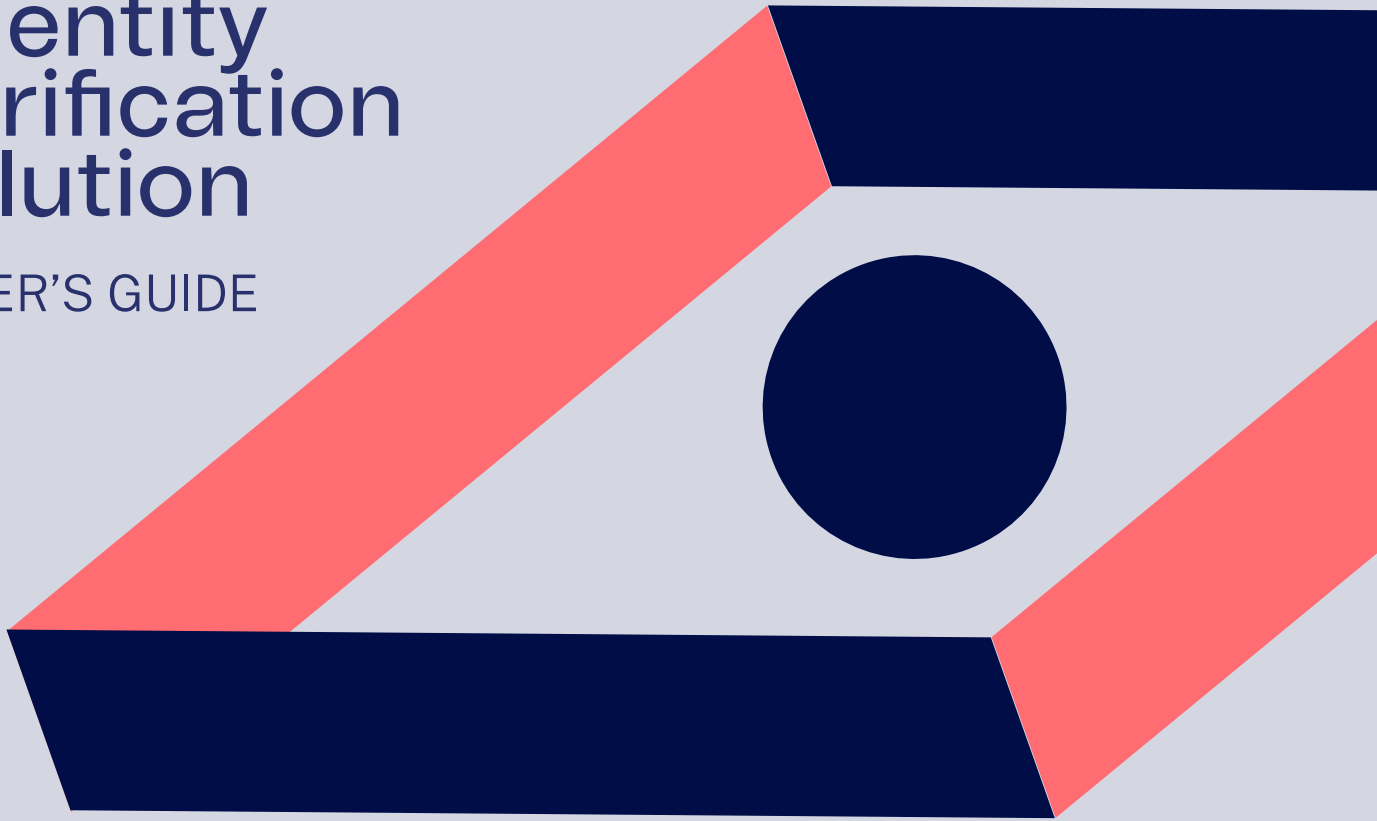


/Identity Verification solution

BUYER'S GUIDE



VeriDas

/INDEX

- /The Challenges of Choosing the Right IDV Solution** 03
- /The business impact of IDV** 04
- /Fraud is Expensive. Identity Verification isn't** 05
- /Identity Verification: Everyone's Business** 06
- /Why Identity Verification Matters** 07
- /ID Document Verification** 08
- /Face Biometric Verification** 10
- /Liveness Detection** 12
- /Fraud Shields & Security Layers** 14
- /User Experience & Accessibility** 17
- /Deployment Options** 20
- /Identity Management & Analytics** 22
- /Integration & Flexibility** 24
- /Add-ons & Compliance Layers** 26

/The Challenges of Choosing the Right IDV Solution

Ask better. Choose smarter.

The IDV market is full of vendors promising fast onboarding, high accuracy, and full compliance. But technology evolves fast. Fraud evolves even faster. And user expectations keep rising.

It's not easy to assess AI models, biometric engines, or fraud protection layers without technical expertise. Most solutions sound similar at first glance, but the differences beneath the surface are critical.

That is why we created this guide. To help you evaluate with clarity and confidence.

How to Use It

This guide breaks down the essential components of an identity verification solution. It explains what matters, why it matters, and what strong solutions typically offer. Use it to:

/Understand the landscape: Start with the business impact and challenges sections to align your internal stakeholders on why IDV matters.

/Evaluate with purpose: Use each chapter to frame what questions to ask vendors — and what great answers should look like.

/Build internal buy-in: Share relevant sections with risk, legal, operations, or product teams to drive aligned decision-making.

/Compare with confidence: Don't just tick boxes — evaluate what makes one solution more adaptable, secure, or scalable than another.

Download the
Evaluation Template



