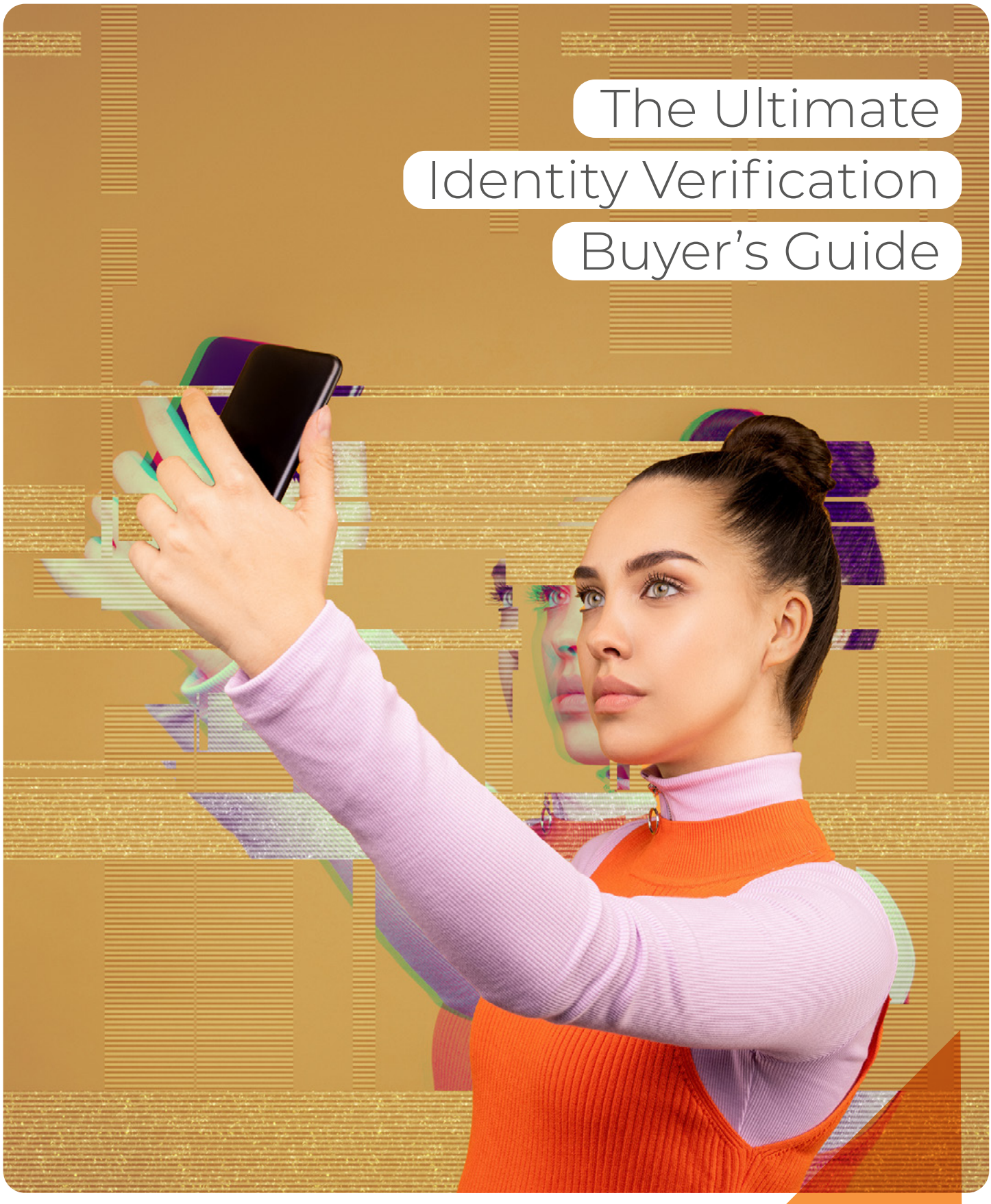
PXL VISION

The Ultimate Identity Verification Buyer's Guide



The Ultimate Identity Verification Buyer's Guide

Everything you wanted to know about identity verification for your business.

Written by: **Karim Nemr, Daniel Long & Michael Knip**

Table of Contents

Welcome

As there is no one-size-fits-all approach to online identity verification, we have written this **Buyer's Guide** to assist businesses at the beginning of their journey in purchasing an identity verification solution.

We understand that the identity verification industry can sometimes be complex to navigate, especially as competing vendors make loud and occasionally unsubstantiated claims to the merits of their products and solutions. That's why we are committed to providing an open & transparent look inside the buyer's journey. This guide sketches every step of the purchasing process. You will receive insights into all aspects of providing identity verification to your own customers.

This guide's sections detail the overall identity verification process, the proven technologies to be aware of, relevant use cases to focus on, and the regulatory and jurisdictional hurdles that can affect your business.

When making a purchase decision, clarity on which software solutions and technologies work best for different requirements is vital. With the content in this document, you will be empowered to take an informed purchase decission that benefits your company and your customers.

Buyer's Tips

Throughout this guide and in each different section, we will highlight some of the best purchasing practices to help you get the most out of your chosen vendor and solution.

1 Background

Fraud is as old as human civilization itself. A 2018 special report by the London-based *Fraud Advisory Panel* listed fraud as one of human society's greatest threats - defining *fraud* as the "intention to deceive for financial or personal gain." Ever since Homo sapiens emerged 200,000 years ago, there has existed a very human desire to lie and deceive.

The report runs through a short history of fraud in the West.

The report concludes that digital (virtual) fraud has led to the highest volumes of fraudulent losses ever recorded during the 20th and 21st centuries. According to the authors, "Fraudsters look for three things: the chance to remain undetected; speed in committing the crime; and naive or unwary victims. The modern internet age handed them all three, on a plate."

> ***"Fraudsters operate with three main areas in mind: Invisibility, speed & targeting victim naivety."***

The global outlook is just as troubling. Crowe, an Irish accountancy and business advisory firm, publishes one of the few reports that attempts to calculate the total cost of fraud globally. Their 2019 report (PDF) points to more than USD 5 trillion in fraud, which is about 6% of global GDP. Even more alarming, in the 10 years leading up to 2019, fraud losses have increased by more than 50 per cent.

In this ten year timespan, Crowe points to one constant: fraudsters continue to exploit new technology in order to commit fraud. For every new tool that businesses use to combat fraud, fraudsters correspondingly refine their techniques to get around it. Furthermore, one of the stated primary reasons for the continued increase in fraud is that business leaders generally adopt a *reactive* approach to fraud, hoping that it doesn't happen to them. And, if it does, to manage the losses and impact if it happens.

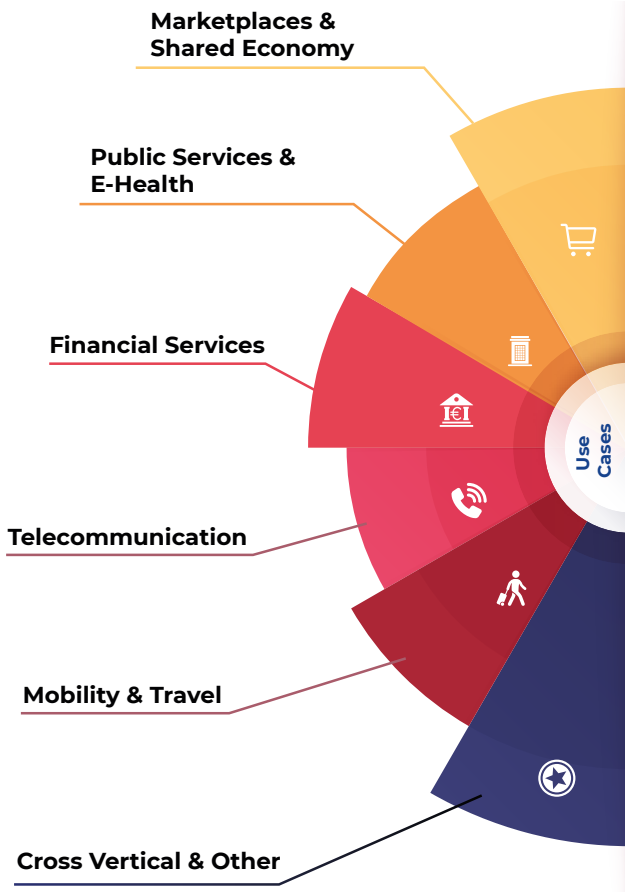
Instead of opting for a reactive approach, the better way of preventing fraud is to use online identity verification. Now, more than ever, businesses need to improve and evolve their customer onboarding processes. As digitalization trends become mainstream, industries as diverse as healthcare, telecommunications and banking are increasingly influenced by global shifts in the way customers transact online, particularly as the economic headwinds of the COVID-19 pandemic continue to disrupt all areas of society.

