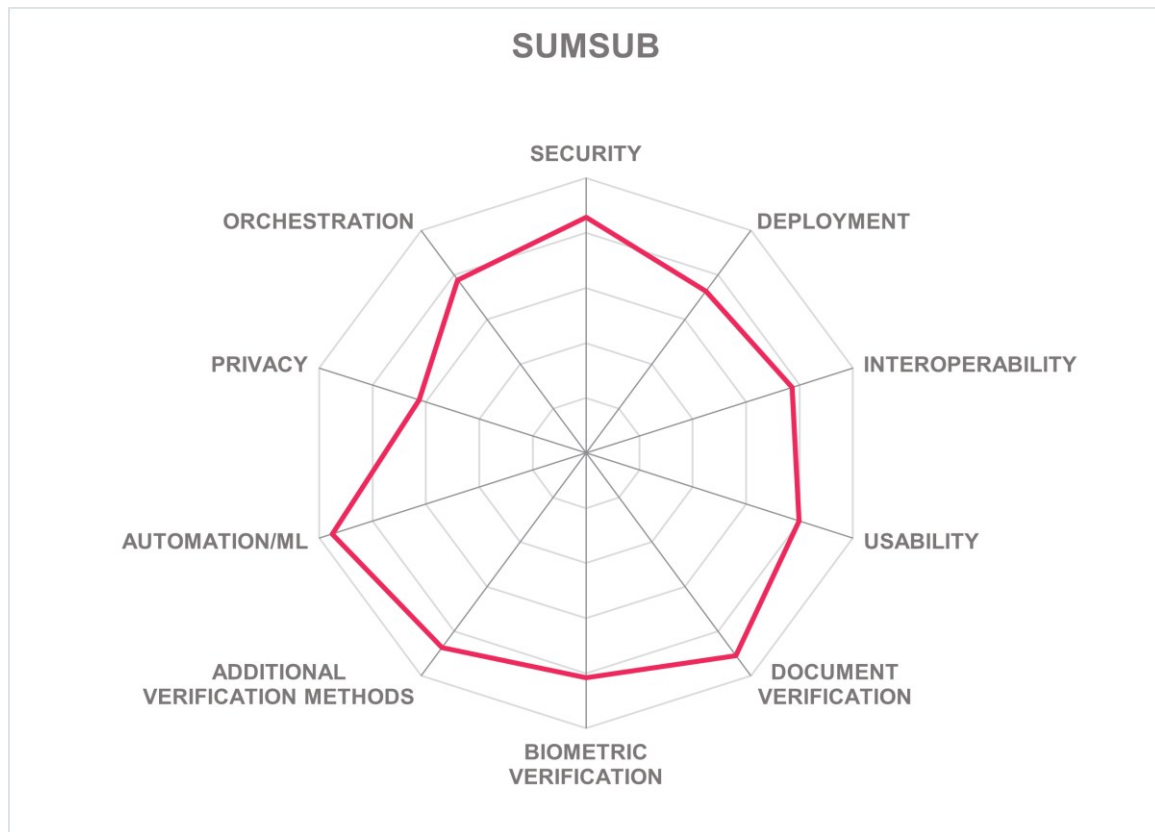
- Large natively owned verification methods, optical document verification, NFC chip reading with cryptographic validation, 35 national eID schemes, and 200+ data sources, under one API and contract, reducing multi-vendor integration effort for pan-European onboarding
- The eID and Wallet Hub positions buyers for the eIDAS 2.0 transition by sourcing identity data from established national eIDs and EU Digital Identity Wallets through the same integration, limiting rework as wallet adoption grows

- Extensive certifications ease procurement in regulated European environments, especially where verification must feed qualified electronic signatures
- Signicat Flow adds no-code and low-code orchestration with device- and risk-based routing, fallback flows, case management, and audit-trailed manual overrides, so verification journeys can be adapted without custom coding
- Flexible adjudication: manual review can be performed by Signicat agents, the customer's own team, or a resold third-party service, which helps buyers match review models to regulatory and cost constraints

Challenges

- SaaS-only delivery hosted in Europe, with private cloud handled as an exception, may limit fit for buyers that require customer-managed hosting, on-premises processing, or contractual regional hosting outside Europe
- Independent biometric assurance evidence is thin for the native pipeline: ISO/IEC 30107-3 PAD and NIST FRTE face-matching submission testing is evidenced only for partner-delivered biometrics
- No separate deepfake reason codes or risk scores, no deepfake-specific configurable thresholds, and no evidence of independent testing or false-positive/false-negative reporting for AI-generated attacks
- Customer and support presence is concentrated in EMEA, and mDL verification according to ISO/IEC 18013-5 is not supported, which matters for buyers with significant North American or mobile-credential-led verification volumes
- Privacy controls are processor-centric: retention is configurable only for selected data categories and not per jurisdiction, and end users cannot revoke access to verified attributes or view an access record

Sumsub – Sumsub User Verification Platform



Leadership



Sumsub is a privately held identity verification and compliance vendor founded in 2015 and headquartered in London. The Sumsub User Verification Platform combines document, and biometric verification with NFC chip reading, address and age verification, AML screening, device intelligence, workflow orchestration, case management, and reporting. Licensing is per successful verification with monthly or annual commitment models. The platform serves consumer and workforce user groups. The customer base is concentrated in financial services, including crypto exchanges, trading platforms, payment providers, and banks, with additional presence in gaming, marketplaces, and mobility, and the strongest regional footprint in EMEA and APAC. Use cases cover onboarding, step-up verification, account recovery, periodic and event-driven re-verification, age assurance, and fraud-led identity checks.

The service is delivered as vendor-managed, multi-tenant SaaS hosted on AWS, with single-tenant configurations available and customer data stored and processed by default in Frankfurt, Germany. A local data processing option keeps applicant data, images, and verification results in the US, UAE, or Singapore, while account and billing metadata remain central. On-premises and appliance deployments are not offered. The service is certified against ISO/IEC 27001, 27017, and 27018, ISO 22301, and ISO 9001, attested under SOC 2 Type 2 for security, availability, and confidentiality, and holds a PCI DSS v4.0.1 attestation. In June 2026, SRC Zert recertified the auto-identification, video identification, eID, and eMRTD modules against ETSI TS 119 461 V2.1.1 at a high level of confidence under eIDAS 2.0.

Document verification is native and covers more than 14,000 document types, from passports to residence permits, across more than 220 countries and territories. Capture supports automatic document classification and immediate quality feedback that rejects unusable submissions before processing. NFC chip reading covers eMRTDs and electronic identity cards in roughly 120 countries, and mobile driver's licenses are supported against ISO/IEC 18013-5. Extracted data can be validated against more than 100 authoritative and trusted sources, including government registries such as Brazil's Cadastro de Pessoas Físicas (Brazilian individual taxpayer registry) and India's Aadhaar via DigiLocker, banking identity networks such as the Finnish Trust Network, Norwegian BankID, and Dutch iDIN, credit bureaus, and telecom providers. Moreover, document-free verification against such sources is generally available in about 18 countries and is typically completed in four to five seconds, with workflow fallback to document capture. Video identification operates around the clock in English and German with vendor- or customer-operated agents, including a SEPBLAC-aligned recorded workflow for Spain, and German flows combining video identification, qualified electronic signatures, and penny-drop checks. Biometric verification is also native and limited to the face modality: 1:1 and 1:N comparison plus active and passive liveness with 3D face mapping, tested by iBeta under ISO/IEC 30107-3 at PAD Level 2. Templates are stored centrally on Sumsb side, encrypted, with regional residency options. Reusable KYC allows participating customers to share previously verified data with user consent. Sumsb ID is a server-side, email-bound account where end users can store their verified documents for reuse across Sumsb-powered services. The account has notifications and blocks unrecognized attempts. This reusable identity is a proprietary system rather than a wallet-held verifiable credential.

Fraud controls extend across evidence types. Document fraud detection includes pixel-level forgery and compositing analysis, template-based and synthetic document detection, and detection of AI-generated or AI-edited document images. Biometric attack detection covers printed photos, masks, replays, face swaps, AI-generated selfie images and videos, virtual cameras, emulators, and image or video injection at the SDK and API level, supported by camera integrity and capture provenance checks; a deepfake detector is retrained continuously using signals from document, device, and biometric checks. Device intelligence contributes to IP reputation, geolocation and geo-velocity, device fingerprinting, VPN, proxy, and Tor detection, jailbreak and root checks, shared devices, and multi-account detection. Behavior monitoring detects unusual interaction patterns and potential account takeover activity across relevant customer touchpoints. Configurable risk scoring with weighted factors drives automated approval or rejection, step-up verification, enhanced due diligence, manual

review routing, and transaction restrictions, with granular analyst-visible reason codes and separate codes, scores, and audit trails for suspected deepfake and AI-assisted fraud. AML screening covers PEPs, sanctions, watchlists, adverse media, and relatives and close associates, with ongoing monitoring and an LLM-based match summarization that helps analysts resolve false positives. The Summy AI Copilot summarizes cases, explains decisions, generates reports, creates visual graphs, and translates plain-language requirements into workflow configuration, and a Model Context Protocol (MCP) server lets customer-operated AI agents perform onboarding, configuration and daily operations tasks under role-based permissions with human approval steps. Sumsb is listed among the official connectors for Claude and ChatGPT.

Privacy controls include user consent collected before verification for biometric processing, database checks, screening, and device data collection. Data is encrypted with keys managed in AWS KMS backed by HSMs operated by AWS. Retention is configurable per customer and per jurisdiction, and end users can see which attributes were collected, request deletion, revoke access, and view which organizations hold their verified data. End-user data is also used for model training and may be shared with regulated data sources as part of checks, which buyers should reflect in their privacy notices; mobile SDKs use Secure Enclave on iOS and the TEE on Android for key storage.

Integration is exposed through REST APIs and webhooks. Authentication is handled with app tokens and signed requests, alongside a Web SDK and iOS and Android SDKs with Flutter, React Native, and Cordova plugins. The no-code Workflow Builder applies conditional logic to any verification, fraud, or device signal, including fallback flows, human-in-the-loop review steps, and periodic or event-driven re-verification. Case management provides configurable case views, automatic and manual assignment, and linked-verification graphs, backed by applicant event logs, an audit trail API, and a tamper-evident audit store. Prebuilt enterprise integrations are recent and still few: Auth0, Okta, Hubspot and Salesforce are generally available, alongside named integrations with Fireblocks, ComplyAdvantage, Chainalysis, Elliptic, OneID, Signicat, and Volt.

Sumsb is suited for regulated, fraud-exposed organizations that verify consumers across many jurisdictions and need to combine document, database, biometric, and video methods under one orchestration and case-management layer, particularly in financial services, crypto, trading, payments, gaming, and platform businesses. The ETSI TS 119 461 certification and iBeta PAD testing give EU-focused buyers documented assurance evidence, while buyers with NIST-aligned procurement requirements will find only alignment work in progress. Delivery is SaaS-only with vendor-managed regional processing, so organizations that require customer-managed hosting should validate the Local Data Processing scope against their obligations. This platform offers more than what buyers with a single market and a simple document check may need, and organizations expecting a broad prebuilt IAM connector catalog from day one should validate current coverage and timelines.