Score providers across all key areas, from compliance and biometrics to UX and fraud prevention.

/The business impact of IDV

Identity Verification it's not just a technical decision.

A strong identity verification solution does more than keep you compliant or block fraud. It improves your bottom line across departments by automating processes, reducing risk, and unlocking new opportunities for growth.

Let's break it down.

Operational efficiency through automation

Manual document checks and identity reviews are slow, inconsistent, and costly. By automating these tasks with AI-powered verification, you reduce time-to-yes, lower labor costs, and free up your team to focus on what matters.

Think about the hours your agents spend reviewing documents or handling onboarding incidents. Automating just part of that process already translates into direct cost savings.

Preventing loss is just as powerful as generating revenue

Every fraudulent account caught by your IDV system avoids potential chargebacks, service abuse, or reputational damage. The more sophisticated the attack — deepfakes, injection attempts, fake identities — the more valuable it is to catch early.

One blocked fraud attempt could mean saving thousands. Now multiply that across a month, a year, a market.

Remove friction, gain more customers

Complex or slow verification flows lead to abandonment. A smooth, mobile-friendly user experience increases your conversion rates, enabling acquisition through digital channels and across geographies.

What would a 5% increase in verified users mean for your revenue? Or a 20% drop in abandonment during sign-up?

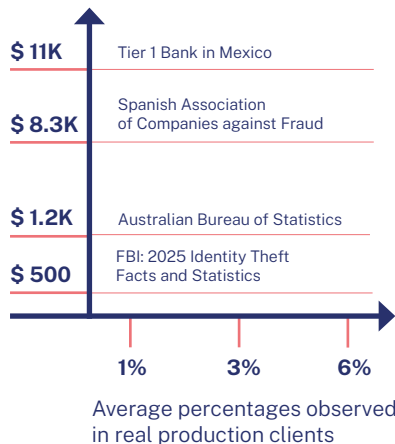
/Fraud is Expensive. Identity Verification isn't.

See the ROI in weeks. Feel the impact immediately.

Identity fraud is no longer a threat, it's a daily reality costing millions.

Banks, utility companies working to fight face fraud 

Average losses per fraud case



Real-time identity verification not only stops fraud – it saves time and money.