With the growing risk of fraud and associated cybercrimes impacting your existing and future customers, onboarding processes are also likely to be impacted negatively, if identity verification best practices are not adopted (we will cover more about these practices later in this guide). That's because the growth of any online platform, including the take-up growth of digital products and services, depends on successfully verifying the identity of all users. This process, known as identity verification, confirms there is a real person behind every user, mitigating attacks by scammers and fraudsters who are becoming increasingly sophisticated in their methods of 'spoofing' fake and stolen identities.

When implementing an identity verification solution, make sure to choose a quality vendor that is experienced in fraud prevention and data security. By verifying and authenticating your customers, you can improve the accuracy and security of the onboarding process.

Industries

There are many industries that can benefit from an online identity verification solution. We write about a number of these on our PXL Vision blog. However, for a quick rundown, have a look at the following Industries diagram:



As you can see, there are a variety of industries that benefit from online identity verification. There has been significant growth in online marketplaces & financial services that provide many relevant use cases for identity verification. In contrast, the continued expansion of the telecommunication industry and other key industry verticals provide ample opportunities for online identity verification to bring trust to the digital world.

Today, there are many different solutions and approaches in the market offering identity verification (IDV) software - and sometimes it can all sound and look very similar. However, when a

business considers purchasing an IDV solution, they also need to be very clear about what they want to achieve. This type of buyer planning can make all the difference between a successful implementation and one that leads to a poor user experience.

How to choose the right solution

It's not unusual for businesses to have multiple questions at the start of the buying process. That's why businesses should be aware of differences in vendor approaches and ask the vendor following useful questions:

Questions to answer before making a purchase decision.

- Where will the data be stored after verifying each customer transaction?
- How user-friendly is the solution? How will this affect the conversion-rate?
- How accurate is the solution?
- What certifications does the solution need to meet in terms of data security (GDPR) and industry regulations? Are they met by the solution?
- What is the provisioning model of the solution?

As many online identity verification platforms lack the flexibility to adapt to every business and customer onboarding model, our guide will help to simplify the technical jargon and advise on what works best for your industry, your business and your needs. Whether you‘re a small or large company or just struggling to choose between multiple vendors and an array of similar-sounding products, our guide can help you work out the minor (but equally significant) differences between the various vendors in the industry.

When evaluating the appropriate solution for your automated identity verification needs, it is essential to understand what criteria the verification procedure has to pass to suit your organisation‘s needs. Though the security and reliability of a solution are prominent decision-makers, other lesser factors should not be underestimated. Independent of a suitable solution, we advise to also consider additional characteristics of the vendor before deciding on who to partner with.

There is no single best software solution for identity verification that can serve every need for all organisations. From our experience working with a diverse and large customer base (drawn across many different industries and use cases), we have found that each organisation has its own unique set of requirements and preferences for building out its business-critical processes.

With IDV software, there is usually a trade-off between security, user experience, performance

or other factors important to a business. In our experience solving processes for our customers, we see a general trend in requirements based on verticals and use cases.

Transparency matters

While this provides a high-level overview of the differences between verticals, we have seen that even within the same segment, each organisation has unique needs based on size, the person you talk to, corporate culture and other factors.

To help you answer these questions and provide you with a better understanding of the subject, this guide will explain how identity verification works, what the most common fraud attempts are and what you should be looking for in the ideal solution that matches your own unique requirements.

When you evaluate a vendor solution, try to answer the following questions and be conscious about which factors are most important.

Some of these questions are:

- What is your company size?
- How many verifications will you need each month?
- Do you want an platform-based/mobile or a platform-independent web solution?
- Will you require a cloud or on-premise solution?
- What level of security is the best fit for your business?
- Are there any regulatory rules your industry must follow?
- What type of user experience (UX) do your customers expect?
- How does the vendor ensure a high customer conversion rate?
- How flexible is the solution when it comes to customized branding?
- How experienced is the vendor with projects in your vertical?
- What do the vendor's customers say about the price/performance, reliability and flexibility of the solution?
- Does any government or major institution trust the vendor?
- Is there adequate developer support?
- Where is the data stored?
- What after-sales support does the vendor offer?

This guide intends to help you find the best vendor with minimal trade-offs to suit your individual needs.

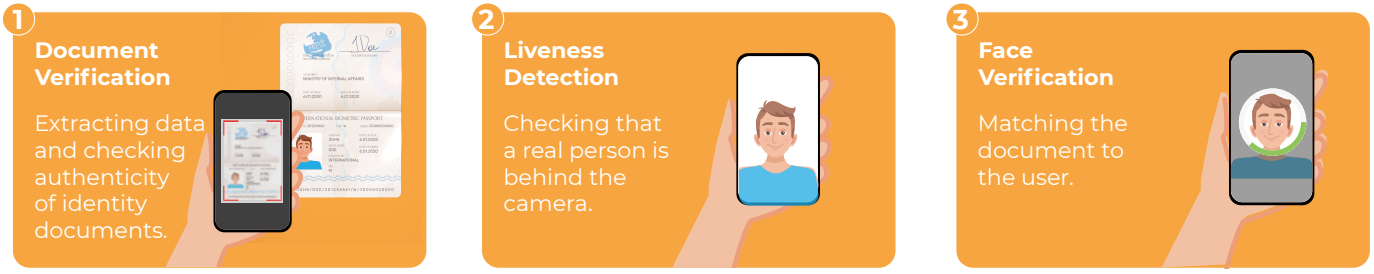
2 How does machine-based identity verification work?

In this section, we take a closer look at the different methods used to verify the identity of users, which industry best practices to be aware of and what you should know before you jump in.

Previous methods of online identity verification were largely based on an imperfect method of humans doing the checking and comparing of user-uploaded photos and government-issued ID documents. Today, the best online ID verification solutions leverage the latest technologies in optical character recognition, computer vision and machine learning to do the heavy lifting.

Machine-learning (ML) algorithms analyse their output and use the result as an input for the next operation. They learn from this data and solve problems that are too complex to calculate with conventional programming - such as matching an individual's real "live" face to a photo.

While there are several online identity verification vendors on the marketplace, each vendor offers their own unique solution with regards to the technologies used. To assess an online identity verification vendor, it is crucial to understand how an ID verification procedure works.



To first verify the identity of a person and their government-issued identity documents, a solution has to: 1) Verify the authenticity of the government-issued identity document; 2) Verify whether a real live person is present; 3) Verify that the submitted document belongs to that person.

Many vendors offer additional, optional functionality to harden the case of the verified identity. By doing so, they enable customers to easily integrate additional steps into their process. Examples are manual verification, residency checks, politically-exposed persons (PEP)-checks or the application of official sanction lists, and many more.

The big difference lies in how different vendors perform the above steps and what impact the method has on the prescribed decision factors, as there can be considerable differences in security, accuracy and user experience.