Strengths

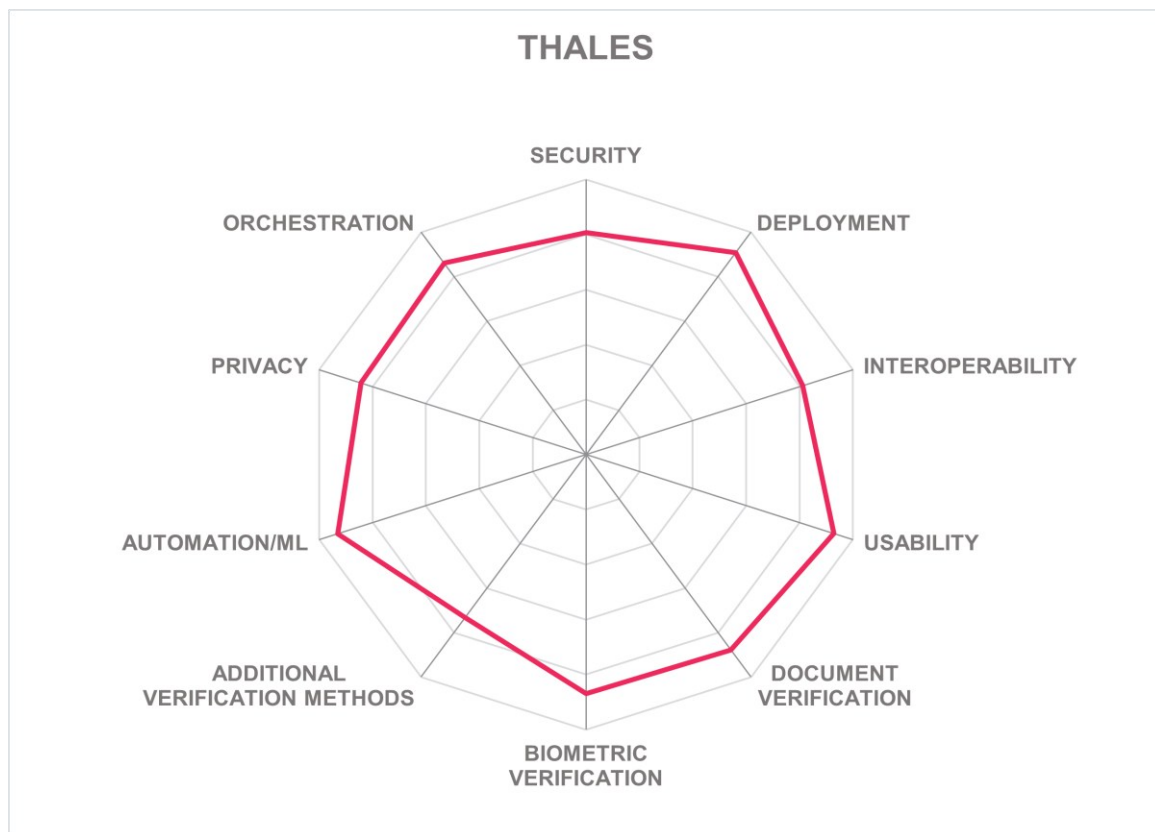
- Numerous orchestrated verification methods: document verification, attributes checks, video identification, QES workflows, and reusable identity, lets multi-jurisdiction buyers design a locally appropriate method within one workflow
- Certification against ETSI TS 119 461 V2.1.1 at a high level of confidence under eIDAS 2.0, combined with iBeta ISO/IEC 30107-3 PAD Level 1 and Level 2 test results, provides documented assurance evidence for EU regulated onboarding
- Document and country coverage of more than 14,000 document types across more than 195 countries and territories, with multi-script OCR and transliteration, reduces the need for fallback vendors for globally distributed user bases
- Granular no-code orchestration with human-in-the-loop steps, configurable case management, and analyst-visible reason codes supports large review teams that must explain and audit every decision
- AI-assisted operations through the Summy AI Copilot and an MCP server for customer-operated AI agents shorten configuration and investigation work while keeping role-based permissions and human approval in place

Challenges

- Delivery is SaaS-only with vendor-managed hosting; data residency is addressed through regional processing options rather than customer-managed or on-premises deployment, which may not satisfy strict sovereignty requirements
- The prebuilt enterprise and IAM connector catalog are limited today, with Auth0, Okta, Hubspot and Salesforce generally available and further connectors planned, so buyers embedding verification into established IAM estates should validate integration timelines
- Independent face-matching accuracy evidence is limited: no NIST FRTE result is available
- The SOC 2 Type 2 attestation covers security, availability, and confidentiality but not the privacy criteria, so buyers seeking independently attested privacy controls must rely on ISO/IEC 27018 and GDPR mechanisms instead
- Reusable identity is delivered as a proprietary, server-side account rather than standards-based verifiable credentials or wallet integration, which limits interoperability for buyers preparing for EUDI Wallet-style flows

Thales – Identity Verification Suite, OneWelcome Identity Platform

THALES



Leadership



Thales, a publicly listed French multinational founded in 1893, provides identity verification through its Cybersecurity & Digital Identity business, substantially expanded by the 2019 acquisition of Gemalto. The enterprise offering, the Identity Verification Suite for remote onboarding and KYC, is delivered within the OneWelcome Identity Platform, which surrounds verification with CIAM, user journey orchestration, consent management, and identity brokerage, alongside a government-focused civil identity suite and a Digital ID Wallet for issuing credentials to smartphones. Identity verification is modular and can be bought standalone or combined with the orchestration, consent, and brokerage modules. Primary use cases are consumer onboarding, account recovery, step-up verification through progressive profiling, and issuance of verifiable credentials from verification results. The

customer base is weighted toward large enterprises and public-sector organizations, strongest in EMEA, and predominantly B2C across banking, telecom, and government services. Licensing is available per user, per transaction, per time period, or at fixed cost depending on use case.

The product is delivered as on-premises software, a Thales-operated cloud service, or a managed service; private-sector customers mainly consume the cloud service, which runs on AWS with regional hubs in Europe, Asia, the US, the Middle East, and Latin America. Single- and multi-tenant operation is supported. The service is certified to ISO/IEC 27001 and holds a SOC 2 Type 2 attestation. Thales also majority-owns S3NS, a GCP joint venture qualified by French national cybersecurity agency (ANSSI) under SecNumCloud 3.2 in December 2025; buyers with French sovereignty requirements should validate when the identity platform becomes available there.

Verification is anchored in optical document verification against a database of more than 10,000 document templates from over 190 countries and more than 200 issuing authorities, from ePassports, national identity cards, and driver's licenses to ISO/IEC 18013-5 mobile driver's licenses, residence permits, and visas. About 80% of documents are verified in-house; regional partners cover the remainder. Capture uses image or video with SDK image-quality checks, and chipped documents can be read over NFC with ICAO passive authentication, including signer-certificate validation against the issuing country's revocation list. Registry checks are country-dependent, while eID-scheme verification, knowledge-based verification, and attribute checks against credit, telecom, and bank sources extend these methods. Biometric verification is native for face, with 1:1 and 1:N face matching. Passive liveness is the default; active liveness is available but discouraged due to measured user drop-off. Thales offers both a PAD Level 2-certified liveness option delivered through an OEM partnership and a native remote liveness algorithm, which is not currently PAD Level 2 certified, allowing customers to select the option as required. The face matching algorithm participates in the NIST FRTE 1:1 evaluation under the Gemalto Cogent name.

Document fraud controls cover photo and text substitution, digital tampering, copy and screen-presentation detection, and AI-generated forgeries including face swap, morphing, and synthetic or template-based documents, plus consistency checks between document and biometric evidence. Injection attack detection combines client-side SDK checks for virtual cameras, JavaScript modification, cloning apps, and rooted devices with server-side analysis; injection detection and dedicated deepfake and morphing detection models were added over the past twelve months. An identity affirmation risk layer adds device intelligence including IP reputation, geolocation, geo-velocity, device fingerprinting. It also adds jailbreak checks, individual- and population-level behavior analytics, and behavioral biometrics such as keystroke, mouse, and swipe analysis, as well as bot detection. A policy engine supports configurable thresholds and jurisdiction-specific fraud policies, returns document- and biometric-level risk scores with separate scores and reason codes for suspected AI-assisted fraud, and can trigger step-up actions such as re-authentication or document re-capture. Manual overrides are recorded in an audit trail. Reporting is separated by document, biometric, and synthetic identity suspicion. Deepfake detection models are versioned and covered by a formal update process. An optional module shares anonymized fraud patterns across customers without exchanging personal data. PEP, UBO, sanctions, denylist, and LEI

screening, as well as AML, PSD2, and US Bank Secrecy Act features, are pulled from third-party content providers.

Consent collection is a native platform service that can be triggered at any workflow step, it also covers liveness and data aggregation, and stores records for legally required periods. The platform usually does not store personal data, acting as a gateway to data sources; hosting, where required, is short-term or project-specific, with database encryption keys in AWS KMS backed by a cloud HSM, and a hold-your-own-key option. Retention is customizable per customer and per jurisdiction, and end users can review collected attributes, revoke access, and see sharing history through a self-care portal.

Orchestration is native: a low-code, drag-and-drop journey designer provides prebuilt flow templates, decision gateways, runtime API calls into customer or third-party services, and policy modeling, with coded extensions in Java, JavaScript, or Python. It also supports progressive profiling and identity brokerage combining document verification with eID-scheme or bank-based verification in a single journey. Functionality is exposed through REST APIs with JSON and XML payloads, authenticated via OAuth2, OIDC, SAML, JWT, or mutual TLS. However, webhooks are not supported. SDKs cover Android, iOS, Java, and web JavaScript, documented in a developer portal. Dashboards report success and failure rates with CSV export, alongside portals for customer fraud and support teams and end-users. Administrative access federates over SAML and OIDC with role-, attribute-, and policy-based controls, tamper-protected activity logs, and syslog output.

Thales is suited for large enterprises and public-sector organizations that want identity verification embedded in a broader identity platform with native orchestration, consent management, and brokerage, particularly where NFC-based high assurance, EU hosting, or French sovereignty options matter. Verification is fully automated: there is no vendor-operated adjudication service, and regulated video verification is delivered through partners. KYC and AML data checks are partner-delivered. ISO/IEC 27001 certification and the SOC 2 attestation are evidenced for the platform. Delivery is project-based, with rollouts of three to six months, which may exceed the appetite of smaller organizations.

Strengths

- Document coverage of more than 10,000 templates across over 190 countries, combined with Thales's role as a manufacturer of identity documents, gives its verification models access to original document templates
- Native low-code journey orchestration including consent management, progressive profiling, identity brokerage and combining document verification with eID-scheme or bank-based routes in one journey
- Layered defense against AI-assisted fraud: client-side and server-side injection detection, deepfake and morphing detection models, separate risk scores, and reason codes for suspected AI-assisted fraud
- Risk analysis depth beyond the verification transaction, including device intelligence, individual- and population-level behavior analytics, behavioral biometrics with bot detection, and optional anonymized cross-customer fraud-pattern sharing
- Deployment options from on-premises software and appliances to vendor-operated SaaS with regional hubs across five regions, plus a SecNumCloud-qualified

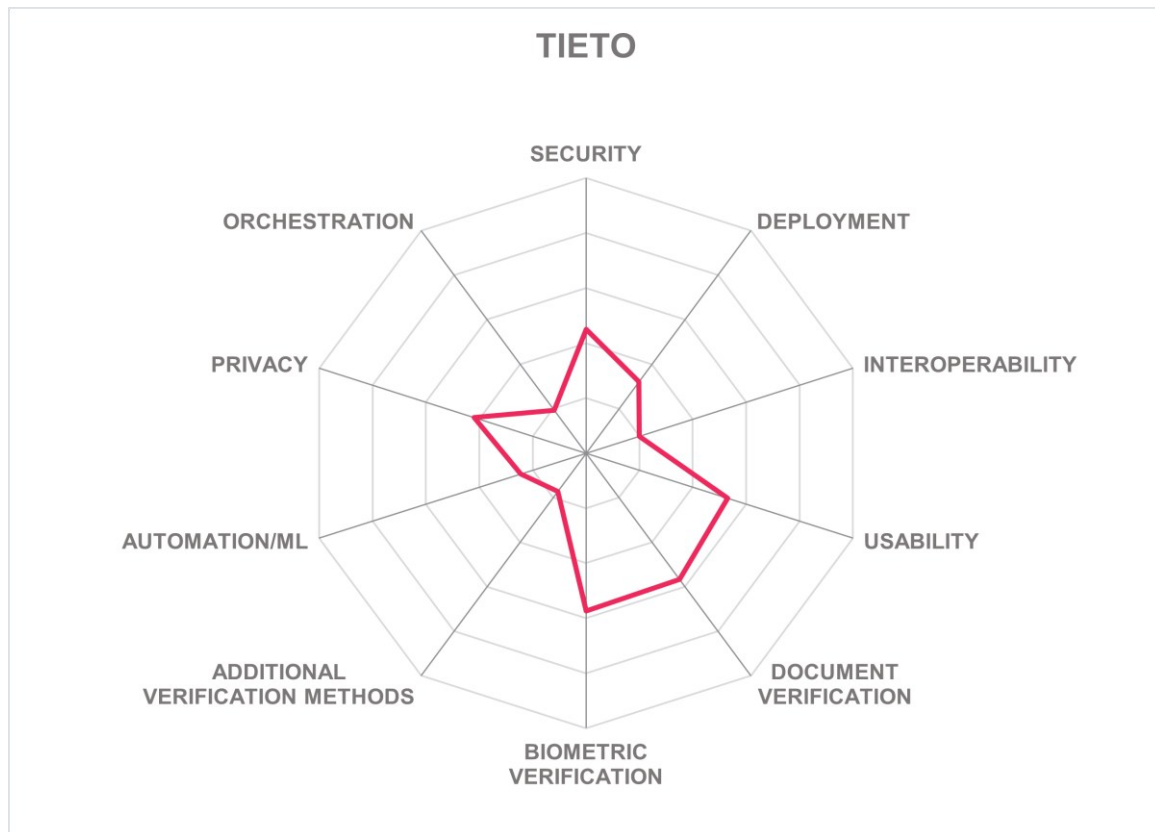
sovereign infrastructure affiliate in France, address data-residency, and sovereignty requirements that many competitors cannot cover