Number of processes per year	100.000
Estimated percentage of fraudulent cases	3%
Estimated losses per fraud case	\$4.000
Annual Economic Impact of Identity Fraud	\$12.000.000
Annual Investment in Veridas Solution against Fraud	\$52.000,00
Return on Investment (ROI)	22977%
Payback period in weeks	1 week(s)

/Identity Verification: Everyone's Business

The real impact of IDV across departments.

Every team benefits from a well-implemented identity verification solution.

Here's how:

FINANCE AND OPERATIONS TEAMS

Reduce internal costs, improve process control

Automated verification lowers manual workload and accelerates back-office workflows. Better traceability and audit logs support compliance and reduce SLA breaches.

FRAUD AND RISK TEAMS

Stay ahead of evolving threats

Detect not only fake documents, but also advanced fraud techniques like injection attacks, synthetic identities, or deepfakes — with minimal user friction.

PRODUCT AND GROWTH TEAMS

Increase conversions and unlock new channels

A seamless IDV flow improves user experience, reduces drop-offs, and enables remote or self-service onboarding — critical for scaling.

COMPLIANCE AND LEGAL TEAMS

Stay compliant, reduce legal risk

Whether it's GDPR, BIPA, AML, or eIDAS — a certified IDV provider helps you meet global and local regulations with confidence and traceability.



/Why Identity Verification Matters More Than Ever

Digital identity is the foundation of trust in today's online world.

Whether you're opening a bank account, renting a car, or signing up for a telecom service, businesses need to know — with certainty — that the person on the other end is who they claim to be.

That's where Identity Verification (IDV) comes in. What once was seen as a regulatory requirement has now become a strategic asset. A strong IDV solution doesn't just prevent fraud — it unlocks growth, improves user experience, and builds long-term trust with your customers. With cybercrime costs rising and fraud methods becoming more sophisticated, IDV is no longer optional — it's essential.

/ID Document Verification

The first layer of trust in any IDV process

At the core of digital identity verification lies the ability to accurately assess an official identity document — whether it's a passport, ID card, driver's license, or residence permit. This is often the first interaction a user has with your IDV flow, and the moment where trust is either built... or lost.

Effective document verification is not just about reading what's on the surface. It's about validating the document's authenticity, extracting data accurately, and doing so quickly and seamlessly — across geographies, document types, and device conditions.



/ID Document Verification

The first layer of trust in any IDV process

Why It Matters

Fraudsters often exploit weaknesses in document verification. Fake, manipulated, or stolen IDs are one of the most common entry points for identity fraud — and if they slip through, the consequences downstream (from financial loss to regulatory breaches) can be serious.

At the same time, users expect a smooth onboarding experience. If your solution requires them to struggle with glare, poor lighting, or clunky capture steps, they'll drop off — and you may lose a legitimate customer.

A strong document verification engine balances both security and usability. It should support a wide range of documents, automatically recognize types and regions, and include built-in mechanisms to detect signs of forgery or tampering.

What to Look For

A strong ID document verification solution should offer broad and up-to-date global coverage — supporting passports, ID cards, driver's licenses, and residence permits from the regions you serve. It should automatically detect the document type without asking the user to choose, and extract all relevant data with high accuracy, even in challenging conditions like poor lighting or low image quality.

Beyond usability, the system must include advanced fraud checks: verifying the logic of printed data, checking MRZ (Machine Readable Zone) consistency, detecting B&W or color photocopies, and identifying signs of photo replacement or tampering.

For an additional layer of trust, some solutions also offer NFC chip reading, allowing the system to compare chip-stored data with what's printed on the document — ensuring even higher levels of authenticity and biometric validation.



/Face Biometric Verification

Proving that the person is who they claim to be

Once a document has been validated, the next critical step is to confirm that the person presenting it is its rightful owner. Face biometric verification does exactly that – by comparing the user's selfie or live image against the photo printed on their ID document.