Document verification

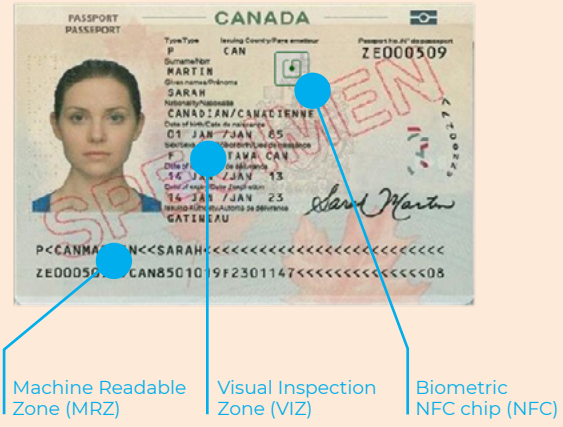
At the core of all identity solutions are the verification of the authenticity of the user's government-issued identity document.
A modern document has numerous built-in security features which an identity solution can check for and verify.

However, document verification presents several challenges. Consider, for instance, passports. Even though the International Civil Aviation Organization (ICAO), a specialized agency of the United Nations, has defined a standard on how international travel documents (i.e. passports) should be structured; there are still hundreds of different passport types and thousands of document types across the globe.

While many international documents adhere to the ICAO standard, there are also many local documents that have their own structure. Even for documents that adhere to the ICAO standard, every country is unique in its design and application of physical security features.

Most documents are designed the following way:

- **Machine Readable Zone (MRZ)**: The MRZ is normally located at the bottom of an identity document and consists of a couple of standardized lines of characters containing the main identity information, such as first name, last name, date of birth etc.
- **Visual Inspection Zone (VIZ)**: The VIZ makes up most of the rest of the document. It contains the document holder's biographical information, photograph, signature, visual security features like holograms and lenticulars and usually some information about the document itself.
- **Biometric NFC chip**: many modern identity documents now have an embedded digital chip. This chip stores biometric information (fingerprints, face scans, etc.) and the additional data found in the VIZ and MRZ.



⚠ To assess the suitability of an identity verification solution, it is important first to identify the behaviour of fraudsters and the most commonly used fraud methods.

Fraud & machine-based document verification

When it comes to fraud detection, solutions in the area of identity verification can differ enormously.

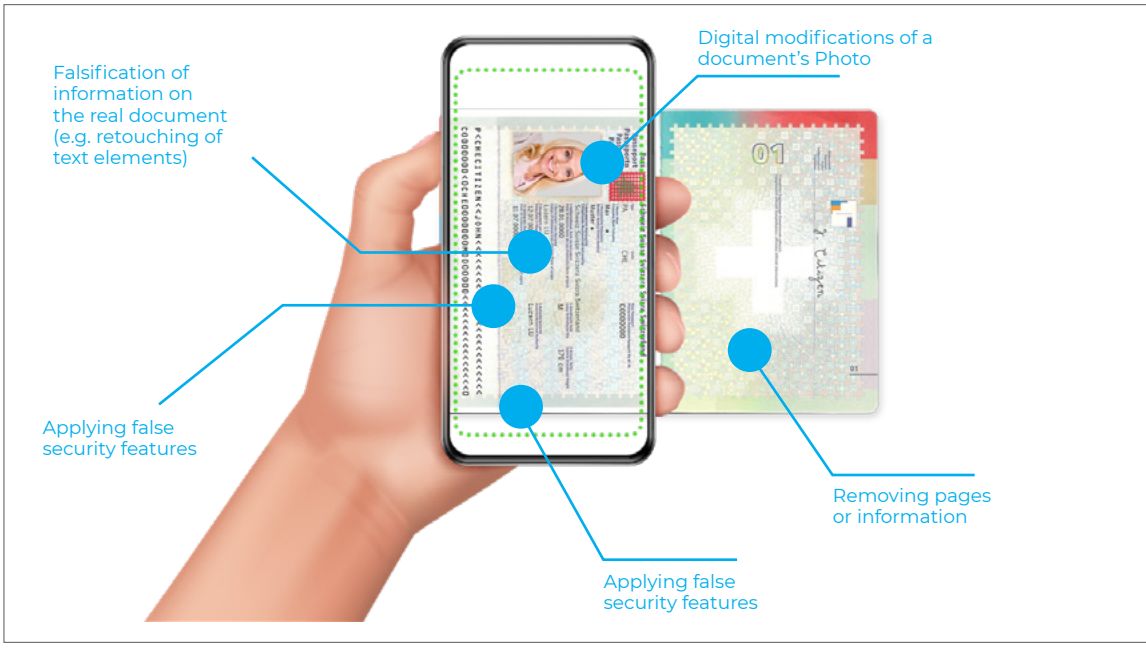
The majority of online identity fraud happens via simple document forgeries and falsifications or amateur attempts (using fake documents or simple falsifications such as glued-on elements). Some high-quality forgeries can only be detected by qualified forensic experts.

There are also highly sophisticated attempts using document blanks & genuine documents with false information, that are almost impossible to detect – even by trained humans and specialized machines.

While a human operator could easily fail the authenticity test in many of these cases, a machine-based verification solution would not.

The most commonly observed fraud attempts in the machine-based verification of identity documents are:

- Falsification of information on the real document (e.g. retouching of text elements)
- Showing pages from two different documents
- Removing pages or information
- Applying false security features
- Digital modifications of a document's photo
- Replacing the document photo
- Completely forged documents
- Stolen blank documents
- Illegally obtained genuine documents
- Fictitious documents from fictitious issuing authorities



The most common fraud attempts used to target machine-based identity document verification.

So what does it take to properly verify an identity document? In our experience, there are five important areas that a solution needs to implement well, in order to get it right:

1. Document image capture

One of the most important factors in document verification is how the source image of a document is captured.

Many solutions simply accept a digital image from any source, asking their users to upload or send a document scan via email. This image is then processed, but chances are high that a verification of such an image will fail since there is no way to influence the image quality for processing.

You may be getting poor quality pictures of documents or pictures of no documents at all, leading to dropouts or the need to repeat the process. Therefore, controlling the capture process and running several checks in real-time while doing the document scans is an important capability.

2. Validation of data integrity

Having a well-developed process for document capture is a precondition for the reliable and secure identity verification process.

With high-quality document images, the document data can be extracted accurately and checked for integrity. Checking the document integrity is one of the most complex areas of document verification and a key differentiator among the solution. This capability (or the lack of it) is a key differentiator of the solutions currently available on the market. There are solutions which simply extract the information from the MRZ, which is a rather straightforward process. However, while the MRZ has a checksum that can be validated, not all fields are included in

Buyer's Tips:

- Capturing a document with a single photo does not allow a reliable check of the security features. Capturing a video sequence is the superior way. A video sequence captures multiple frames, which allows a reliable check of the document's security features.
- Look for a solution that provides live document-capturing during the identity verification process. Images and videos captured outside of the identity verification process are not reliable.
- During the video capture, the solution should prevent removal of a document from camera view and potentially swapped with another document.
- The solution should allow for high resolution capturing to ensure all necessary checks can be carried out.
- The solution should ensure that the capture is not blurred and the entire document must be visible, document edges must not be cut off.
- A good solution will employ a user interface guiding and informing the user about possibilities for improving the resolution and conditions.

the checksum, including the first name and last name of the document holder. Also, there are many documents that do not comply with the ICAO standard for the MRZ. As it is relatively easy to generate a fake MRZ, a proper way of verifying document authenticity is going beyond checking the integrity of the MRZ checksum. An advanced solution also extracts the information from the VIZ and runs additional checks.

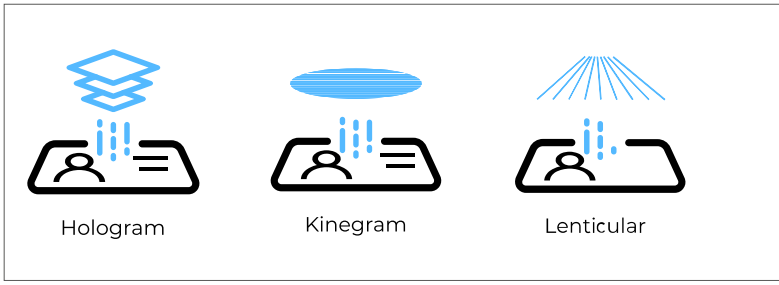
The extraction of the VIZ also comes with multiple challenges. Almost every document type is unique regarding information, structure, font face and font sizes. As a result, ML algorithms need to be specifically trained for accurate extraction of information. When you find a solution that claims a high accuracy, make sure it is transparent what this accuracy actually relates to.