Challenges

- Verification is fully automated with no vendor-operated manual review or adjudication service, and regulated video verification is handled by partners; buyers subject to regulations requiring human-assisted verification, must source and govern it separately
- The latest NIST FRTE submission (as Gemalto Cogent) dates from January 2023, and the verifiable ISO/IEC 30107-3 PAD Level 2 test covers a hardware capture-device configuration, with certification of the remote liveness algorithm still in progress
- Reliance on partners for KYC and AML data checks and supplementary liveness and data-intelligence components in some regions means more than one party in testing, support escalation, and data handling for those parts of the flow
- Connections to authoritative sources of truth are country-dependent and not evidenced as a standard connector set
- The multi-brand portfolio and project-based delivery model add evaluation and implementation overhead, and integration is API- and SDK-centric so smaller organizations may find the engagement model heavier than specialist alternatives

Tieto – Identity Proofing

tieto



Tieto, the Finnish IT services group founded in 1968, headquartered in Espoo, listed on Nasdaq Helsinki, and renamed from Tietoevry in March 2026, serves the Nordic financial sector through its Tieto Banktech business, which supplies cards, payments, core banking, and financial crime prevention software to more than 400 financial institutions. Identity Proofing is Banktech's identity verification service, developed and operated by the Financial Crime Prevention unit in Norway that also houses the group's fraud prevention and AML offerings. The service establishes the identity of a natural person from the chip of a government-issued electronic identity document and binds it to the user through face matching and passive liveness detection. Licensing is per started transaction combined with a fixed monthly fee. Consumer use cases at Nordic banks include activation of mobile banking apps and device biometrics, refreshing, expired identification documents in KYC files, verification before electronic signing, caller verification for bank support centers, and account recovery on new devices. The installed base is small and concentrated in Norway, where mandatory in-person enrollment for national eIDs has kept remote verification volumes low.

Identity Proofing is delivered only as a vendor-operated managed service. The software runs containerized on Kubernetes hosted in a sovereign private cloud in Oslo and on AWS in Frankfurt; current customers are served from the sovereign Norwegian environment. All components are multi-tenant. The group holds ISO/IEC 9001, 14001, 27001 and 27701 certifications for its integrated management system.

Verification is based solely on NFC chip reading: the SDK reads the machine-readable zone and then the embedded chip of ICAO-compliant biometric passports and electronic national identity cards, validating the document signer certificate chain cryptographically. Passports from 59 issuing countries and electronic national identity cards from 13 countries are validated in production, and ICAO-compliant documents from all regions are supported. There is no optical verification of physical documents, and no support for mobile driver's licenses, verifiable credentials, or eID scheme verification. Three authoritative sources are connected: the German country signing certificate authority, the Norwegian National Population Registry, against which name, date of birth, and nationality are compared, and the Norwegian lost-and-stolen register for Norwegian passports and identity cards. Biometric binding uses a selfie captured on the user's personal phone through an Android or iOS SDK embedded in the bank's own app or in Tieto's authentication app; there is no browser flow. Face matching is a 1:1 comparison against the chip photograph. It is performed on the server together with passive liveness detection by software from Mobai. Mobai is a Norwegian biometrics vendor that acts as an OEM supplier. Its containers run entirely inside Tieto's environment, so no biometric data reaches the supplier. Verification is fully automated; a verified passport photograph can later be reused as a server-stored reference, so that a fresh selfie with presentation attack detection re-authenticates the user without repeating document capture.

Fraud controls concentrate on the capture channel and the biometric comparison since document authenticity rests on chip cryptography rather than optical inspection. The passive presentation attack detection covers printed photos, screen and video replays, and mask artefacts; Mobai's solution was tested in 2025 by the Swiss Center for Biometrics Research and Testing at the Idiap Research Institute, a FIDO-accredited laboratory, which attested a 0% attack presentation classification error rate and a 0.246% bona fide error rate against ISO/IEC 30107 Level A and Level B attack instruments. Detection of AI-generated or manipulated selfie images and video, face swaps, and morphing attacks has recently been added from the same supplier. Injection attacks, virtual cameras, and emulator-based capture are addressed through SDK-level capture provenance checks and application shielding from partner Promon, complemented by device identifier and device type signals, jailbreak and root detection, and device integrity attestation through platform services. Mobai's matching algorithms participate in the NIST FRTE 1:1 evaluation. Biometric verification provides a risk score, reason codes, and confidence scores for suspected deepfakes. Document checks, on the other hand, return discrete results without a risk score. There is no cross-factor risk engine: risk factors cannot be weighted, policies cannot trigger differentiated actions, and no PEP, sanctions, or other KYC screening is included.

Customers can require a manual approval step for specific processes. Currently, this mechanism is used when names on non-Norwegian passports are truncated and fail registry matching. In this case, bank or Tieto staff accept or decline the session in the administration

client. Rejections from face matching or liveness cannot be overridden, and review rules are configured by Tieto rather than by the customer.

Privacy controls begin with a consent module presented before capture, and users are informed of the passive liveness check. All processing happens on the server side, and nothing is stored on the device. Identity data, images, and biometric templates are stored encrypted with keys held in an HSM, and stored verification evidence is HSM-signed for use in the banks' KYC archives. Following guidance from the Norwegian data protection authority, photographs retained for re-authentication are converted into encrypted biometric templates rather than kept as reusable images. Retention is configurable per customer, though not per jurisdiction; end users can learn which attributes were collected and revoke the customer's access, and no end-user data is used for model training or shared externally.

Integration is exposed through REST APIs with JSON payloads, covering all capabilities, plus the Android and iOS SDKs and a developer portal. Outcomes are delivered as a fetchable status, a structured JSON result, or a signed PDF report. Built-in workflow templates cover the main flows, and extensions require coding in Java, Kotlin, or Swift. Webhooks and no low-code tooling are currently not supported. Prebuilt connectors to CIAM, IAM, or fraud platforms are not offered; the evidenced integrations are into Tieto's own banking portfolio, including mobile and internet banking, core banking, archiving, and customer service systems. An administration client gives bank staff a session-level view of each verification with selfie and document images, per-check outcomes, decision details, and manual accept and decline actions, complemented by a statistics view showing funnel drop-off, document nationalities, and device platforms. Administrator's access is federated through SAML and OIDC. Administrator activity, policy changes, and failed access attempts are logged. However, there is no syslog or SIEM forwarding.

Tieto is suited for banks and financial institutions in the Nordics, particularly Norway, which want high-assurance chip-based verification operated as a managed service and integrated with the same vendor's banking platform, for app activation, KYC evidence refreshes, and re-authentication scenarios where national eID schemes require prior physical enrollment. Buyers must accept firm boundaries: only NFC-chipped ICAO documents on NFC-capable phones can be verified, registry and lost-and-stolen checks apply to Norway only, and decision logic beyond configurable manual review must live in the customer's systems. Assurance rests on the cryptographic verification chain, group-level ISO/IEC 27001 certification, and the OEM's laboratory testing; no SOC 2 Type 2 attestation. Given the small installed base, buyers outside the Norwegian banking market should validate operational scale, document coverage for their user population, and the track record of the recently added deepfake and morphing detection features.

Strengths

- NFC Based verification rather than optical document assurance, which suits high-assurance onboarding and KYC refresh in markets where chipped passports and identity cards are widespread
- Embedding in the Tieto Banktech platform lets banks consume identity verification integrated with cards, payments, core banking, and a 24/7 banking operations

organization, reducing integration effort for institutions already running on Tieto's stack

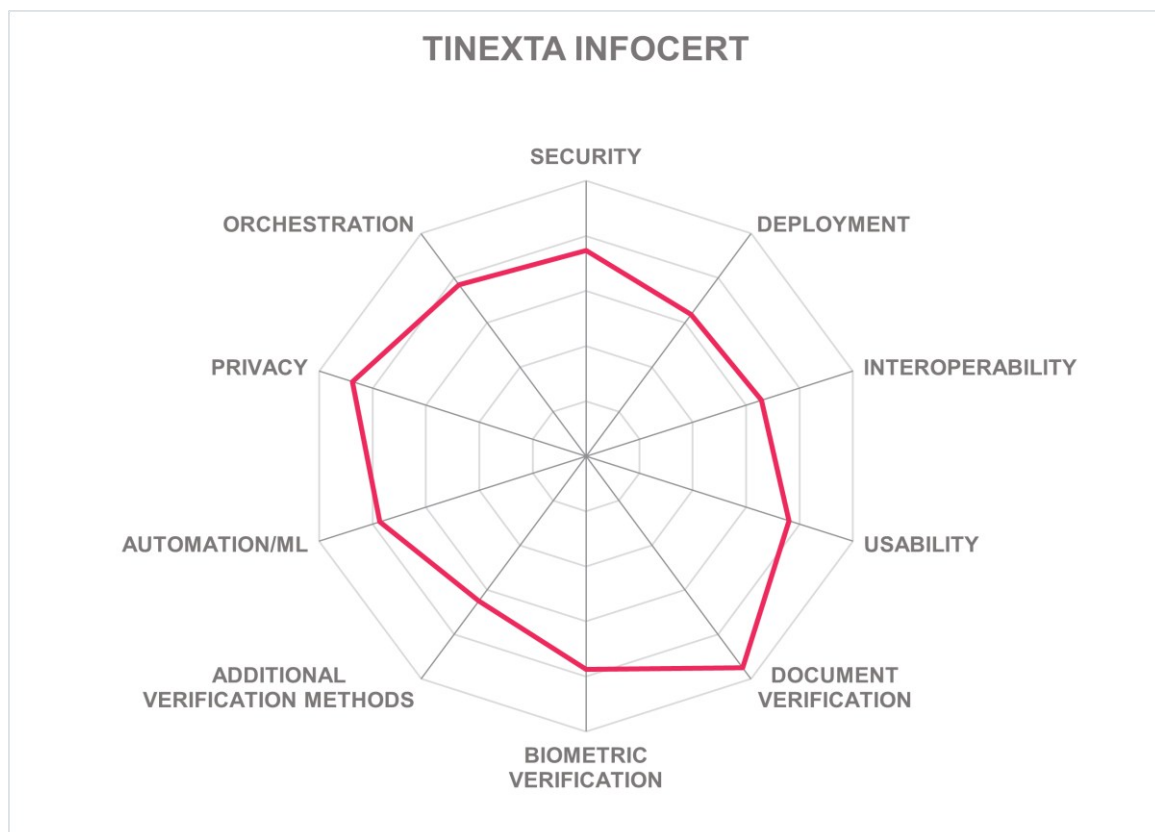
- The biometric pipeline is independently tested: the OEM supplier Mobai participates in the NIST FRTE 1:1 evaluations, and its presentation attack detection was attested by the Idiap Research Institute's FIDO-accredited
- The privacy architecture, sovereign hosting in Norway, , HSM-signed evidence aligned with Norwegian data protection authority guidance, can matter to banks with strict data protection expectations
- Reuse of the verified passport photograph as a protected server-stored reference enables biometric re-authentication and account recovery beyond what possession-based Nordic eID authentication demonstrates

Challenges

- The solution is delivered only as a managed service
- NFC-only verification excludes users whose documents lack chips or whose phones lack NFC, and there is no optical fallback, browser flow, mDL, verifiable credential, or eID verification; buyers with heterogeneous user populations will need a complementary vendor
- Authoritative-source and lost-and-stolen checks are Norway-specific, and the customer base is small and Norwegian; buyers in other markets should validate document coverage, local attribute sources, and support reach before committing
- There are no cross-factor risk engine, policy weighting, or automated risk-based actions, and no PEP or sanctions screening; manual-review rules are configured by Tieto rather than self-service, so fraud teams must orchestrate decisions in their own systems
- Face matching, liveness, deepfake, and morphing detection are OEM-delivered by Mobai, and app shielding is partner-delivered by Promon; even though all processing stays inside Tieto's environment, buyers should validate how algorithm updates, retesting, and support escalation are handled across this chain

Tinexta Infocert – TOP (Trusted Onboarding Platform)

tinexta
infocert



Leadership



Tinexta Infocert, headquartered in Roma, founded in 2007 and the core of the Digital Trust business unit of Tinexta, an Italian group listed on Euronext STAR Milan, is one of Europe's larger QTSPs under eIDAS, with group companies in 12 countries across EMEA and Latin America. Identity verification is delivered through TOP, the Trusted Onboarding Platform, a modular offering that combines verification of natural persons with qualified trust services, so that an onboarding journey can end in a qualified or advanced electronic signature, evidence preservation, or qualified electronic registered delivery on the same platform. Identification

methods include face-to-face verification, operator-led remote video identification, a fully automated self-service method, a hybrid unattended method approved for qualified certificate issuance (SelfQ), NFC-based document reading, and national eID schemes brokered through the company's eID Gateway. Licensing is pay-as-you-go per transaction with a one-off setup fee and optional paid services. Primary use cases are consumer onboarding in regulated services, pre-employment identity checks, verification of legal representatives in B2B onboarding, and re-verification of returning users. The customer base is concentrated in EMEA, above all Southern Europe, with government, services, and financial customers prominent.