This step plays a central role in preventing impersonation and synthetic identity fraud.

/Face Biometric Verification

Proving that the person is who they claim to be

Why It Matters

Face biometrics bring powerful security to identity verification — but not all solutions perform equally. A mismatch here can either block legitimate users or allow bad actors through, especially when environmental conditions are far from perfect.

From differences in lighting and facial accessories to changes in appearance over time (glasses, beards, makeup, aging), a robust biometric engine needs to handle real-world variability. And it must do so with speed, accuracy, and minimal friction.

In regulated industries, biometric verification is often required by law or internal compliance frameworks. But even in unregulated environments, it's increasingly used to reduce fraud and create a more secure, streamlined user journey.

What to Look For

An effective facial recognition system should be trained specifically for selfie vs. ID photo comparisons — not just general-purpose biometrics. It must be able to handle a wide variety of skin tones, ages, and conditions, and work well across devices and camera types.

Performance metrics from independent evaluations (like NIST rankings) are essential indicators of quality and reliability. In high-stakes environments, even small differences in accuracy can have major consequences.

Beyond matching, biometric verification should be tightly integrated with other security layers (like liveness detection and anti-spoofing) to ensure the image being analyzed is real and current — not a photo or video of someone else.

/Liveness Detection

Ensuring there's a real,
live person behind the screen

Face matching alone isn't enough. In today's fraud landscape, attackers use printed photos, videos, deepfakes, and even 3D masks to trick biometric systems. That's where liveness detection becomes essential — it verifies that the user is a real person, present in real time, and not a spoof.

This technology acts as a safeguard against increasingly sophisticated fraud tactics — and is often a compliance requirement for regulated digital onboarding processes.



/Liveness Detection

Ensuring there's a real,
live person behind the screen

Why It Matters

Spoofing attacks are evolving quickly. Fraudsters can now use AI-generated faces, synthetic identities, and hyper-realistic masks to pass weak biometric checks. Without robust liveness detection, even high-performing facial recognition engines can be fooled.

Beyond the threat of fraud, there's also a user experience trade-off. If liveness detection is too complex or intrusive, users may abandon the process. If it's too permissive, security is compromised. Striking the right balance is critical.

In many industries — especially in finance and telecommunications — liveness detection is required to meet anti-money laundering (AML) and KYC regulations. But even when it's not mandatory, it's quickly becoming the norm in any serious identity verification strategy.

What to Look For

Modern IDV solutions typically offer active or passive liveness detection — or both.

/Active methods ask the user to perform actions (like turning their head or blinking). These are often considered more secure, but may slightly increase friction.

/Passive methods analyze the image or video automatically, without requiring user interaction — providing a smoother experience while still blocking basic attacks.

Top-tier systems are evaluated against global standards, such as ISO 30107 and iBeta Levels 1 and 2, which test a provider's ability to detect a wide range of presentation attacks — from replayed videos to silicone masks.

It's important that liveness detection works consistently across platforms (web, mobile, native apps) and under different lighting, camera, and connectivity conditions. Seamless integration with biometric matching is also key for streamlined flows and stronger security.



/Fraud Shields & Security Layers

**Protecting the full identity journey
— not just one step**

Identity fraud is no longer limited to fake documents or spoofed selfies. Today's attackers exploit every possible weak spot in the identity verification flow — and they're using advanced tools to do it.

Modern threats go beyond what the user sees. While document and biometric checks are essential, they must be reinforced by security mechanisms that operate behind the scenes — capable of detecting injection attacks, deepfakes, virtual devices, and other invisible manipulations.

/Fraud Shields & Security Layers

Protecting the full identity journey
— not just one step

Why It Matters

Fraudsters now operate like professionals — using automation, emulated environments, and deepfake technologies to bypass standard checks. Two of the most dangerous methods are injection attacks and advanced injection attacks, which differ in both approach and impact:

Injection Attacks

These involve inserting fake media (like pre-recorded selfies or videos) into the system — not through a real camera, but by hijacking the data flow. The system “thinks” it received a real-time video or image, when in fact it was fed altered content.