3. Visual authenticity checks

The verification of the biometric NFC chip provides the highest security in document verification today.

However, not every user device has the reading capability and most locally used identity documents, such as driver's licenses or national ID cards don't yet have a chip embedded. Therefore, a vendor's solution needs to perform authenticity checks based on the visual information of the captured document.

Visual authenticity checks are complex. They require sophisticated computer vision and machine-learning technologies to check for visual characteristics, anomalies, and signs of tampering. This is completed by comparing the captured document to a known reference template of the specific document type. This can range from simple template matching, which checks the general look of the documents and finds the data fields in the VIZ to extract information from, to highly sophisticated approaches that compare hundreds of visual key features to the template.



Validation of a document's physical features

Some solutions can also go a step further by validating the structural integrity of specific physical security features, such as holograms, kinegrams or lenticular features.

Buyer's Tips:

- Choose a solution that extracts the data from both MRZ and VIZ.
- Ensure that the solution validates not only the MRZ checksum, but also checks for syntax and logic, and also for non-standard ICAO documents.
- Certain information from the MRZ (e.g. document number, birthday, year of expiry) is compared with the information from the VIZ.
- If available, biometric NFC chip data should be extracted, verified and compared with the MRZ and VIZ data.

These advanced checks are not yet commonly used, as they require deep technical capabilities. An adequate solution needs to be manually trained for each specific document type with actual physical data sets. On the one hand, this makes the approach less scalable. On the other hand, this approach becomes very valuable for custom document types in the context of individual and high-security use cases.

Buyer's Tips:

- Ensure that the vendor's solution applies a so-called "key-feature template-matching" approach, where numerous visual key features (e.g. corners, edges, data fields, background patterns, flags, etc.) are identified and compared with a reference to achieve the highest possible match.
- Even if you might not need this for your own purpose, choose a vendor which can verify the authenticity of physical security features like holograms and lenticulars. Make sure a solution claiming this capability cannot easily be fooled with a piece of shiny, reflective material, such as aluminium foil. Make sure that the solution is capable of checking the structure, the color gradient and the behaviour of the reflection at different angles, corresponding to the reference.
- In the case of lenticular features, stored information (e.g. document number and year of expiry on some documents) can also be extracted and compared with the information from the MRZ. Avoid solutions that claim to check these specific features based on a single image. These kinds of checks need movement of the documents and the analysis of different angles for a reliable result.
- Other checks, such as detecting font and font size anomalies, correct rounding of the document corners, printing colours, etc., are not sufficiently reliable*. If a solution claims to perform these checks, make sure you have certainty regarding their impact on the document verification-result.
- Rather go for a vendor with many years of experience in document verification. Building a reliable solution takes a lot of time and a great number of datasets for training the machine-learning algorithms.
- Numbers can be misleading: Don't just rely on the number of documents a solution supports. There are solutions which claim global coverage with thousands of documents supported. When you dig a little deeper, try to understand to what extent they support all of these documents and what kind of checks they do and what fields they extract.
- A solution may support 3.000 document types but is only accurate at verifying the authenticity of 5. This would, of course, be fine if those 5 happen to be the same document types used in your country. Look for a solution that has very strong technical capabilities for the most important documents for your use case. Rather consider solutions that can easily extend their coverage to support your specific needs.

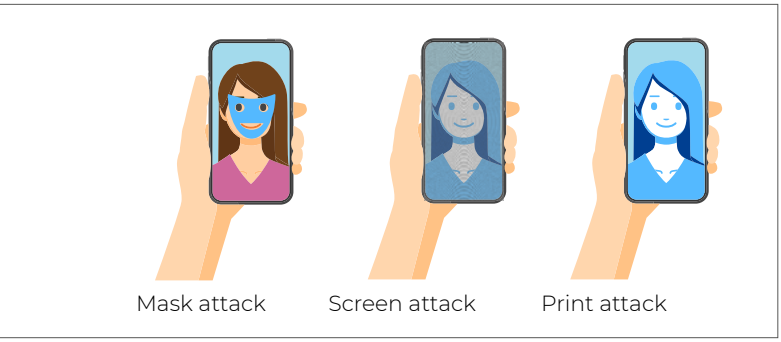
*Source: PXL Vision-internal tests with over 100.000 documents.

4. Liveness detection

All online identity verification solutions are vulnerable to some form of sophisticated presentation attack or fraud.

ID verification solutions need to verify whether or not the person going through the verification process is a real person. Liveness detection solutions help to solve this problem by determining whether the person in front of the camera is real or not. This is critical for ensuring a safe and accurate identity verification for your customers.

In the past few years, fraudsters have continued to find ingenious methods to spoof facial biometrics using a number of different attack methods. Here we differentiate between two types of attacks: those in front of the camera and those behind the camera.



Fraud attacks in front of the camera

For attacks in front of the camera, a 'bad actor' (fraudster) may try to defraud the system by using what is referred to as a presentation attack. The most common methods of a presentation attack involve wearing a professionally designed mask or placing a printed face or a video recording (or rendering) of another person in front of the camera.

Behind the camera attacks usually involve an attack on the server where the liveness detection software is running. Attacks behind the camera are prevented with the highest standards of IT security, data encryption and communication.

Today, malicious hackers constantly devise new technologies and innovative methods to spoof identity verification platforms. Solutions offering a solid liveness module minimize the risk of 'spoofs' or 'presentation' attacks from criminals.

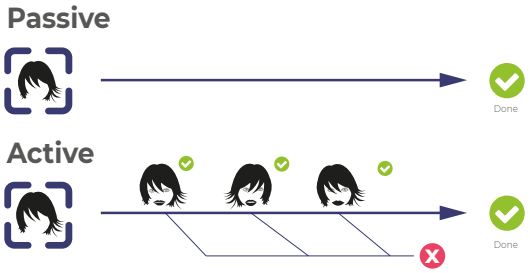
Most solutions offer a liveness detection tool as one of the core technologies behind their identity verification platform. Vendors should be transparent about the liveness technology they use in their solution. Be sure to find out before you sign up to any verification platform.

There are two main liveness technologies available on the market today: Active & Passive. However, there are some significant technological differences between the two liveness options:

Active liveness detection uses a "challenger response" method which requires the end user to follow instructions until they can prove that they are a genuine user in front of the camera. The challenger response instructions are known to lead to user fatigue. For example, a given active liveness solution will instruct users to turn their head in a particular direction: blink, nod or otherwise perform intricate movements so that the software accepts the user's liveness.

Following these instructions (especially when you have to repeat steps) causes some customers to drop out of the process. On the other hand, passive liveness detection uses deep convolutional neural networks with improved depth analysis that analyzes texture and facial appearance.

With passive liveness detection, the process is simplified for the user – boosting conversion and reducing the risk of dropouts. There are no interactions needed, and the user is only required to look into the camera for a few seconds without the need to respond to active challenger instructions. Similar to authenticity checks of documents, liveness detection based on a single image is not sufficient. A 'selfie video' is the preferred method to achieve consistent and accurate results during the liveness check.



Unfortunately, there are still solutions on the market which use the outdated and less secure active liveness detection. Before making a purchase decision on a solution, make sure it uses the more secure and sophisticated passive liveness detection.

5. Facial biometric verification

Biometrics have been used to identify and verify people for many years, and the technology has been applied to fingerprints, irises, voice frequencies and even the way people walk.

Lately, many solutions focus on facial biometrics. Scanning one's face is straightforward. Anyone that has taken a selfie can do it – and it offers increased security.

Facial recognition technology works by comparing the face from the photo on the document with the face of the individual captured in a video selfie. There are, however, various challenges that can negatively affect the results of the verification process. These are: low lighting, poor camera quality, low quality document photos, ageing of the individual, beards, wearing glasses and even ethnic biases.