TOP is delivered as a vendor-operated SaaS service and is primarily hosted on dedicated AWS infrastructure in EU regions (Dublin and Milan), plus Tinexta Infocert's own Italian data centers. The service is multi-tenant, with single-tenant deployment available on a project basis. The service is certified against ISO/IEC 27001 and holds a SOC 2 Type 2 attestation scoped to security and availability. On-premises deployment is not part of TOP's standard offering. Document verification combines image and video capture with OCR extraction, MRZ checksum validation, consistency checks between the visual and machine-readable zones, and physical security feature checks; SelfQ adds a guided document video for operator review of holograms. NFC chip reading cryptographically validates issuer signatures on ICAO-compliant passports and electronic identity cards. A proprietary OCR and machine-learning component verifies several tens of document types, mainly physical documents for selected countries, while OEM technology from Veridas extends coverage to hundreds of document types across roughly 170 issuing countries. However, ISO/IEC 18013-5 mDL verification is limited to pilots. Biometric verification is face only: 1:1 matching between the document portrait and a live selfie and active liveness with randomized challenge-response gestures are native, while passive liveness is delivered through the partner IdentifAI, and video identification sessions run on OEM infrastructure from Vonage. Fully automated flows complete in roughly one to three minutes. For qualified or advanced electronic signature workflows where Tinexta InfoCert acts as the QTSP/TSP, hybrid verification flows are normally routed to back-office checks by Tinexta Infocert operators per requirement of the QES service model. Customers may perform these activities using their own operators only after execution of a Registration Authority Officer (RAO) agreement with Tinexta Infocert and successful RAO qualification and training of the customer-designated personnel. Where back-office reviews are performed for purposes unrelated to certificate issuance or regulated trust services, customers may use their own operators without a RAO agreement or specific training. EIDAS Low, Substantial, and High can be reached depending on evidence and configuration, with NFC or notified eIDs used for High. Beyond chip validation and notified eID schemes, registry checks are integrated per project rather than through a standing network, and Finextra reports national conformity for identification in Spain (SEPBLAC), Germany (Bundesanstalt für Finanzdienstleistungsaufsicht AML context), and Switzerland (ZertES).

Fraud controls on the document side detect photo substitution, compositing, print and screen-replay artifacts, photocopies, layout, and typography anomalies, and AI-generated or AI-edited document images; stolen-identity and synthetic-document indicators are derived from consistency checks across document, biometric, and contextual signals. The liveness component holds March 2025 certificates of conformity at Substantial level from the French

conformity assessment body CLR Cert for presentation attack detection (ISO/IEC 30107-3) and biometric data injection attack detection (CEN/TS 18099). Injection detection at SDK and API level and session-integrity checks are supported; virtual-camera and emulator detection are not. Verification returns risk and confidence scores with configurable weighting, thresholds, and jurisdiction-specific policies, driving outcomes from automated approval through step-up, evidence requests, and adjudication to rejection. Reason codes are organized by attack pattern rather than labeled as deepfake or AI-assisted, and there is no deepfake-specific false-positive reporting or separate audit trail. TOP ID Protect, introduced within the last year, adds a controlled 1:N check of new applicants against anonymized, vectorized face representations of previously verified or fraud-flagged identities. These representations are held per customer or shared across Tinexta Infocert's certificate-issuance base with consent, in order to flag cases where the same face presents different personal data. The in-house face matcher has been submitted to the NIST FRTE 1:1 track. PEP, UBO, and sanctions screening are not native and are integrated per project with customer-selected providers; LEI issuance and validation are native, through Tinexta Infocert's GLEIF Local Operating Unit accreditation. Default device intelligence is limited to IP address, derived geolocation, and device type. The solution deliberately avoids persistent user behavior analytics and behavioral biometrics.

Consent is collected at the start of each flow for document capture, active and passive liveness, and biometric processing. Biometric templates are processed transiently and not persistently stored by default; raw evidence is retained only to meet audit and QTSP obligations, with retention configurable per customer and jurisdiction. Data is protected with HSM-protected keys and cryptographically signed, write-once logs. End-user data is not used for model training or shared externally. Customers retrieving evidence via the API become independent controllers for further processing. Data-subject rights are handled by the customer because no end-user portal is provided.

Integration is exposed through REST APIs with webhooks and callbacks, SOAP interfaces for specific legacy services, an embeddable web widget for capture, and Android and iOS SDKs, documented on a public developer portal. The IQP backend orchestrates workflow sequencing, scoring, and state management with preconfigured templates for common onboarding processes, but workflows are configured by Tinexta Infocert's technical team. However, there is no customer-facing workflow builder, and the adjudication back office is a web console whose data is retrievable via API but not operable through it. There are no prebuilt IAM connectors; integrations follow OAuth 2.0 and OIDC patterns and project-specific work. Downstream outputs include verification results, assurance levels, risk scores, reason codes, and audit-grade evidence dossiers. All of these outputs can flow directly into qualified signature issuance on the same platform. The eID Gateway provides a single integration point for more than 50 national eID schemes, including Italy's Sistema Pubblico di Identità Digitale, FranceConnect, and the German eID via Authada technology and itsme. It also enables organizations acting as relying parties to verify wallet-based verifiable credentials. Tinexta Infocert is suited for organizations onboarding customers in the EU, particularly in Italy, Spain, and France, and in banking, insurance, utilities, and the public sector whose verification outcomes must carry legal effect through qualified certificates, signatures, or registered delivery. The platform is available only as an EU-hosted SaaS offering, with vendor-configured workflows and a customer and support presence

concentrated in Southern Europe. These factors may be limiting for organizations requiring global coverage or self-service workflow orchestration. Presentation attack and injection attack detection are independently certified, and identification methods hold eIDAS Article 24 conformity assessments, with AgID approval in Italy. Buyers should validate document and registry coverage outside Europe, the scope of mDL support, and current independent face-matching accuracy evidence.

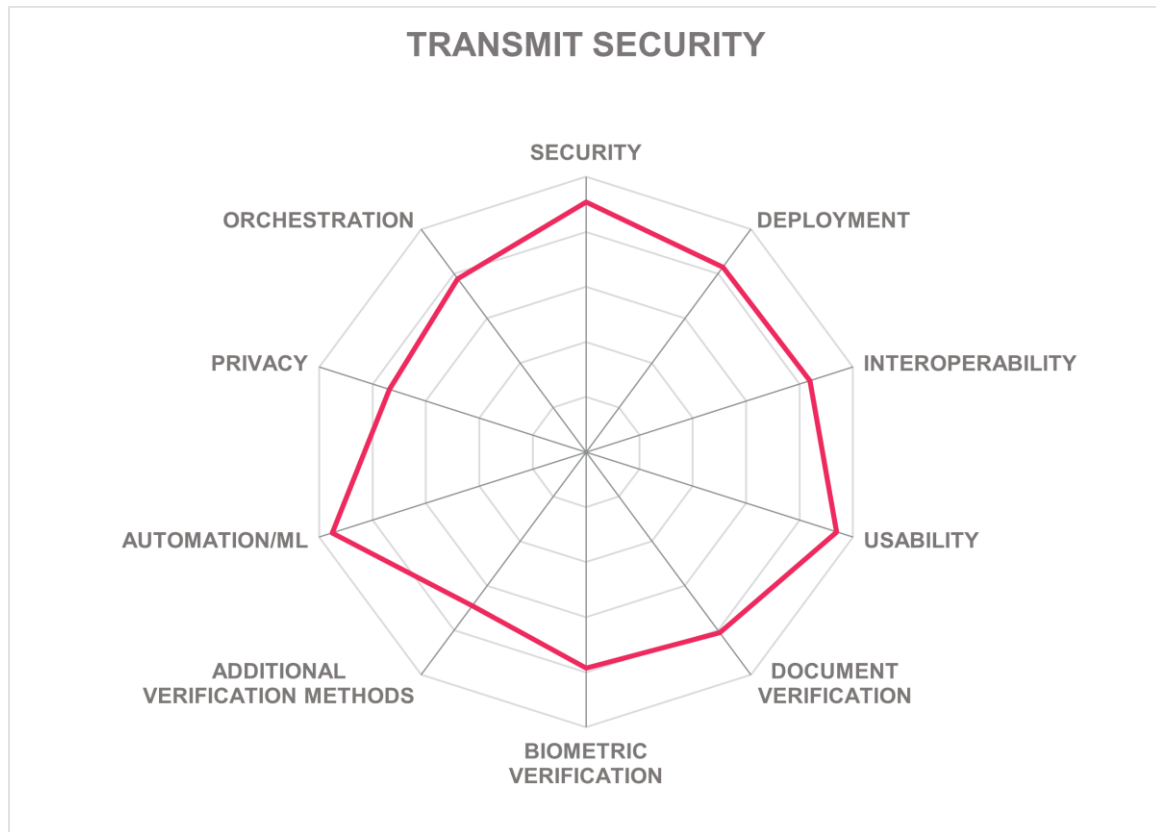
Strengths

- QTSP-grade verification bound to legally binding outcomes: which shortens the path from identity proofing to enforceable transactions for regulated EU onboarding
- Independent biometric assurance on two fronts: certificates of conformity at Substantial level from CLR Cert for both presentation attack detection and injection attack detection reduce procurement uncertainty for buyers that must document liveness controls against AI-assisted attacks
- A wide range of assurance-graded identification in a single platform so buyers can match the method to each country's regulation without re-integrating
- The eID Gateway brokers SPID, FranceConnect, the German eID, itsme, and other national schemes through a single interface, positioning buyers for the EUDI Wallet transition with limited rework as wallet-based identification becomes available
- TOP ID Protect adds consent-based 1:N duplicate and impersonation detection using anonymized, vectorized face representations, per tenant or across Infocert's certificate-issuance base, which helps fraud teams catch repeat use of the same face under different identity data

Challenges

- Customer base, on-site support, and registry integrations are concentrated in EMEA which calls for additional due diligence from buyers with significant verification volumes in North America or APAC
- Orchestration is vendor-configured: there is no customer-facing workflow builder or self-service administration console, and the adjudication back office is not API-operable
- Broad document coverage, passive liveness, and video-identification infrastructure depend on OEM and partner components (Veridas, IdentifAI, Vonage); buyers that require one vendor should validate accountability boundaries
- Fraud reporting is unified rather than segmented which constrains fraud-team tuning and audit in the face of evolving AI-assisted attacks

Transmit – Mosaic Platform



Leadership



Transmit Security, privately held, founded in 2014 and operating from Boston and Tel Aviv, offers the Mosaic Platform, which combines CIAM, authentication, orchestration, fraud detection and response, and identity verification. Mosaic for Identity Verification is sold standalone or as a platform module, and its results feed the same journey engine that drives authentication and fraud decisioning. Licensing is subscription-based per monthly active user, with per-transaction pricing for identity verification and annual or multi-year enterprise terms. Primary use cases are account opening, high-risk transaction approval, step-up verification, and account recovery, including secure credential-reset scenarios delivered with privileged access management (PAM) partners such as CyberArk. The customer base consists mainly of large enterprises, is strongest in financial services with growing activity in

telecommunications, retail, insurance, and travel, and is weighted toward North America with additional presence in EMEA and Latin America.