Advanced Injection Attacks

These go even further. Here, attackers emulate entire devices or environments (like using a virtual machine or a custom app) to bypass every layer of protection. They can simulate user behavior, modify runtime conditions, and execute complex fraud at scale — making detection incredibly difficult without specialized protections.

Both forms of attack are dangerous — but advanced injection attacks are particularly threatening because they can be automated and deployed on a massive scale, often without triggering obvious red flags.

/Fraud Shields & Security Layers

Protecting the full identity journey
— not just one step

What to Look For

An effective IDV platform should offer layered protection that addresses both standard and advanced fraud techniques, including:

Virtual camera detection: Identifies when images or videos are injected, not captured in real time.

API misuse prevention: Blocks unauthorized access to backend services via rogue integratio

Emulated device detection: Flags virtual or tampered environments that mimic real phones or browsers.

Runtime analysis: Detects if dev tools or debugging software are active during the process.

Deepfake detection: Uses AI to identify synthetic content — including faces, voices, or movements.

Behavioral anomalies: Spots bot-like activity, repeated patterns, or suspiciously fast interactions.

These layers often work silently in the background — but they're essential to prevent fraud that would otherwise go undetected. A secure IDV solution should evolve constantly to stay ahead of emerging attack vectors.

/User Experience & Accessibility

**Frictionless flows for real people,
on real devices**

A strong identity verification process should feel almost invisible to the user. Fast, clear, and intuitive — that's what builds trust and drives conversion. Whether onboarding a new customer or verifying a returning user, the experience needs to be smooth across all platforms, devices, and connectivity conditions.

But great UX isn't just about looking good. It's about accessibility, adaptability, and performance — especially in a global context where users may have limited technical literacy or lower-end devices.



/User Experience & Accessibility

**Frictionless flows for real people,
on real devices**

Why It Matters

Every extra second in the IDV flow increases the risk of user drop-off. Poor lighting, confusing instructions, unsupported devices, or errors during capture can cause frustration and abandonment — even from legitimate users. And if the process feels invasive or untrustworthy, users may hesitate to proceed at all.

At the same time, accessibility is a growing concern. Users may access your service through a wide range of operating systems, browsers, and network conditions — and they all expect the same: speed, clarity, and security.

For high-volume onboarding or time-sensitive processes, the impact is clear: better UX = higher conversion, fewer support tickets, and stronger engagement.

/User Experience & Accessibility

Frictionless flows for real people,
on real devices

What to Look For

A user-centric IDV solution should be built with real-world conditions in mind:

Browser and device compatibility:

Full support for major web browsers and native mobile platforms, including older OS versions and lower-end devices.

Adaptive capture flows:

Automatic guidance for document and selfie capture — helping users align, focus, and adjust in real time without needing to “figure it out.”

Customization & branding:

Flexible UI options that allow you to adapt the look, language, and tone to your brand — ensuring consistency and trust throughout the journey.