Buyer's Tips:

- We recommend choosing passive liveness detection for higher security and lower drop-out rates. However, make sure you test the solution first. Solutions offering passive liveness detection based on a single image or through other means may not be able to keep their promise.
- Do not fall prey to false marketing claims. While there are providers (footnote: For example iBeta, IDIAP, TÜV IT) which perform liveness detection tests, there is no official certification for liveness detection in place.

When selecting a vendor, look for a solution that was specifically tuned, trained and tested on datasets that represent your identity verification use case. While there is no proper certification for facial verification, organizations such as the US-based National Institute of Standards and Technology (NIST) perform tests and benchmarks on facial biometric algorithms.

NIST tests algorithms against several large datasets of faces and provides a test report for further analysis. However, NIST does not have a dataset for testing document photos against smartphone selfies specifically, so the result will not accurately represent reality. While the reports will not give you any assurance of the accuracy of a solution for your own business (it takes a specialist to understand and analyze these reports) - choosing a vendor who has at least gone through the process of benchmarking and who understands the implications of the results is a great starting point.

Buyer's Tips:

- Choose a vendor that uses an algorithm which is specifically tuned for your own identity verification use case.
- Choose a solution that can be tuned and adapted to your own security needs.
- If applicable, choose a vendor solution that is flexible enough so its facial biometric module may also be applied to other use cases in your organization, such as facial recognition or mobile authentication.
- Ask the vendors, whether they have gone through a benchmark, like the one from NIST. If they have, ask for the corresponding report. Do not worry if the resulting information seems intimidating. The way the results are explained will give you an impression of the vendor's competence.

The suitability of a solution for your own business depends on a variety of factors. The most important being which algorithms are used and what kind of dataset they were trained on. For example: If you are based in Asia, but use a European solution that was trained explicitly on European faces, the results will probably be disappointing when using the solution in Asia.

Other suitability factors include:

Performance.

Support of multiple use cases for face recognition.

Deployment options.

Dynamic configuration of the security level to match your requirements.

3 Accuracy & automation

We are often asked: How accurate is your solution? While we can fully relate to this question, we find it difficult to give a simple answer to that.

It is not because we are not proud of our results, but because it's simply impossible to provide an honest, transparent answer without having at least a half-day workshop to discuss what accuracy means in the context of real-life applications and how it is measured.

First of all, it is essential to understand the difference between accuracy and the overall degree of automation. Accuracy needs to be looked at as a form of verification accuracy for each individual component or feature within an identity verification platform. The overall degree of automation is the percentage of successful verifications which automatically pass your process, without the need of manual verification or rejection of the identity.

Accuracy

Accuracy needs to be examined across each of the functions in identity verification. For document verification, there are different accuracies for the extraction of the MRZ, the extraction of the VIZ, as well as for each different authenticity check.

A key question worth asking is how the accuracy can be measured and defined. Usually, a solution is tested against a large dataset of documents for which the base truth is already known. For every field on each of the documents, you can know exactly what each character represents. When testing a solution you compare the results of running these images through the algorithms against the ground truth.

Now there are different ways to calculate accuracy from it: You can divide the number of wrongly extracted characters by the total number of characters to get a failure rate, or you can divide the number of wrongly extracted fields (if one or more characters was wrong) by the total number of fields. Alternatively, if one character was extracted incorrectly, you might decide that the entire document verification has failed and then divide the number of incorrectly extracted documents by the total number of documents. Consequently, you could obtain 3 different accuracy-results for the same documents and the same solution, representing 3 different messages. To summarize, the resulting accuracy depends on the taken approach and the definition of failure.

Though it may appear easier with face verification and liveness detection because it is just one feature each, that is not entirely true. In actuality, it is a bit more straightforward and standardised. Same for determining the accuracy of a solution when you run an algorithm through a large dataset of images or videos. The closer these datasets are to our specific use case (document picture against selfie-video), the more reliable the result will be.

Understanding these results would require attendance of a technical workshop. In essence, the result is determined by a match score or

confidence value and a match threshold. For face verification, the confidence value determines how similar the two captured faces are. Different algorithms may have different approaches to measure and quantify confidence values. For example, it can range from 0 - 1, with zero indicating the lowest similarity and 1 indicating the highest similarity. The match score is then evaluated against a preset match threshold. The system predicts that one face matches another if the match score is above the threshold. The confidence value is not to be mistaken by a percentage and does not represent a degree of “certainty” or “confidence” in the results presented to the user. For example, a confidence value of 1 on a scale of 0 - 1 does not guarantee that the two faces belong to the same person. It rather says that based on how the system is designed and trained, the system predicts that the images represent the same face with a very high probability.

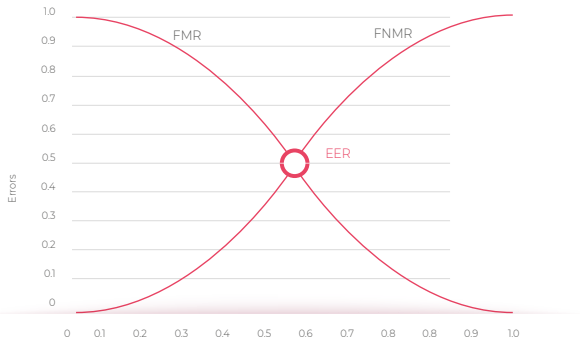
The match scores are returned automatically by the algorithm, while the thresholds are set by humans (developers and/or users). The threshold determines which images/videos the system will accept as a potential match. So, a higher threshold will return fewer accepted results, with the possibility that a potential match was missed. On the other hand, a lower threshold will accept more images as matches, with a higher chance of incorrect predictions.

Because they are adjustable, the thresholds have no meaning by themselves and do not indicate the accuracy of any system. Adjusting the match threshold to a higher number, for instance, does not mean that the results returned are more accurate. Instead, the specific use case and your requirements for the system define the decision of where a match threshold should be set. This choice involves complex, real-world trade-offs.

Benchmarking

In identity verification, a low match threshold could result in a false positive and verify someone incorrectly. This could result in an unauthorised person gaining access to goods or services or a building.

Setting a match rate too high could result in false negatives and prevent someone from getting their identity verified, leading to dropouts in your onboarding process.



"FMR = False Match Rate. FNMR = False Non-Match Rate. EER = Equal Error Rate'

When you choose a digital identity verification vendor, you should also be aware of how facial recognition algorithms work and why the technology can have its limitations. Just as humans can make mistakes, so too can computers - via false acceptances or false rejections during the identity verification process.

False acceptances occur when the algorithm incorrectly believes it has found a positive match between two different facial images (which are not actually a match at all). The opposite happens with a false rejection. A false rejection indicates there is NOT a match between two images – where there actually should be.

Failed facial recognition process

Similarly, when biometric algorithms incorrectly categorise two images from the same person as being from two different individuals, this is known as the False Non-Match Rate (FNMR) and is directly correlated with the rate of false rejections or false negatives. It is also sometimes referred to as a False Reject Rate (FRR). Likewise, the False Match Rate (FMR) is directly correlated with the rate of false acceptances or false positives.

A glossary of terms to be aware of:

FMR = False Match Rate
FNMR = False Non-Match Rate
EER = Equal Error Rate

When benchmarking a face verification solution against a specific database of images, you would typically see the confidence value on a receiving operator curve. The curve represents the prediction on how many false positives and false negatives are expected with the chosen threshold on each point of the curve. Now the results will heavily depend on the database of images that the algorithms are trained on and the database of images it is tested against. If you use the same dataset you used for training to perform your test, you will always get good results but this does not reflect reality. A solution that is trained mainly on caucasian faces, for example, will perform poorly on faces of a darker complexion. And the same concept also applies to liveness detection.

If you ask a vendor and they tell you that they have a 99.9% accuracy rating, it is highly questionable, unless the vendor can explain to you in detail how they calculated the results. It's easy to generate a test dataset to get 100% accuracy on that particular dataset, but this does not mean the results will be close to 100% in reality. So the right answer you expect when asking a vendor is “it depends”, followed by an explanation.