The service is delivered as vendor-managed SaaS in multi-tenant or single-tenant form, hosted on Google Cloud in regions in the United States, the EU (Belgium and the Netherlands), Canada, Australia, and Japan, with the region selected per customer. Customer-managed keys (BYOK/HYOK) and HSM integration are supported.

Verification is based on optical document verification and facial biometrics. Documents are captured as images with automatic quality feedback, then checked through template matching, OCR and MRZ extraction, and physical security feature analysis, with image-based coverage across 244 countries and territories. ICAO 9303 ePassports are read via NFC with PKI validation of chip data across more than 150 issuing states, and the same chip-reading stack supports ICAO-compliant electronic national identity cards, currently the Chilean identity card, while country-specific eID protocols such as the German nPA are reachable through orchestration partners. ISO/IEC 18013-5 mobile driver's licenses are not supported.

Document verification is native for North America and Latin America and for passports globally; other regions are covered through partner technology. Facial verification is native and uses passive liveness; 1:1 comparison matches the selfie against the document portrait, and 1:N search runs against customer-uploaded face blocklists and repeated-face detection across sessions within a tenant. The face matching algorithm was submitted to the NIST FRTE 1:1 evaluation for the first time in December 2025. Checks against government registries, PII validation services covering SSN, address, and name and date-of-birth, phone-number verification, and AML/KYC data sources are configured per customer through orchestration partners rather than connected by default.

Fraud controls are closely integrated with verification. Passive liveness applies AI-based analysis of imagery and session telemetry to detect spoofing, 2D masks, screen and video replay, virtual cameras, emulators, and SDK- or API-level injection, with capture provenance checks confirming that samples originate from a live session. AI-generated or AI-manipulated selfie images and videos are detected, and a specialist third-party deepfake-detection service adds a further layer, while dedicated face-swap detection and deepfake-specific reason codes and scores are not yet available. Document fraud models detect tampering, compositing, portrait replacement, template-based or synthetic generation, and AI-edited document images.

Cross-session intelligence correlates faces, devices, networks, and profiles to expose repeated identities and fraud rings, with offline models producing cohort alerts and link analysis, and an opt-in consortium shares IP and device risk signals across customers. However, face data is not shared across tenants. Device intelligence, user behavior analytics, and behavioral biometrics from the Mosaic fraud module can feed verification decisions, with depth depending on licensing scope. Risk scoring with configurable factor weighting produces allow, challenge, or deny outcomes, while the Admin Portal exposes reason codes and contextual indicators such as bot activity, impossible travel, or emulator

use, and detection models are versioned with a formal update process. Manual review can be handled by the customer or by the vendor's own analyst teams, offered as a service.

Consent is collected before verification, covering biometric extraction and processing of document data, and passive liveness is disclosed to the user; notice of data aggregation depends on customer implementation. Verification data is stored in the vendor's cloud infrastructure in the customer's selected hosting region, with encryption at rest and in transit, tokenization and pseudonymization, role-based and privileged access controls, and audit logging; document images, selfies, and biometric templates remain in-region. In addition, customers can retrieve images, results, scores, and session metadata via API for their own governance, but templates remain vendor-side. Retention is configurable per customer and per jurisdiction, end-user data is not used for model training or shared externally, and SDK keys reside in the iOS Keychain and Android Keystore.

Integration centers on the orchestration layer. A drag-and-drop journey builder composes modular verification steps for document acquisition, biometric acquisition, and decisioning inside wider journeys that create users, register the verified selfie as a biometric authenticator for later step-up or recovery, and route fallbacks; extensions are no-code or low-code with TypeScript for advanced logic. The Integration Hub connects external data validation, AML/KYC, phone verification, and third-party identity verification services, so customers can orchestrate incumbent verification vendors alongside or instead of the native engine. Journey analytics report conversion, drop-off, and step duration, and offline workflows convert fraud alerts into tickets, messages, or downstream actions. Capabilities are exposed through REST APIs and webhooks, with SDKs for Android, iOS, Java, C/C++, .NET, and Python; administrative access federates via SAML and OIDC with role-, attribute-, and policy-based access control, and integrity-hashed, signed logs export to SIEM via syslog. Verifiable credential issuance and verification following OpenID for Verifiable Credential Issuance can be assembled from custom orchestration steps but is not productized, and no vendor wallet is offered.

Transmit Security is suited for large enterprises, particularly in financial services, telecommunications, and retail, that want identity verification embedded in a customer identity, fraud, and orchestration platform and that value consolidation or coexistence with existing verification vendors. The solution holds an ISO/IEC 27001 certification and a SOC 2 Type 2 attestation across all five Trust Services Criteria. Buyers with European data-residency requirements should confirm in contract the hosting region, the sub-processor footprint, and in-region processing. Buyers that need mDL acceptance, native sanctions and PEP screening, or independently documented presentation attack detection testing should validate current status and timing.

Strengths

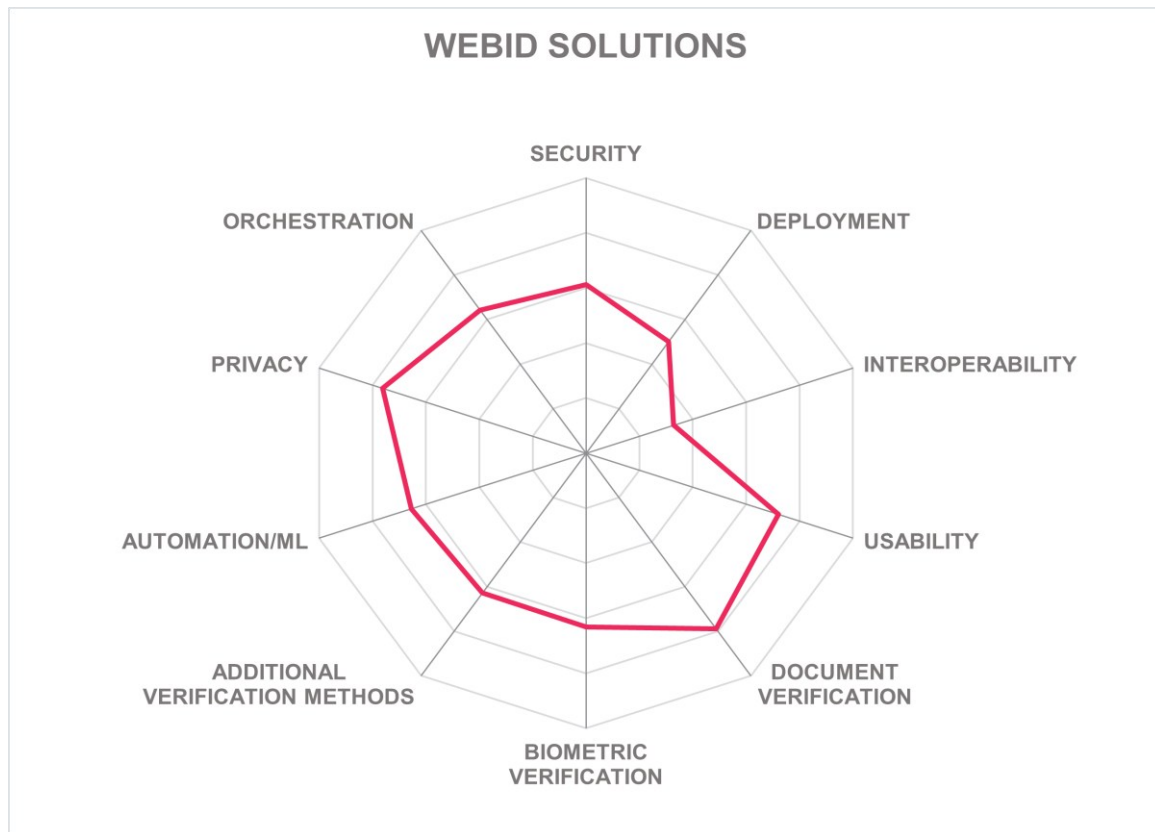
- Orchestration-first architecture that decomposes verification into modular journey steps and can drive third-party verification services through the same journey builder
- A natively integrated fraud stack, device intelligence, user behavior analytics, behavioral biometrics, and cross-session repeated-face and repeated-device detection with offline fraud-ring analysis

- The verified selfie can be registered as a biometric authenticator in the same platform, so onboarding, step-up, account recovery, and login reuse one identity anchor without integrating a separate authentication product
- Vendor-provided analyst teams for fraud and verification review, combined with Admin Portal reason codes and decision evidence, reduce the operational burden for buyers without an in-house review team
- Orchestration policies and user journeys can be generated, simulated, and deployed from natural-language input, with auto-generated risk insights and chatbot-style guidance in the admin tooling

Challenges

- Identity verification is cloud-only, so buyers with data-residency or local-processing requirements should have in-region processing, not only in-region storage, written in the contract
- Independent biometric assurance is still thin: presentation attack detection testing is reported at ISO/IEC 30107-3 Level 1, Level 2 is not tested, and deepfake-specific reason codes are not yet available
- Document coverage outside the Americas (except passports) is partner-delivered, and sanctions, PEP, and AML screening are not native, so buyers needing single-vendor accountability for those checks should verify the partner arrangements in their geographies
- Fraud thresholds and per-jurisdiction policies are configured in the platform on request rather than through customer self-service, and face blocklist intelligence does not extend across tenants, which limits detection of fraudsters already seen at other customers

WebID – Identity Verification Product Suite



WebID Solutions GmbH, founded in 2012 and headquartered in Germany, is a privately held, private-equity-backed vendor that introduced video-based remote identity verification for German AML compliance, accepted by the financial regulator BaFin in 2014. The 2026 offering is a full-service identity verification suite whose methods can be combined per use case: VideoID and VideoID International for human-assisted video verification, VisualID for automated capture with extended hologram checks and offline human review, AutoID for fully automated document and biometric verification, eID and ePassID for NFC-based verification of the German eID card and chipped passports, AccountID for bank-account-based verification, TrueID for re-identification against previously verified identities, an automated age-check variant, CorporateID for business verification including UBOs and qualified electronic signing through SignID and Multi-QES. Licensing is per transaction for all identification and signing products, with a monthly service fee and a per-user fee for the business portal. The primary use case is consumer KYC onboarding, with additional fraud- and risk-led verification and contract-signing scenarios. The customer base is concentrated in German-speaking Europe and dominated by financial services, with further customers in

telecommunications, e-commerce, travel, and gaming. A distinctive asset is the consent-based store of more than 25 million verified identity profiles in Germany, which TrueID draws on for re-identification.

The service is delivered as vendor-managed SaaS from a PlusServer data center in Cologne, Germany, with AWS used for selected processing services. Each customer, and in some cases each customer-specific product, runs as an isolated instance. On-premises deployment has been performed in the past but is not in current demand. The human video channel runs 06:00–22:00 German time with in-house and EU-based outsourced agents, while automated routes are available around the clock.

Verification methods span human-assisted and automated routes. Document verification is partner-delivered using Regula technology covering documents from 195 countries and more than 9,000 document pages; capture is via image, video, or NFC chip reading, physical security features are checked, and there are no connections to issuing-authority or other source-of-truth registries. Mobile driver's licenses under ISO/IEC 18013-5 are not supported. ePassID reads the passport chip, including the chip portrait, for comparison against a live selfie. AccountID combines automated capture with a bank-account login and a one-cent reference transfer, a fully automated route that satisfies German AML requirements. Attribute verification covers name, date of birth, address, phone number, and identification numbers via data aggregation from credit reference agencies and bank account data. Facial biometric comparison is partner-delivered through the Amazon Rekognition cloud service, with 1:1 matching, and 1:N blocklist screening, while active liveness detection with randomized head-movement challenges is delivered with ID R&D Liveness technology. Biometric templates are stored encrypted in the platform's central database. Fully automated verification completes in 40 seconds to five minutes, and hybrid verification with human adjudication is available. VideoID and VisualID are certified by TÜV Informationstechnik against the eIDAS regulation for identity verification.