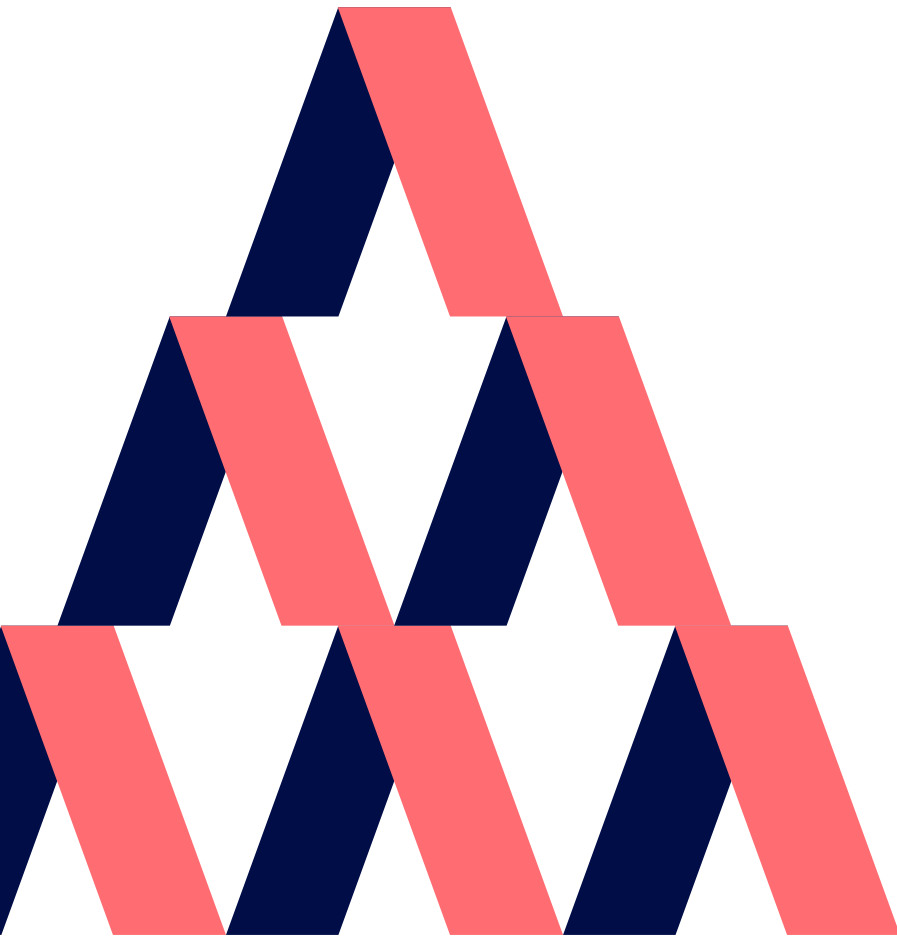
Offline-ready or low-bandwidth modes:

Options that ensure usability even in markets with unstable connections.

Support for diverse use cases:

Whether it's remote onboarding, assisted registration, or self-service kiosks — the UX should adapt to your operational model.

The goal is to make the IDV process feel intuitive — so users don't think about it. When it's done right, users get verified in seconds and move on. When it's done poorly, they leave — or worse, call support.



/Deployment Options

Scalable solutions that fit your infrastructure

Behind every user-facing identity verification flow is a deeper question: where does it run, how is it managed, and who controls the data?

Deployment matters — not just for performance and scalability, but for compliance, integration, and long-term maintainability. Whether you operate in a highly regulated industry, require full data control, or simply want fast time-to-value, the way an IDV solution is deployed can make a major difference.

/Deployment Options

Scalable solutions that fit your infrastructure

Why It Matters

Some organizations prefer cloud-based solutions for their speed, scalability, and ease of updates. Others — especially in government, finance, or defense — may need full control via on-premise deployments due to strict data residency or infrastructure requirements.

Each approach comes with trade-offs. Cloud deployments typically offer faster setup, better monitoring, and continuous improvement. On-premise installations can offer tighter control, but may involve longer integration times, more manual maintenance, and limited scalability.

Choosing a provider that offers flexibility — and understands the nuances of both models — is essential to ensure your IDV stack aligns with your business and regulatory needs.

What to Look For

Behind every IDV process is a bigger question: where does the system run, how is it maintained, and who controls the data?

For many, cloud deployment offers the fastest path to value. It simplifies integration, ensures continuous updates, and allows you to scale effortlessly. Look for providers that operate on trusted cloud platforms — like AWS or Google Cloud — and offer clear SLAs, real-time monitoring, and secure data isolation between clients.