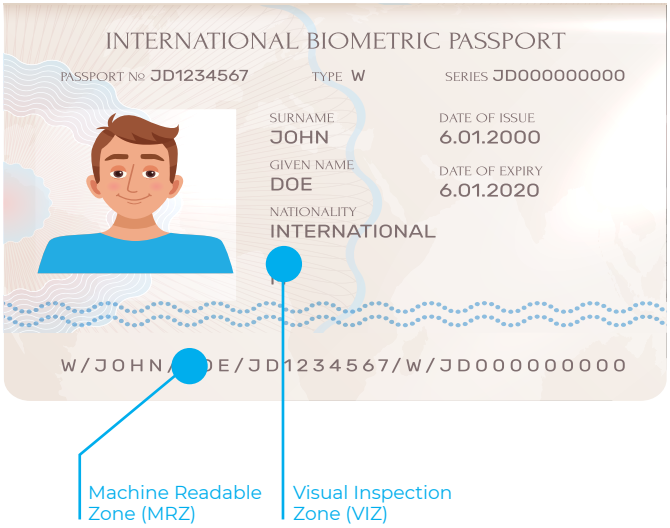
Automation

What ultimately counts is the overall degree of automation for your use case. You want to know how many identity verifications will pass through the entire process automatically, how many false positives, and how many false negatives are expected across all verification steps.

The degree of automation really depends on many factors, such as the configuration of business rules and your specific use case requirements.

However, to give an example, if you insist that for every document type, every single character of the MRZ needs to match every single character of the VIZ, your degree of automation will take a big hit. Consider a person's name in an official ID-document. The name in the MRZ is not covered by the resulting checksum and the used OCR-B font does not allow for any special characters. Also, longer names will be truncated in the MRZ. So if you apply this very strict rule, anyone with a special character or a long name will be kicked out of the automated process - boosting your false negatives rate.

On the other hand, if you really don't care much about extra security, but just want to do simple age verification, you can boost the overall degree of automation by relying on the MRZ alone and not even check the VIZ.



If you insist that for every document type, every single-character of the MRZ needs to match every single character of the VIZ - your degree of automation will take a big hit.

Buyer's Tips:

- Ask the vendors on your shortlist how accurate their solution is. If they respond with a simple number, like 99% or even 100%, they are either providing incorrect information or don't have the necessary know-how to answer the question.
- Preferably work with a vendor who is transparent about the different trade-offs and interdependencies of identity verification. Explaining the technological context and providing insight into the process are great steps towards trust and transparency.
- Choose a vendor that can fine-tune accuracy and automation to your own individual use cases.

4 User experience (UX)

We have covered the security, accuracy and reliability of an identity verification solution. However, the best solutions will be worthless if your users don't manage to make it through the identification process.

This is where the demand for a more convenient and streamlined online identity verification process comes into play. The most successful digital onboarding platforms are designed with UX as a primary focal point because a better-designed UX leads to higher customer conversion rates.

Meeting user expectations in the digital onboarding journey might be the most difficult obstacle to overcome. For example, in e-commerce platforms, the top two issues when shopping for an identity verification platform are speed and ease of use. If the process is too time-consuming or overly complicated, you run the risk of customer abandonment and a decrease in sales. High customer abandonment rates in the online ID verification market often come down to a poorly designed UX. Some ID platforms in the European market have even reported 40-50% customer abandonment rates. The following points will help you find the identity verification platform that meets your company's needs:

Less is more

A UX involving as few screens as possible during the onboarding process is important, as it directly impacts how long it takes your customers to complete the onboarding journey. A visual screen indicator that informs users of the screen number they are currently on and the number of screens remaining is a best practice. In general, you want to limit the amount of interaction needed by the user, every click and any movement required by the user leads to a higher chance of abandonment.

Furthermore, the submission of one's identity through an internet-connected device is not something that most people are immediately comfortable with, so clear instructions help.

To better gauge the attention that the user experience receives at an ID verification vendor, choose a company that has UX specialists onboard who ultimately inspire the overall customer and UX design.

Ideally, the user should be walked step-by-step through the onboarding process. When compiling code for an identity platform, developers often spend much of their time on functionality - as this is their main charge – and as a result, the customer UX often lacks consideration.

In doing your research, a solid acronym to follow is KISS* or Keep It Simple Stupid.

*This acronym was coined by a US Navy engineer as his team was designing a jet engine that had to be easily repairable by an average mechanic out in the field under combat conditions.

The KISS principle implies that most systems work best if they are kept simple rather than made complicated. Therefore, simplicity should be a key goal in design and unnecessary complexity should be avoided. An overly complicated onboarding process will lead many potential new customers to abandon the onboarding process.

For example, with regards to the capturing process (which we discussed above), the best ID solutions will take full control of the process; guiding the user and providing real-time feedback. This ensures the image quality is high enough to avoid a repetition of the process.

Also, some solutions may ask the user which kind of document type and from which country they are going to capture. While this might help the algorithms to perform better on that document type, they will not be able to deal with a case where the user then captures a different document from the one initially selected. Even if this is a user error, it will lead to a repetition of the process, and ultimately to frustration and potential abandonment.

Another key area of failure for many solutions is the liveness detection module.

To recap from a UX perspective, active liveness detection asks the user to make a series of specific movements, which will ultimately lead to a higher drop-out rate for your onboarding process. With passive liveness detection, the user only has to hold still in front of the camera for a couple of seconds – this is manageable for most users.

Lastly, it's also important to consider the languages of your target markets. As the de facto international business language, English would fit the language need of most end-users, but the addition of other languages will make the onboarding journey much easier for people with limited foreign language skills. If you are using a standalone solution that is branded, make sure that the languages you need are covered.

There are vendors who also offer white-labelled solutions which allow you to completely adjust the UX, not just in terms of branding, but also other considerations such as languages.

Workflow and platform support

The overall workflow itself and how it interacts with your existing business processes is as important as the actual verification. A tightly integrated workflow into your existing processes allows the user to feel "at home" with your brand, which decreases the chances of abandonment.

Some vendors have a very stiff process and limited possibilities for integration - if a user has no choice but to download an external mobile app in order to perform the verification, chances are higher that the process will be abandoned. Identity verification solutions need to be deployed across different platforms and to be configurable to your own specific needs and process workflows.

Even though many people use a desktop or notebook as their primary device, many identity verification platforms focus their product to work only on smartphones. Smartphones are the key catalysts transforming the digital identity verification market today. The reason is that today's smartphones have improved camera sensors which operate well in low-light and are paired with snappy operating systems. These

considerations have helped to accelerate the overall online identity verification market in the recent years.

As the performance gap between desktops and smartphones continues to narrow, the trend towards greater smartphone use will persist*. The report estimates that 4.3 billion smartphones were in use globally by the end of 2017 — three times the number of PCs. And smartphone users are expected to keep growing by 9 percent per year, reaching 7.2 billion users by 2023.

There are, however, still a number of people who use a desktop/notebook as their primary device, so some vendors also offer support for these platforms. The problem with PCs is the complexity and virtually unlimited combination of cameras, operating systems and drivers used. Supporting and actually testing all these combinations is almost impossible, not to mention that many systems don't even have a camera. Even if it works, it poses an additional challenge to UX as some cameras are mirrored which makes it difficult to place a document in front of the camera appropriately; especially since you are blocking your own view of the screen at the same time.

In consequence and based on our experience, we recommend routing your users to a smartphone-based verification using a QR code, email, or SMS link.

Buyer's Tips:

- Speed and accuracy are two variables that often conflict with one another. This is especially true for online identity verification platforms where speed is desired and therefore accuracy often takes a backseat. We encourage you to look for solutions that achieve speed through minimal user interaction and an optimized UX, while staying mindful of accuracy.
- A great solution should take no longer than 30 - 60 seconds max. to perform the full identity verification.
- Go for a solution that can be adapted to meet your own UX and workflow needs.
- Choose a solution that guides the user through the verification process and provides instant feedback. Avoid making users waiting for 5 minutes, only to learn that the process needs to restart all over again.
- Choose a solution that employs passive liveness detection over active liveness detection and one that does not require users to select the document type beforehand or manually capture and upload pictures.