Fraud controls combine machine and human mechanisms. Document tamper detection from ID R&D, a Mitek company, identifies AI-generated or AI-edited document images, compositing, and template-based synthetic documents, with a separate score and distinct error categories for suspected AI-assisted document fraud. Biometric checks address spoofing, masks, AI-generated selfie images and videos, face swaps, replay, virtual camera, emulator, and SDK- or API-level injection attacks, with capture provenance verification and randomized challenge prompts designed to expose injected media. Video agents are trained to detect social-engineering and behavioral cues, and a facial blocklist hashes the faces of detected fraudsters to block them across all products. Signals from document, biometric, liveness, and device checks like geolocation, device ID, type, and fingerprint are aggregated into a weighted risk score, or returned individually to customers that prefer to decide themselves. PEP, UBO, denylist, sanctions, and LEI screening are partner-delivered, with AML- and PSD2-specific features. Deepfake detection models are versioned and follow a formal update process; there are no customer-configurable thresholds, no false-positive reporting, and no deepfake-specific audit trail.

Privacy controls reflect the German AML heritage. Consent is collected before verification for the entire process, and identity storage for reuse requires consent both at storage and at

each reuse. Data is held in the German data center with database and field-level encryption, pseudonymization, and keys protected in an HSM; the hosting provider is ISO 27001, PCI-DSS, and Bundesamt für Sicherheit in der Informationstechnik (BSI, German Federal Office for Information Security) C5 certified, and WebID itself maintains an ISAE 3402 Type 2 report on its service-related internal control system. Retention is customizable per customer and per jurisdiction, users can learn which attributes were collected and revoke a customer's access, and end-user data is not used for model training or shared externally. Mobile capture uses the device Secure Enclave or TEE, and local data is deleted afterward.

Orchestration is a core offering: the WebID Hub can link products in any sequence. For example, customers can route users based on risk score, transaction value, or regulatory requirements. The system can fall back to a video call when an automated score is borderline. Flows are configured by WebID staff rather than by customers, although the new WebID Portal lets customers without an API create transactions, manage verification processes, and retrieve evidence data. Integration is exposed through REST/JSON APIs with JWT-based authentication, Android and iOS SDKs, a vendor app, and browser flows, documented in a developer portal; a Shopify plugin serves e-commerce checkouts. Webhooks, IAM platform connectors, and SIEM export are not provided, and customer-facing reporting is delivered through dashboards updated daily or monthly PDF reports.

WebID is suited for organizations onboarding consumers under German and EU AML rules like banks, insurers, telecommunications providers, and payment or crypto services that need certified video identification, qualified electronic signing, and automated alternatives from one vendor, with conversion supported through method fallbacks and identity reuse. Buyers should note the limitations: delivery is vendor-managed SaaS from Germany only, evidenced coverage and video-agent language support center on German-speaking Europe, core recognition technologies are partner-delivered, and the certification portfolio rests on the TÜV eIDAS product certificates and the ISAE 3402 report rather than ISO 27001 or SOC 2 Type 2 held by WebID itself. Organizations outside the DACH region, or those requiring self-service workflow control and IAM integration, should validate fit.

Strengths

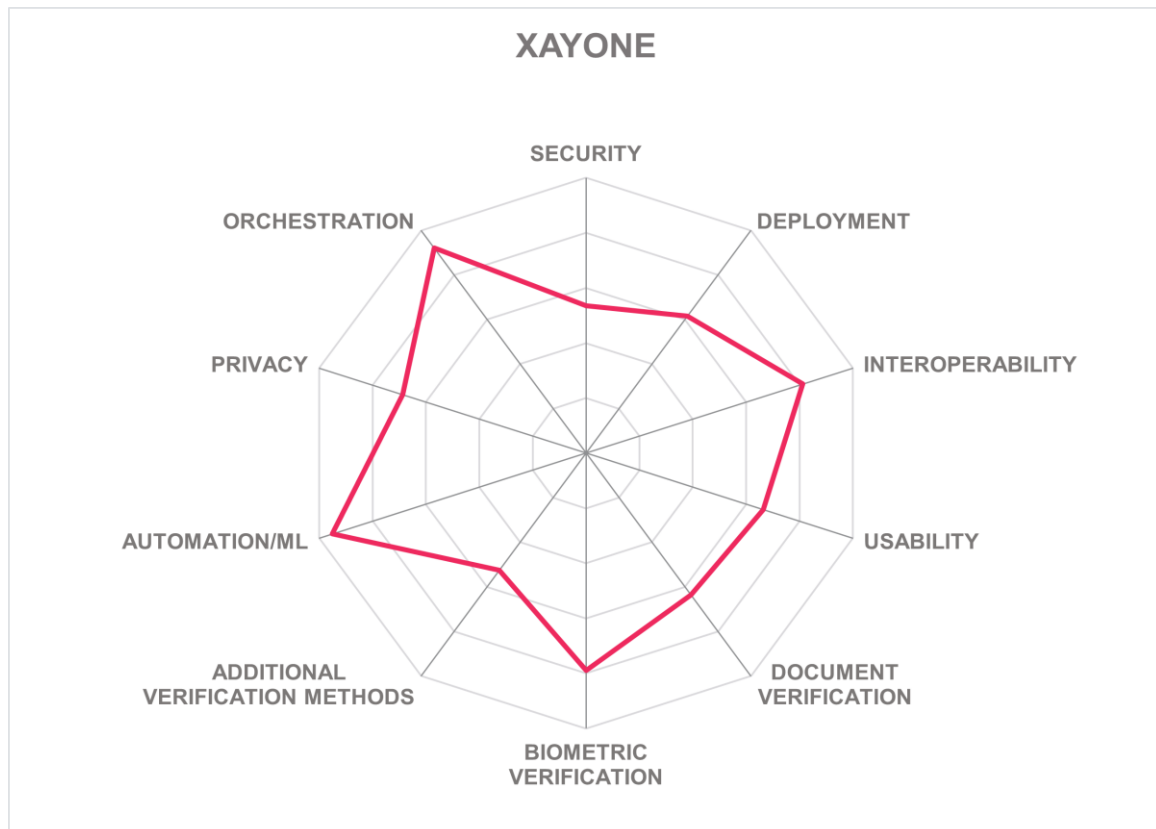
- The breadth of verification methods under one contract lets buyers match method to regulation, risk, and conversion goals without adding vendors, which few competitors offer at comparable regulatory depth in Germany
- Regulatory anchoring in the strictest German AML context: BaFin-accepted video identification since 2014, TÜV Informationstechnik eIDAS certificates for VideoID and VisualID, and integrated qualified electronic signing shorten compliance diligence for regulated onboarding in the DACH region
- The consent-based store of more than 25 million verified identity profiles gives TrueID a re-identification route that completes in seconds, improving conversion for returning users and positioning WebID for reuse-friendly provisions under the EU Anti-Money Laundering Regulation (AMLR)
- The human-assisted video channel doubles as a deepfake countermeasure: trained agents, randomized head- and hand-movement challenges that expose injection artifacts, and scripted social-engineering probes address attack classes that purely automated flows handle with less context

- A cross-product facial blocklist that hashes and screens the faces of previously detected fraudsters (1:N) blocks repeat attempts across all verification methods, a control that grows more effective with WebID's transaction volume

Challenges

- Core recognition technology is partner-delivered which may matter for buyers that want one vendor to own algorithm testing, performance evidence, and escalation across the verification chain
- Customer and operational concentration in German-speaking Europe: video agents work in German and English by default, other languages require per-customer agreements
- Video agents work 06:00–22:00 German time with no follow-the-sun operation, so buyers with international or off-hours populations depend on the automated routes
- Verification flows are configured by WebID staff rather than by customers, the self-service portal is new and does not yet include workflow building, which may slow buyers that expect to tune flows
- No customer-configurable fraud thresholds, analyst-facing reason-code tooling, or override audit trails, which may slow fraud teams that expect to tune thresholds themselves

XAYONE – XAYONE ID Verification (Trust Platform)



XAYONE, established as Oxylium Solutions and renamed in 2022, is a privately held identity software vendor with offices in Luxembourg and Casablanca, owned by its founding partners and an investment fund. XAYONE ID Verification (XVID) is the identity verification component of the XAYONE Trust Platform, which also provides CIAM, access governance functions, and electronic signature services, so a verified identity can move directly into enrollment, authentication, and signing journeys on the same platform. Licensing is flexible per use case, spanning per-user, per-transaction, subscription, and fixed or infrastructure-based models. Primary use cases are consumer onboarding and KYC in banking and fintech, age verification, e-government, and travel-document verification for airlines and ground handlers. The customer base is mid-market and concentrated in EMEA, strongest in North Africa, and the solution serves consumer rather than workforce identity scenarios.

The product is delivered as on-premises software, a vendor-hosted cloud service, or a managed service. XAYONE-hosted cloud service runs in a data center in Luxembourg operated in partnership with EBRC and supports multi-tenant and single-tenant operation. The platform holds no independent ISO/IEC 27001 or SOC 2 Type 2 certifications.

Verification is anchored in optical document verification of passports, national identity cards, and driver's licenses, captured as images or video through web and mobile channels, with stated coverage of more than 16,000 document templates from 195 countries and territories. Checks include OCR extraction, MRZ check-digit validation, barcode and document-number format checks, date validation, hologram and photocopy detection, and cross-comparison of visual zone, MRZ, barcode, and NFC chip data on ePassports and electronic identity cards. Document authenticity classification uses Regula's Automatic Authenticity Control module as OEM technology within XAYONE's own capture and decisioning workflow; the airport use case adds handheld readers with infrared and ultraviolet light sources for security-feature inspection beyond smartphone capture. Mobile driver's licenses according to ISO/IEC 18013-5 are not yet supported. Face matching relies on OEM algorithms from Aware, a NIST FRTE participant, in both 1:1 and 1:N modes. Liveness detection is passive, analyzing skin texture, lighting, compression artifacts, and micro-movements in video, and returns a liveness score; the underlying Aware engine passed iBeta presentation attack detection testing at ISO/IEC 30107-3 Levels 1 and 2 in 2020. Alongside fully automated verification, an agent-assisted video mode lets the customer's own staff guide document capture and adjudicate results in a live session.

Fraud controls cover documents, biometrics, and session context. Document checks detect tampering and compositing, template-based and synthetic document generation, AI-generated or AI-edited document images, and inconsistencies between document and biometric evidence, with separate reason codes and risk scores for suspected AI-assisted document fraud. Biometric checks address spoofs and masks, AI-generated or manipulated selfie images and videos, face swaps, screen and video replays, virtual cameras, emulator-based capture, and image or video injection at SDK or API level, plus capture provenance and session-integrity checks. Device intelligence evaluates IP address and reputation, geolocation and geo-velocity, device identifiers, fingerprints, health, reputation, and jailbreak or root status; user behavior analytics evaluate login and transaction patterns, and behavioral biometrics are not offered. KYC screening spans PEP, UBO, denylist, sanctions, and LEI checks, with AML verification delivered through a third-party partner. Risk factors are weighed in customer-defined policies that yield a risk score and drive step-up authentication or allow and deny decisions; thresholds are configurable by geography or jurisdiction, analysts see reason codes and supporting evidence, and manual overrides are recorded in an audit trail.

Privacy controls include user notification of liveness checks and data aggregation, with consent collected for each attribute verified against an external source. Sensitive data is stored encrypted in the platform database behind user-based and privileged access controls, keys can be held in HSMs or managed by the customer, and mobile applications use the device Secure Enclave or TEE with keys in the Secure Element. Retention policies are configurable per jurisdiction, though not per customer, and end-users can see which attributes were collected and verified, revoke a relying organization's access, and view which organizations hold access. End-user data is not used for model training or shared externally.