But some sectors require more control. In industries with strict data residency or security policies, on-premise deployment may be necessary. If that's your case, check how the provider handles maintenance, updates, and scalability in self-hosted environments — as on-prem setups can be harder to operate long-term.

Also consider resilience. Does the platform support backup and disaster recovery? Can it trigger alerts in case of anomalies? Are logs centralized and accessible to your tech team?

Your deployment model should align with your internal policies and compliance obligations — without compromising performance or user experience.

/Identity Management & Analytics

**Visibility, control, and insights
for every process**

Capturing and verifying a person's identity is just the beginning. What happens after the verification — where that data goes, how it's reviewed, and how it's used — is just as important.

A modern IDV solution should provide centralized tools for managing identity data, reviewing verification outcomes, and generating insights. This helps not only with compliance, but also with operational efficiency, fraud detection, and funnel optimization.

VeriDas



/Identity Management & Analytics

Visibility, control, and insights for every process

Why It Matters

Without centralized identity management, organizations are left piecing together verification evidence from different tools or providers — increasing the risk of data loss, duplication, or inconsistency. In regulated industries, this lack of visibility can also create legal exposure, especially when audits or reporting are required.

On the operational side, teams need to quickly review and validate edge cases — whether due to low-confidence results, flagged documents, or user errors. Without a clear view into what happened during the verification process, agents can't act confidently, and fraud can slip through.

Finally, analytics are key. Understanding how many users convert, where they drop off, and how each step performs allows organizations to optimize onboarding and reduce friction — without compromising security.

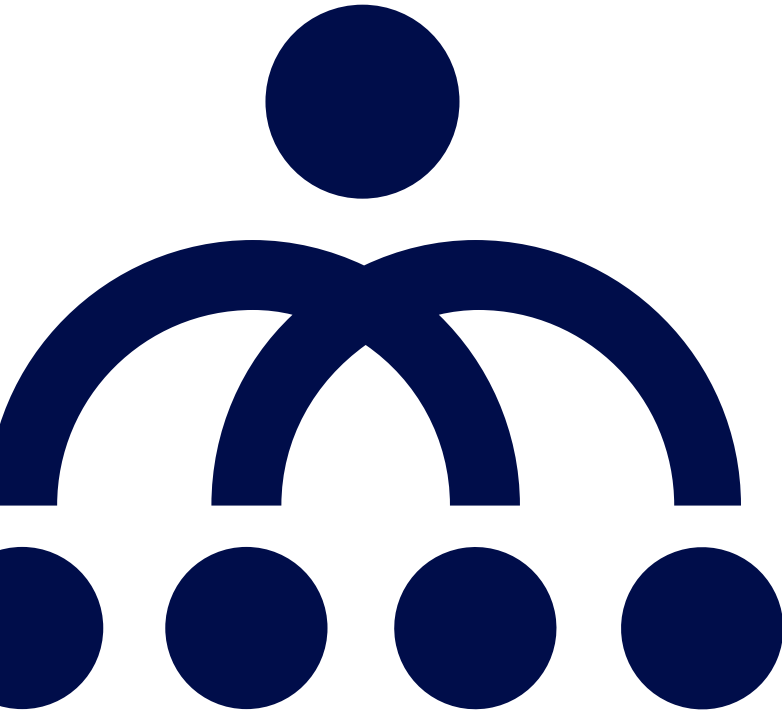
What to Look For

Once an identity is verified, managing that data effectively becomes just as important as capturing it. The best IDV solutions offer a centralized dashboard where you can monitor every process in real time — from verification volumes and success rates to error patterns and funnel drop-offs.

This visibility isn't just for analytics — it's operational. Your teams should be able to drill into individual verifications when needed: review images and evidence, validate low-confidence cases manually, and track how long each step took.

Governance also plays a key role. Make sure the system allows you to define roles and permissions for your internal users. Not everyone needs access to everything, and compliance often depends on being able to control (and track) who can view or export identity data.