*Samsung's Insights publication

5 Flexibility & configurability

The more successful and larger companies become, the greater the impact an identity verification process will have on their business.

Small, medium and large size businesses all have their own requirements depending on their use case(s). Even for the same use case in the same industry, two companies of similar size will likely have totally unique requirements and preferences when it comes to identity verification. Identity verification is rarely a requirement, which can be implemented as a standalone solution since it has to tie into the organisation's existing processes, which includes the existing IT environments and business rules.

In your search for an identity verification partner, preferably go for a solution or platform that offers maximum flexibility and customizability and one that can scale with your company as it grows. When we write about flexibility and configurability we are first talking about the ability to adapt and fine-tune the applied business rules and verification logic for accepting or rejecting an identity. Secondly, we are referring to the different possibilities of integration and deployment for a solution within your preexisting IT environment and business processes.

Business rules & verification logic

Business rules are your company's own unique requirements or filters that should be applied to your use case.

By building identity verification solutions from the bottom up, we have learned that every company is unique and requires things to be done differently.

Identity verification platforms should be sufficiently flexible and configurable enough to adapt to the needs of your company. Business rules can apply to people, processes, corporate behavior, and computing systems

Exemplary filters that help creating the most efficient and accurate onboarding process:

Which document types and nationalities should be allowed, and which ones rejected?

Which data integration and validation checks are mandatory, and which ones are optional?

Which authenticity checks (e.g. NFC verification) are mandatory?

How many times should a user be allowed to repeat the process in the case of failure?

Which thresholds should be applied for face verification and liveness detection?

How to deal with expired documents?

in an organization. Their mission is to help an organization achieve its goals. Ultimately, business rules define the criteria that need to be fulfilled to accept or reject an identity. These criteria are not just defined by the identity verification process but also by the legal and regulatory requirements, company internal compliance, or more simply, individual business preferences. The decision of whether an identity should be accepted or rejected should ideally be left up to you – no vendor solution should make that decision for you.

Many vendor solutions will provide you with a simple binary fail/success result. For some companies and use cases, this might already be sufficient and serve the basic needs; for example, in cases involving compliance. However, this does not indicate the success of the overall process or how this can be improved for your specific needs.

A good identity verification vendor will provide you with all the necessary information to make a well-rounded decision for accepting or rejecting an identity based on your filtering criteria. However, the best solutions also provide you with the flexibility to directly apply your filtering criteria or business rules (and dynamically change them over time) as part of the process. These solutions also help you deal with various scenarios, such as unforeseen rejections, encountered along the way.

Applying business rules as part of the process will substantially impact the UX, the overall degree of automation for your business, and ultimately the cost of ownership. For example, if you are a retailer wanting to sell alcohol and tobacco online, you will most likely not have the same regulatory restrictions as a bank onboarding a new customer.

As a retailer, you only need to know that the person is 18 years or older, and for that, even an expired document might suffice. So having a very strict identity verification process that checks every single detail will result in a high dropout rate and lost revenues. A bank on the other hand has much stricter requirements that must be met.

There are vendor solutions that address these requirements for flexibility by applying various checks and returning error codes that can later be acted upon, either dynamically during the identity verification process or afterwards.

There are hundreds of flags that can be returned, such as:

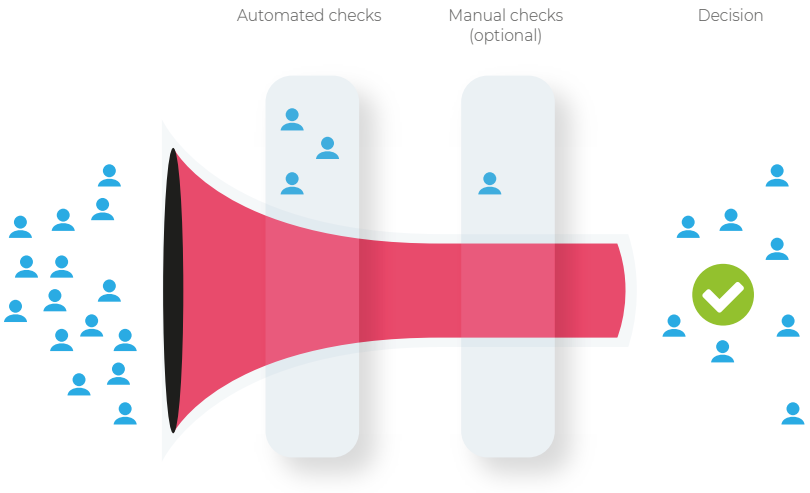
- Image resolution too low
- Document not recognized
- Document expired
- Face not detected
- Specific MRZ fields not valid
- Face verification failed
- Image blurred

The best solutions can use such error codes in real-time during the verification process. By extension, such errors can help determine all kinds of onboarding requirements and whether these should be classified as blocking or non-blocking. Blocking errors would lead to aborting or repeating the process immediately and non-blocking would let a verification go through despite certain errors.

As an organization, it is critical to know what is important to you and how a solution should behave under differing situations. For example, if

you are a retailer, the potential monetary damage via a fraudulent identity is much smaller than for a bank. So if you don't care too much about banking-grade security and regulation, and want to optimize your process for maximum conversion, you would want to let through as many verifications as possible, even if this means accepting expired documents and / or blurred images.

You may also want to be more tolerant on the face verification and liveness detection thresholds. As a bank on the other hand, you would want to be strict and comply with all the regulations. Using the error codes to block certain cases in the identification process will help boost the overall degree of automation and minimize the effort to filter through errors with verifications ending up on your backend.



Another advantage of applying business rules and error codes dynamically is that it helps you deal with different scenarios. In an ideal scenario, everything works great and an identity is automatically verified. However, in many cases, it is not so black and white, as the machine isn't 100% sure and certain business rules are not met. Instead of just blocking or rejecting the user, the information can still be passed on and a back-office employee who can run a manual verification check as a fallback option. While this has an impact on your degree of automation, it helps you manage your potential customers better and increase the overall conversion rate.

Even though the best identity verification solutions on the market today are built to be as fully automated as possible, this is a lot easier said than done.

A highly configurable verification logic is key to ensuring that your onboarding process can be tuned to your own requirements in terms of UX, security, compliance and automation.

A well-equipped vendor helps you identify these requirements and defines – together with your company – the various filters (business rules) that should be applied to the verification process. Because of that collaboration, the solution will drive the optimal results based for your needs. The best solutions allow you to define such business rules even on a transactional basis, meaning that they can dynamically change depending on certain user characteristics. This not only allows you to further boost the overall degree of automation but also helps you cover several different use cases with the same implementation of the vendor's solution, reducing your cost of ownership.

Some vendor solutions also employ human operators as part of their identity verification process by default. However, there are academic studies that suggesting that certain gender

and ethnic biases can lead human operators to improperly (and possibly, subconsciously) verify an individual's identity. Also, by using human operators, other regulatory and data protection challenges might apply.

If you are located in an EU country, for example, but your vendor uses human operators in India, the solution may not be compliant with your local data protection laws. So depending on your own requirements, you may not want to use human operators at all, or at least be able to use your own employees as a fallback option in case certain business rules are not met.

Integration & deployment

Each organization has its own preferences when it comes to the integration and deployment of a solution. Depending on the complexity of an organization's existing processes, some approaches may be more suitable than others.

The first question to ask yourself is whether a standalone all-in-one solution is sufficient for your internal requirements or if a deeper integration into your existing IT environment and business processes is needed. An all-in-one product includes all modules of an identity verification solution in a single end-to-end process. Additional peripheral functionalities such as 3rd party database checks, sanction lists, PEP (politically exposed persons) and optional manual checks are also sometimes included. These kinds of solutions usually offer a simple integration but lack the modularity, flexibility and configurability described in the preceding sections.

Typically, smaller companies, including startups, which do not have their own IT department or engineering resources and do not have strict requirements and business rules, prefer to have simple, plug and play solutions that provide a simple output. However, as companies mature and grow, the number of use cases might also expand. At this point, it becomes evident that an all-in-one solution can no longer cope with the increasing complexity. Larger organizations typically prefer to have a more modular and configurable approach, allowing them to deploy single modules and components in distinct areas of their infrastructure and integrate deeply with existing business processes and IT environments.