Integration is exposed through REST and GraphQL APIs, webhooks, WebSockets, and W3C WebAuthn, with OAuth2, SAML, OIDC, JWT, and key-exchange options for API authentication, and SDKs for Android, iOS, Java, C/C++, .NET, and Python documented in a

developer portal. Verification flows are designed in a no-code and low-code policy orchestrator that maps identity and authentication assurance levels to verification steps and authenticators, supports Business Process Model and Notation (BPMN) import and export, and provides prebuilt workflow templates. The administration console combines identity status, verification evidence such as document images and expiry dates, and risk and governance dashboards, with tamper-protected logs and syslog output for SIEM integration. Federation connectors for external identity providers including FranceConnect, LuxTrust, Ping One, and Microsoft support eID-based sign-in in orchestrated journeys, while external IAM platforms consume verification results through the APIs; in the aviation use case, connectors to Amadeus and International Air Transport Association (IATA) Timatic bring travel and document-rule context into verification decisions. A self-service portal lets end users re-verify attributes and manage authenticators after a failed verification.

XAYONE is suited for mid-market organizations in EMEA, particularly in North African and francophone markets, which want identity verification, CIAM, and electronic signature from a single vendor, and for airlines and ground handlers that need assisted travel-document verification with dedicated hardware and evidence-preserving reporting. Deployment options from on-premises to Luxembourg-hosted SaaS support EU data-residency requirements. The platform has not been independently audited, and face matching and document forensics are OEM-delivered. Organizations with large multi-region programs, mDL requirements, or dependence on broad authoritative-source coverage should validate country-level fit.

Strengths

- Deployment flexibility includes on-premises software, vendor-hosted cloud on AWS, Azure, or Google Cloud, and a managed service. The primary data center in Luxembourg, supports EU data-residency requirements
- The no-code policy orchestrator models identity, authentication, and federation assurance levels and maps them to verification steps and authenticators, with risk-score-driven step-up, which helps regulated buyers formalize tiered assurance without custom coding
- A differentiated travel-document verification offering combines handheld infrared and ultraviolet readers, NFC chip validation, country-specific document rules via IATA Timatic, Amadeus integration, and evidence-preserving reporting, publicly documented in production at Royal Air Maroc Handling across Moroccan airports
- Hybrid delivery of fully automated flows and agent-assisted video verification lets banks keep human adjudication inside regulated onboarding while using the same document and biometric checks
- Document template coverage of more than 16,000 templates, with new document types added at no extra cost, supports user bases holding fewer common documents, which matters in African and Middle Eastern markets

Challenges

- The platform holds no independent ISO/IEC 27001 or SOC 2 Type 2 certifications which can lengthen procurement in regulated environments and remain unchanged from the prior assessment

- Face matching, PAD-tested liveness, and document authenticity classification are OEM-delivered by Aware and Regula, buyers should validate which algorithm versions ship today and how OEM updates and escalations are handled
- A small vendor footprint with a customer base concentrated in EMEA and on-site support limited to EMEA may require additional diligence for large or multi-region verification programs
- Mobile driver's licenses according to ISO/IEC 18013-5 are not supported and European Digital Identity Wallet compatibility is still in development, which matters for buyers with near-term reusable-identity requirements

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

AccuraScan

AccuraScan was founded in 2017 and is headquartered in Dubai, United Arab Emirates. AccuraScan provides AI-powered identity verification solutions including ID document scanning, facial recognition, liveness detection, and real-time KYC compliance. Its mobile first platform supports over 190 countries and reads passports, visas, and national IDs with OCR technology optimized for speed and accuracy. AccuraScan is widely adopted in sectors such as banking, travel, and telecom for seamless digital onboarding and fraud prevention.

Why worth watching: AccuraScan's end-to-end identity verification suite combines global document coverage with fast, lightweight deployment, making it an agile choice for businesses scaling digital identity services across borders.

CLEAR

CLEAR was founded in 2010 and is headquartered in New York City, New York. CLEAR offers identity verification services that combine biometric authentication with real-time data validation to enable frictionless access experiences in airports, stadiums, and digital environments. Its platform extends beyond physical security, supporting digital identity use cases such as age verification, health credentials, and secure onboarding. CLEAR leverages a network of verified users and secure infrastructure to streamline identity confirmation across multiple industries.

Why worth watching: CLEAR's expansion into digital identity verification demonstrates its potential to unify physical and digital trust frameworks through a biometric -first, privacy conscious approach.

Cognito

Cognito was founded in 2014, acquired by Plaid in 2022, and is headquartered in San Francisco, California. Cognito offers identity verification and compliance solutions tailored for fast-growing fintechs and digital platforms. Its platform provides real-time ID verification, watchlist screening, and ongoing AML monitoring, with a focus on seamless integration and developer-friendly APIs.

Why worth watching: Cognito's API-first approach to identity verification and AML compliance makes it a compelling choice for digital-native businesses seeking to scale quickly without compromising security.

DuckDuckGoose AI

DuckDuckGoose AI was founded in 2020 and is headquartered in the Netherlands. Its platform, Phocus, validates the authenticity of biometric and audiovisual evidence before that evidence is used for identity binding or decisioning, analyzing images, video, and audio for deepfakes, face swaps, synthetic media, cloned voices, and injection attacks. Outputs include authenticity scores, generation-type indicators, uncertainty scores, and explainability artifacts such as activation maps, delivered through APIs into existing identity verification, KYC, authentication, and risk systems. Phocus is deliberately not an identity verification product in its own right: it performs no document verification, no face matching, no chip reading, and no authoritative source checks, and it issues no assurance level of its own.

Why worth watching: DuckDuckGoose AI is a focused specialist in a threat class that the identity verification market has only recently begun to treat as distinct from presentation attack detection.

Element

Element was founded in 2012 and is headquartered in Singapore. Element offers AI-powered identity verification solutions focused on emerging markets, combining biometric authentication with real-time document verification to enable secure digital onboarding. Its platform is designed to work in low-bandwidth environments and supports a wide range of identity documents and facial biometrics for underserved populations. Element partners with governments, financial institutions, and mobile network operators to provide inclusive and scalable identity infrastructure.

Why worth watching: Element's focus on privacy-preserving, mobile-first identity verification tailored for developing regions positions it well in driving global digital inclusion and secure access.

FACEKI

FACEKI was founded in 2021 and is headquartered in Lahore, Pakistan. FACEKI provides AI-driven identity verification and facial recognition solutions focused on fraud prevention and secure user onboarding. Its platform includes features such as liveness detection, biometric matching, and real-time ID document verification, with support for global compliance standards like KYC and AML. FACEKI's technology is optimized for seamless integration into digital platforms across fintech, healthcare, and telecom sectors.

Why worth watching: FACEKI's emphasis on biometric security and accessibility, combined with its rapid innovation cycle, positions it as a rising contender in global identity verification and fraud prevention.

Facephi

Facephi was founded in 2012 and is headquartered in Alicante, Spain. Facephi specializes in biometric identity verification solutions, offering facial recognition, document authentication, and liveness detection to support secure and user-friendly digital onboarding. Its customer base is primarily in the banking and healthcare sectors, particularly across Latin America and Europe. Facephi's platform complies with international regulatory standards, and it emphasizes ethical AI and data privacy in its design.

Why worth watching: Facephi's strong regional footprint and commitment to ethical biometrics make it a key innovator in trusted identity verification for highly regulated industries.

GBG

GBG is a global specialist in identity data intelligence, founded in 1989 and headquartered in Chester, United Kingdom. Its verification portfolio centers on two products, ID3global for data-based verification and IDscan for document verification, supported by KYB and fraud analytics. IDscan combines document authentication, face matching biometrics, iBeta-accredited passive liveness, deepfake/tamper detection, and NFC chip reading; ID3global is a multi-bureau solution adding PEPs/sanctions screening, synthetic-identity scoring, and ongoing monitoring, with in-country data across 38 countries. Verdicts are delivered via console or API with configurable accept/decline/refer rules, serving finance, gaming, crypto/FX, insurance, retail, and public sector

Why worth watching: GBG couples a long-established multi-bureau data footprint with modern document and biometric verification, focusing on frictionless yet secure onboarding powered by ML-driven verification and configurable real-time decisioning.

HyperVerge

HyperVerge was founded in 2014 and is headquartered in Mountain View, California. HyperVerge provides AI-powered identity verification and KYC solutions, with a focus on image and video-based verification for financial services, telecom, and government sectors. Its platform includes facial recognition, document verification, liveness detection, and fraud detection, optimized for low-bandwidth environments and rapid deployment. HyperVerge's technology is widely adopted across emerging markets, particularly in Asia and Africa, where digital onboarding demands scalability and resilience.

Why worth watching: HyperVerge's strength in delivering high-accuracy identity verification with minimal infrastructure makes it a strategic player for organizations scaling digital access in bandwidth-constrained and high-growth regions.

iDenfy

iDenfy was founded in 2017 and is headquartered in Kaunas, Lithuania. iDenfy provides AI-powered identity verification and fraud prevention services, including document authentication, facial recognition, liveness detection, and AML screening. The platform supports a broad range of industries, from fintech and e-commerce to gaming, with a focus on fast, compliant digital onboarding. iDenfy offers customizable workflows and manual review options to balance automation with accuracy.

Why worth watching: iDenfy's flexible, scalable identity verification suite and emphasis on combining AI with human oversight make it a strong contender for businesses seeking efficient and compliant onboarding solutions.

IDENTT

IDENTT was founded in 2014 and is headquartered in Cologne, Germany. IDENTT provides identity verification solutions that include ID document authentication, facial biometrics, and liveness detection, tailored to meet strict regulatory requirements such as KYC and AML. Its platform combines AI-driven automation with optional manual review to balance speed and accuracy in customer onboarding. IDENTT serves financial institutions, mobility providers, and e-commerce platforms across Europe and beyond.

Why worth watching: IDENTT's combination of regulatory precision, AI-powered automation, and strong European market focus makes it a trusted choice for secure and compliant digital identity verification.

Identyum

Identyum was founded in 2018 and is headquartered in Varaždin, Croatia. Identyum provides digital identity verification and personal data management services through its secure, consent-based platform. It enables users to verify their identity, sign documents, and manage credentials while maintaining full control over their personal data. The platform is designed to support GDPR compliance and is tailored for sectors such as finance, telecom, and public services.

Why worth watching: Identyum's privacy-first approach to identity verification and its focus on user-centric data control make it a standout vendor in the evolving landscape of digital trust and compliance.

Incode

Incode was founded in 2015 and is headquartered in San Francisco, California. Incode acquired AuthenticID in 2025. Incode provides a fully automated identity verification platform that includes biometric facial recognition, document verification, liveness detection, and orchestration tools to streamline onboarding and access management. The company emphasizes privacy, speed, and compliance, serving industries like banking, hospitality, and

government. In 2024, Incode acquired MetaMap, a digital trust platform known for contextual identity signals, enhancing Incode's ability to assess financial inclusion, risk, and compliance in real time.

Why worth watching: Incode's strategic acquisition of MetaMap expands its capabilities beyond identity verification into dynamic trust assessment, making it a comprehensive platform for digital identity and risk intelligence.

LexisNexis IDVerse

LexisNexis acquired IDVerse in 2025. IDVerse offers fully automated, AI-powered identity verification solutions, including document recognition, facial biometrics, and liveness detection, designed to eliminate bias and support global compliance. Its platform requires no human intervention, enabling rapid, secure onboarding for users in over 195 countries and other territories. IDVerse focuses on inclusivity, ensuring high accuracy across a wide range of demographics and document types.

Why worth watching: IDVerse's commitment to ethical AI and zero-human-in-the-loop automation positions it as a trailblazer in scalable identity verification for global enterprises.

Jumio

Jumio was founded in 2010 and is headquartered in Palo Alto, California. Jumio provides end-to-end identity verification and digital onboarding solutions that leverage AI, biometrics, and ML to authenticate ID documents and verify user identities in real time. Its platform includes document verification, facial recognition, liveness detection, and ongoing fraud monitoring, supporting compliance with global KYC, AML, and GDPR regulations. Jumio serves a broad range of industries including banking, healthcare, and travel, with a focus on scalable, secure identity assurance.

Why worth watching: Jumio's advanced AI capabilities and global footprint make it a leading provider for organizations seeking robust, automated identity verification across diverse regulatory landscapes.

