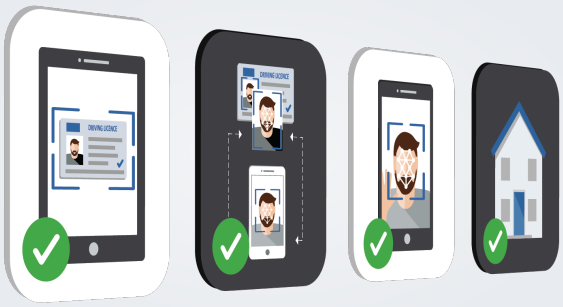
ID-Pal's Multi-Layered Verification Delivers Industry-Leading Outcomes

ID-Pal's customer on-boarding journey is not only frictionless, but it delivers industry-leading accuracy in identity verification outcomes. This accuracy is achieved using a series of best-of-breed verification technologies that work together to answer the below questions:

- Has the Identity Document been tampered or forged in any way?
- Is the person submitting the document the rightful owner of the document?
- Does the verified identity match a verified address?

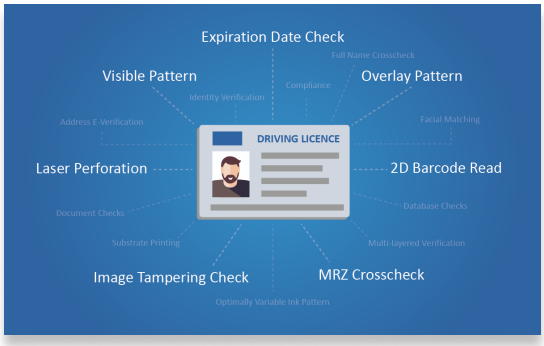
Here we take a closer look at the technologies that answer these questions.

- Document Verification
- Facial Matching
- Liveness Testing
- Address E-Verification



What is Document Verification?

Document verification is the process of verifying that a document submitted for identity verification purposes has not been forged or tampered with. The ID-Pal platform submits every Identity Document to a suite of rigorous technical checks to confirm that it is authentic.



Up to 70 checks are performed per document, with many authentication tests comparing the data from two or more data sources (human-readable and machine-readable) to verify that they match. The visible and machine-readable fields are crosschecked, within and across both types of data sources. This document verification process ensures that the facial image used in the Facial Matching technical check has come from an authentic document (see below).

What is Facial Matching?

Facial Matching is the use of technology to compare two facial images. The process maps biometric features in facial images and takes measurements (e.g. the distance between the eyes) in order to determine if the images match (i.e. if the images are of the same person). In the Identity Verification process, facial matching is used to compare the face from an identity document to the face of the person completing the process.

However facial matching on its own is not sufficient for a robust identity verification process as it does not confirm the following 2 factors:

- That the identity document from which the facial image is taken is authentic, such as a Government-issued ID, or
- That the image of the person submitting the information is a real live person (as opposed to a digital or physical photo)

This is why the ID-Pal solution not only conducts a comprehensive 50-point biometric facial comparison, but it blends this with the Document Verification mentioned above and with Liveness Testing.

What is Liveness Testing?

Liveness testing, also known as facial liveness, is a key authentication step in the ID&V process that determines if the face being presented during onboarding is live. This check protects against fraudsters who may try to trick the system by using a digital or physical representation of another individual (e.g. a photo or a video).

By confirming that the person submitting the information is a real live person and by conducting facial matching and document verification, ID-Pal confirms that the person providing the information is present, is the true owner of the documentation and that the documentation is authentic.

ID-Pal has 2 types of Liveness Testing available on the platform:

1. Active Liveness leverages software that detects things such as facial gestures, eye movement and lip movement. This method requires a user to complete an action of some sort to confirm that they are real – e.g. blinking when completing the Liveness step.

2. Passive Liveness does not require the user to complete any action. This type of liveness test can be carried out in a number of different ways, including but not limited to; light exposure variation, micro-movement detection, depth measurement etc. There are a number of advantages to this method, from both a user experience and security standpoint.

- **Simpler User Experience:** Minimal effort required from the end user makes the process simpler and more convenient, resulting in more customers completing the onboarding process.
- **More Secure:** The fact that this method can be carried out in a number of different ways makes it harder for fraudsters to succeed at tricking the system as they do not know which technique is in place, making this method typically more secure than Active Liveness.
- **Speed:** Passive Liveness tends to be faster than Active solutions.

iBeta Certification

ID-Pal's Passive Liveness software is iBeta quality assured. iBeta Quality Assurance is a uniquely accredited third-party biometrics testing lab and works with a wide variety of biometric technology companies to ensure their products function to the highest standards. iBeta Quality Assurance has received a Mastercard accreditation for its biometrics test lab.

The approved scope of the independent testing facility includes biometrics testing for mobile and wearable devices using the modalities of facial recognition, palm recognition, voice recognition, and fingerprint recognition.

What is Address E-Verification?

Address E-Verification is available through the ID-Pal platform. This additional level of fraud protection leverages database-matching, where the individual's Name and Address is extracted from the onboarding information and verified against multiple databases to confirm that there is one clear, Full Address Match.

Not only does this Enhanced Verification provide stronger fraud protection for your business, but the customer journey becomes even simpler as they no longer need to submit a Proof of Address document.

Read More about how our Address E-Verification works here.

See how our 'Unique Blend of Document and Database Checks Delivers Real-Time Address & Identity Verification' - Read now.

Multi-layered Verification for Advanced Accuracy

The unique blend of the above 4 technical checks provides businesses with strong, multi-layered verification of an individual's identity, whilst keeping the journey seamless for customers. This robust approach results in the vast majority of customers being verified in real-time, with flagged submissions diverted to a dedicated Alerts section of the business portal.

Auto-diversion of potentially risky submissions allows the back-office compliance team to concentrate on the submissions that need it most. Using the portal workflow they can review and manage each submission, ensuring a timely and effective exceptions handling process.