More than a back-office tool, a solid identity management layer is a strategic asset — giving you the clarity to optimize, the control to comply, and the evidence to act.



/Integration & Flexibility

Make it yours — wherever and however you need it

Even the most advanced identity verification system won't deliver value if it can't be integrated smoothly into your environment. Every business has its own systems, workflows, and user journeys — so flexibility in how IDV is implemented is key.

From full plug-and-play solutions to highly customized API-based integrations, a modern IDV platform should adapt to your architecture — not force you to adapt to theirs.

/Integration & Flexibility

Make it yours — wherever and however you need it

Why It Matters

Speed of integration directly impacts time-to-value. If setting up the IDV solution takes months or requires heavy development, it delays your ability to launch, iterate, and generate results.

But it's not just about speed. Integration defines how much control you have over the user experience, what data you can capture or store, and how IDV fits into your backend processes (like CRM, KYC checks, fraud platforms, or analytics tools).

Whether you're embedding verification into a mobile app, enabling cross-platform onboarding, or creating complex identity flows across multiple systems, the flexibility of the integration model can make or break the project.

What to Look For

Every business has its own architecture — so integration should never be one-size-fits-all.

If you're looking for speed, a plug-and-play solution might be ideal: minimal configuration, fast setup, and a pre-built flow that gets you to market quickly. But if control is more important — over the capture process, user experience, or data handling — SDKs are the way to go. They let you embed the IDV experience into your own apps or platforms, with flexible customization.

And then there's full API integration: perfect for advanced teams who want to handle capture independently and send media directly to the verification engine. This approach gives you total freedom to build complex, multi-step flows or integrate with multiple backend systems.

Whatever your level of customization, make sure your provider supports both mobile and web environments — including edge cases like hybrid apps, offline capture, or low-connectivity regions. And don't overlook the basics: clear documentation, sandbox environments, and responsive tech support make all the difference during and after integration.

/Add-ons & Compliance Layers

Completing your IDV strategy with the right extras

Every organization has unique compliance requirements, risk profiles, and customer workflows. While the core of identity verification covers document and biometric checks, many real-world use cases demand more – whether it's electronic signatures, AML screening, or assisted validation.

That's where add-ons and compliance layers come into play. These optional modules can enhance your IDV stack, making it more secure, more compliant, or more aligned with specific business processes.



/Add-ons & Compliance Layers

Completing your IDV strategy with the right extras

Why It Matters

In many sectors, identity verification is only part of a larger compliance process. For example, in financial services, you may need to screen users against sanctions lists or perform video-based verification to meet local anti-money laundering (AML) laws. In government or public sector contexts, identity checks may need to match against official databases.

On the operational side, having tools like assisted review panels or biometric electronic signatures can streamline internal processes, reduce manual effort, and ensure legal defensibility in case of disputes or audits.

Choosing an IDV solution that supports these extensions — and integrates them smoothly — allows you to grow your capabilities without adding new vendors or reworking your existing flows.

/Add-ons & Compliance Layers

Completing your IDV strategy with the right extras

What to Look For

The right add-ons depend on your sector, geography, and risk level — but some common high-impact options include:

Electronic signatures: Generate legally binding biometric signatures during the onboarding process, tied to the verified identity.

Video verification (selfie or call):

Required in certain jurisdictions to comply with AML regulations — especially when opening financial accounts remotely.

PEPs & Sanctions screening:

Run automated checks against global watchlists as part of your KYC process.

Assisted back-office tools:

Allow agents to manually review edge cases with full access to captured evidence and decision history.

Government database checks:

Validate ID data against official registries (where legally authorized), adding another layer of assurance.

24/7 support & monitoring:

Especially important in high-volume or high-risk environments, where downtime or delayed troubleshooting isn't an option.

The ability to selectively activate these services — and adapt them to each use case — ensures your IDV setup remains lean, compliant, and ready for growth.

VeriDas

veridas.com