Nametag

Nametag was founded in 2020 and is headquartered in Seattle, Washington. Nametag provides identity verification purpose-built for security-critical account events rather than compliance-driven onboarding. On the workforce side this covers employee and contractor onboarding, helpdesk caller verification, self-service MFA and password resets, and, since the May 2026 launch of Nametag Recruit, candidate verification during hiring. The same verification also protects high-value consumer accounts during customer support and account recovery. Its mobile-first platform combines document and biometric verification with a device-focused security model. Hardware-backed keystores, secure enclave storage, and cryptographic attestation establish that a submission originates from a genuine device, countering deepfakes and injection attacks deterministically rather than through probabilistic

detection alone. Patented techniques such as device re-binding and Selfie Chain support this approach. The platform integrates with identity providers, directories, HR systems, and incident response tools, with partnerships including Microsoft and Okta. Its customer base is primarily in North America.

Why worth watching: Nametag targets a gap that KYC-oriented identity verification vendors leave open: securing workforce and customer account lifecycles, from onboarding to helpdesk and recovery, against deepfake and injection attacks. Its cryptographic device assurance adds a deterministic layer where most of the market relies on detection algorithms alone.

Nomidio

Nomidio was founded in 2019 and is headquartered in Reading, United Kingdom. Nomidio offers cloud-native identity verification and biometric authentication solutions designed with privacy and consent at the core. Its platform supports facial recognition, voice biometrics, and identity-as-a-service capabilities for secure, passwordless access and digital onboarding. Nomidio is built on zero-knowledge encryption principles, ensuring personal data is protected and user-controlled throughout the identity lifecycle.

Why worth watching: Nomidio's privacy-by-design architecture and emphasis on biometric, decentralized identity verification position it as a forward-thinking vendor in the evolving landscape of digital trust and secure access.

Microsoft

Microsoft was founded in 1975 and is headquartered in Redmond, Washington. Microsoft Entra ID, formerly known as Azure Active Directory, is an identity and access management solution designed to secure user and workload access across cloud and on-premises environments. Within the Entra product family, Microsoft is advancing Decentralized Identity through Entra Verified ID, a standards-based solution that enables organizations to issue, request, and verify digital credentials in a user-controlled, privacy-preserving model.

Why worth watching: Microsoft Entra's push into decentralized identity positions it at the forefront of the shift toward verifiable, portable digital credentials.

OARO

OARO was founded in 2017 and is headquartered in Halifax, Nova Scotia, Canada. OARO provides digital identity verification and access control solutions that leverage blockchain technology, facial recognition, and secure credential issuance. Its platform supports identity verification across sectors including aviation, healthcare, and professional sports, offering both remote and on-site authentication capabilities. OARO emphasizes privacy, data integrity, and interoperability in its identity services.

Why worth watching: OARO's integration of blockchain with biometric identity verification creates a tamper-resistant, high-trust framework for secure digital interactions across regulated industries.

Prembly

Prembly was founded in 2021 and is headquartered in Lagos, Nigeria. Prembly's flagship product, IdentityPass, offers real-time identity verification, biometric authentication, and compliance tools tailored to the unique regulatory and infrastructural challenges of African markets. The platform supports ID document validation, facial recognition, and data source verification across multiple African countries, empowering businesses to securely onboard users and detect fraud. IdentityPass is built to scale with APIs and dashboards that simplify KYC, AML, and user risk assessment.

Why worth watching: Prembly's focus on building inclusive, infrastructure-aware identity solutions positions it as a critical enabler of secure digital access and compliance across rapidly growing markets in Africa.

ProofID

ProofID was founded in 2014 and is headquartered in Manchester, United Kingdom. ProofID specializes in IAM solutions, offering managed services and custom integrations built around leading platforms such as Ping Identity. Its capabilities include identity verification, access governance, and secure federation across cloud and hybrid environments. ProofID serves enterprises in finance, healthcare, and government, helping them navigate complex regulatory and security requirements.

Why worth watching: ProofID's expertise in identity orchestration and its strategic partnerships make it a key player in delivering tailored, enterprise-grade identity verification and access solutions.

Prove

Prove Founded in 2008 and headquartered in New York, Prove is a digital identity verification and authentication company that offers phone-centric solutions to help businesses reduce fraud and enhance user experience. Its platform leverages mobile phone signals and behavioral data to verify identities without requiring traditional methods like document uploads or biometric scans.

Why worth watching: Given the increasing importance of secure and user-friendly identity verification in digital transactions, Prove's solutions are relevant for organizations seeking to enhance their authentication processes.

ShareID

ShareID was founded in 2020 and is headquartered in Paris, France. ShareID provides a privacy-preserving identity verification solution that links a user's real identity to their digital interactions using real-time, biometric re-authentication. The platform enables passwordless login and consent-based identity sharing, ensuring that verified identities remain secure and under user control. ShareID supports use cases in finance, healthcare, and digital services, emphasizing compliance with GDPR and other data protection regulations.

Why worth watching: ShareID's unique approach to persistent identity verification through live biometric checks positions it as an innovative force in building trust and security in ongoing digital engagements.

Shufti

Shufti was founded in 2017 and is headquartered in London, United Kingdom. Shufti offers a global identity verification platform that includes services such as ID document verification, facial biometrics, liveness detection, address verification, and AML screening. The platform supports over 150 languages and verifies identities across more than 195 countries and other territories, enabling businesses to meet KYC and compliance requirements at scale. With AI-driven automation and a flexible API, Shufti serves industries including finance, crypto, healthcare, and travel.

Why worth watching: Shufti's global coverage, multilingual support, and customizable verification workflows make it a strong contender for organizations seeking scalable, real-time identity verification across international markets.

Smile Identity

Smile Identity was founded in 2017 and is headquartered in Lagos, Nigeria, and San Francisco, California. Smile Identity provides identity verification and biometric authentication solutions specifically designed for African markets, supporting ID document verification, face matching, liveness detection, and government database checks. The platform integrates easily with mobile and web apps and is optimized for low-bandwidth environments, ensuring accessibility across urban and rural regions. Smile Identity partners with fintechs, banks, and mobile operators to help them comply with KYC and AML regulations while expanding digital access.

Why worth watching: Smile Identity's deep regional expertise and infrastructure-aware technology make it a leading provider for scalable, inclusive digital identity verification across Africa's rapidly growing economies.

Toppan iDGate

Toppan iDGate is a subsidiary of Toppan Inc., a Japanese multinational founded in 1900 and headquartered in Tokyo, Japan. Toppan iDGate offers advanced identity verification and

authentication solutions, including biometric facial recognition, document verification, and secure mobile identity services. Its platform emphasizes user privacy, data integrity, and regulatory compliance, supporting applications in finance, telecommunications, and government services. Toppan iDGate provides secure, real-time identity validation across digital and physical channels.

Why worth watching: Toppan iDGate's fusion of strong biometric security with Japan's rigorous data protection standards positions it as a trusted vendor for high-assurance identity verification in regulated markets.

Trustmatic

Trustmatic was founded in 2021 and is headquartered in Tallinn, Estonia. Trustmatic provides AI-driven identity verification solutions that include ID document authentication, facial biometrics, and liveness detection, tailored for mobile-first and low-bandwidth environments. Its platform supports user onboarding with real-time verification and integrates via SDKs and APIs. Trustmatic emphasizes compliance with global KYC and AML regulations while delivering frictionless user experiences across fintech, telecom, and digital services.

Why worth watching: Trustmatic's mobile-optimized, AI-first approach makes it a compelling choice for businesses seeking scalable, secure identity verification in both emerging and developed digital ecosystems.

uqudo

uqudo was founded in 2012 and is headquartered in Dubai, United Arab Emirates. uqudo provides digital identity verification solutions tailored to the Middle East and Africa, offering services such as facial recognition, liveness detection, ID document verification, and eKYC compliance. The platform integrates national identity systems and supports Arabic script, enabling fast, secure onboarding across financial services, telecom, and government sectors. uqudo also embraces decentralized identity standards to empower users with control over their personal data.

Why worth watching: uqudo's region-specific capabilities and support for government grade identity integration positions it as a key enabler of secure digital transformation in emerging markets.

Veratad Technologies

Veratad Technologies was founded in 2002 and is headquartered in Teaneck, New Jersey. Veratad provides identity verification and age verification solutions designed to support compliance, fraud prevention, and secure customer onboarding. Its platform includes tools such as ID document verification, biometric authentication, knowledge-based authentication (KBA), and real-time data source checks. Veratad serves industries including finance, healthcare, gaming, and e-commerce with configurable, privacy-conscious solutions.

Why worth watching: Veratad's blend of traditional and emerging verification methods offers businesses flexible, compliant identity solutions adaptable to both regulatory requirements and user experience expectations.

Veriff

Veriff was founded in 2015 and is headquartered in Tallinn, Estonia. Veriff offers AI-powered identity verification services including document authentication, biometric facial recognition, and liveness detection to support secure digital onboarding. Its platform is designed for high scalability and accuracy, serving clients across fintech, mobility, healthcare, and the gig economy. Veriff emphasizes global coverage, GDPR compliance, and fraud prevention through continuous AI model training and risk analysis.

Why worth watching: Veriff's commitment to automation, global reach, and fraud detection positions it as a leading identity verification provider for fast-growing digital-first businesses.

Verimi

Verimi was founded in 2017 and is headquartered in Berlin, Germany. Verimi provides a secure digital identity platform that offers identity verification, electronic signatures, and data wallet capabilities, enabling users to authenticate, share, and manage their personal data with full control. The platform is GDPR-compliant and integrates with government and private sector services, making it a trusted provider in finance, healthcare, and public administration. Verimi emphasizes privacy, interoperability, and secure digital interactions in the European identity ecosystem.

Why worth watching: Verimi's user-centric identity wallet and strong alignment with European data protection standards position it as a pivotal player in the trusted digital identity landscape.

Veritrان

Veritrان was founded in 2005 and is headquartered in Buenos Aires, Argentina. Veritrان offers a low-code digital solutions platform that includes identity verification features such as biometric authentication, document validation, and secure onboarding flows. Its platform is designed for rapid deployment and scalability, primarily serving the financial services industry across Latin America and other emerging markets. Veritrان emphasizes user experience, security, and regulatory compliance to support digital transformation in banking and fintech.

Why worth watching: Veritrان's integration of identity verification within a broader low-code development platform makes it a powerful enabler of secure, agile digital experiences for financial institutions.

VU Security

VU Security was founded in 2007 and is headquartered in Buenos Aires, Argentina. VU Security offers identity verification and cybersecurity solutions with a focus on secure digital onboarding, fraud prevention, and identity lifecycle management. Its platform combines biometric verification, document validation, behavioral analytics, and risk scoring to provide comprehensive identity assurance across sectors such as banking, government, and healthcare. VU Security is known for its commitment to Latin American markets, providing localized solutions that meet regional compliance and infrastructure needs.

Why worth watching: VU Security's fusion of identity verification and cybersecurity capabilities positions it as a unique and strategic player in protecting digital identities across high-risk, high-growth environments.

Yes:ID

Yes:ID was founded in 2020 and is headquartered in Paris, France. Yes:ID offers a reusable digital identity solution that enables users to verify and share their identity securely across multiple platforms with a single sign-on experience. The platform uses biometric authentication, ID document verification, and consent-driven data sharing to simplify onboarding while preserving user privacy. Yes:ID is designed to support compliance with GDPR and other data protection frameworks, making it suitable for fintech, e-commerce, and government applications.

Why worth watching: Yes:ID's user-controlled, reusable identity model aligns with the future of decentralized identity, offering businesses a frictionless yet compliant way to verify and engage users.

Related Research

[Leadership Compass: Identity Verification 2025](#)

[Leadership Compass: Provider of Verified Identity 2022](#)

[Leadership Compass: Reusable Verified Identity](#)

[Buyer's Compass: Identity Verification](#)

[Whitepaper: Navigating the Future of Authentication in the Age of AI and Deepfakes](#)

Copyright

© 2026 KuppingerCole Analysts AG. All rights reserved. Reproducing or distributing this publication in any form is prohibited without prior written permission. The conclusions, recommendations, and predictions in this document reflect KuppingerCole Analysts' initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinement or significant changes. KuppingerCole Analysts disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole Analysts' research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole Analysts assumes no liability for errors or inadequacies in the information contained in this document. Any expressed opinion may change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole Analysts offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole Analysts 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 technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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