Another key question to ask is with regards to platform preference: differentiating between native mobile apps, mobile browser-based solutions and PC based solutions. Earlier in

Buyer's Tips:

- Be aware of your own requirements in terms of UX, security, automation and compliance.
- Choose a solution that is dynamically configurable to your own business rules.
- Choose a solution that gives you ownership of the process, allowing you to dynamically change business rules and filtering on a transactional basis; without the vendor's involvement.
- Choose a futureproof solution that will scale with your organization as it expands.
- Work with a vendor that guides you through your overall business process and helps you in defining the optimal verification logic.

the guide, we essentially eliminated the use of desktop/laptop-based browsers for security and UX reasons. So the remaining choice is between mobile apps and mobile browser-based web apps. If your entire user journey is browser-based, it may not be suitable to deploy a mobile app, given that your customers would need to download it for completing their verification journey.

If you already operate on a mobile app, the choice to do a native integration might be obvious. However, when making this choice there are several factors to consider which involve some trade-offs. Of foremost importance is the consideration that processing identity verification checks directly on a mobile device has advantages and disadvantages over server-based processing using web apps.

Mobile apps

Running the ID software directly on a mobile device has the benefit that you can use the local processing power of the device.

This means that you can process more images faster, allowing you to guide the user in real-time to achieve a better image and extraction quality. Also, certain functionalities, such as biometric NFC chip verification are (as of today) only possible on the smartphone. But that may also change in the future.

Another advantage of a native mobile implementation is the ability to apply real-time error handling, ultimately resulting in better performance and a higher degree of overall automation. Furthermore, verification can be done completely on-device and offline, however, this may not be very relevant, as most use cases require internet connectivity anyway.

Platforms:

Native App

+ Real-time user guidance
+ Best image and extraction quality
+ Better speed and performance
+ Higher security with NFC and hologram or lenticular
+ Document verification can run completely offline on-device
+ Real-time error handling

VS

Web App

– No real-time user guidance
– Less control over camera and image quality
+ No download needed
+ Quicker to integrate
+ Easier to update and maintain

Web apps:

Web apps have a big advantage: users can go through the identification process without the need of downloading a mobile application first.

With a web app, the mobile camera is controlled through the browser, to capture all necessary image/video frames for processing the identity verification on a server. The big drawback here is that the camera cannot be used the same way in a browser as it can within a mobile app, usually because there is less available processing power. This leads to a less responsive UX and usually a somewhat lower degree of automation. On the other hand, a web app is much easier and quicker to integrate and also easier to update and maintain over time.

One of the most important factors to consider is the technical architecture of the identity verification platform with regards to choosing a cloud-based deployment or an on-premises implementation into your own infrastructure.

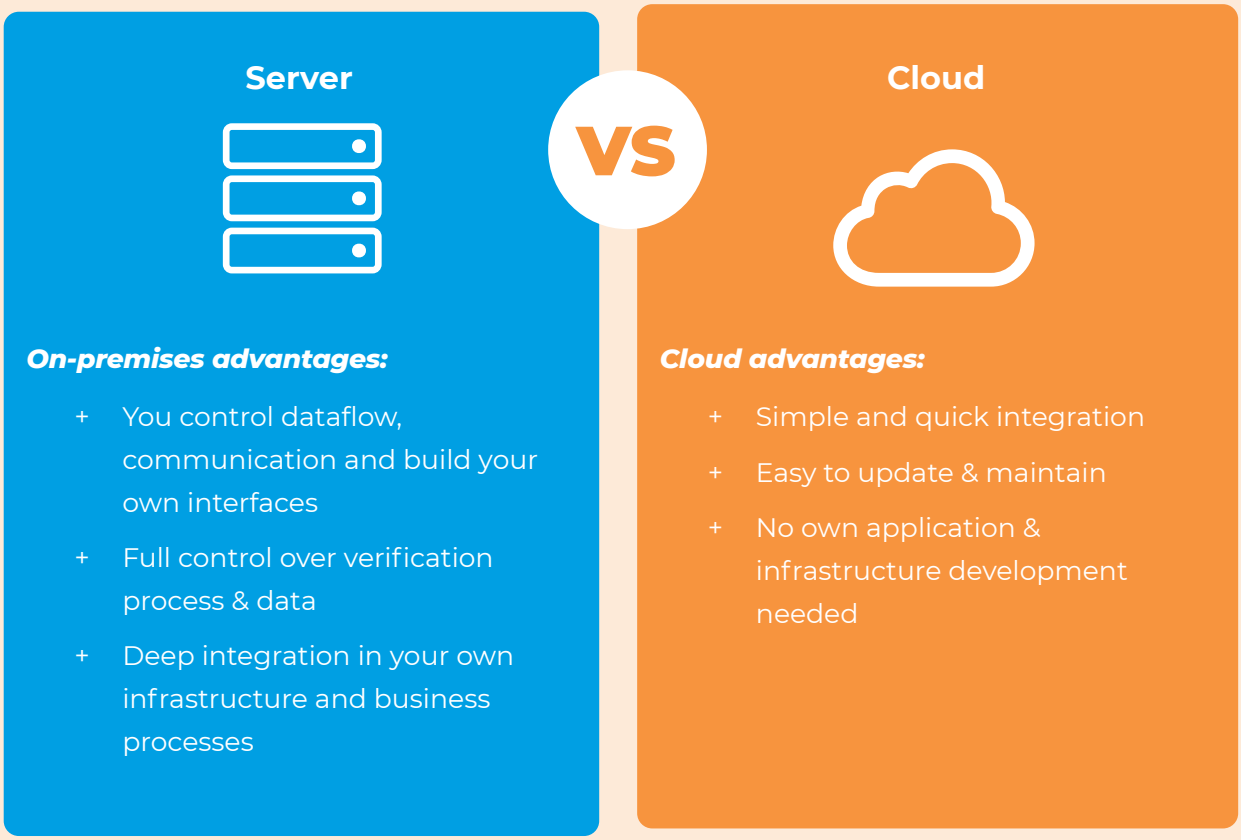
Most vendor solutions are available as a cloud solution that can be accessed through an Application Programming Interface (API). This is useful when your product or service already has an app and/or website but requires the addition of an identity verification platform. In this case, the platform can easily be integrated via an API. An online identity platform operating in the cloud implies that there is no need to install any software within the company's own infrastructure. However, the “cloud” is a broad term and there are differences.

Make sure you really understand what kind of cloud the vendors operate on and check whether they are using a public cloud, like from Google, Amazon or Microsoft, or their own private cloud infrastructure. This will have an impact on compliance with your data protection laws as well as data security.

Where you store your customer’s data is also a big deal. Your online identity platform should value data security, including data flow and where data is stored. If the vendor’s cloud sits in a remote country, this means that the sensitive data of your users is leaving the country and that you have no control over what is happening to it. This is not only non-compliant in many cases but also poses a potential privacy risk.

Buyer’s Tips:

- Be aware of your requirements and the trade-off between mobile and web apps.
- Choose a solution that has a cross-platform approach and covers all relevant scenarios.
- Flexibility is key, choose a vendor solution that provides you with the full range of options on technical architecture (cloud, on-premises, hybrid).
- Look out for vendors who already have the necessary integrations, or ask them if they can do it themselves.
- Even if you need a simple all-in-one cloud solution, work with a vendor who can offer complex “on-premise” integrations as well - as this is a sign of overall competence.



So, if you value data protection, ensure that you use a vendor with a local, ideally private, and certified data center infrastructure.

The alternative is an on-premises deployment. In such a case, all the necessary components for the identity verification are installed and run directly on your own hardware/infrastructure or on your own private cloud. This provides you with full control over the identity verification process, how user data flows and how it is integrated with your other systems. Also, you will have the sole responsibility for IT & data security. Despite the many advantages, there aren't many vendors offering full on-premise solutions, given the added integration complexity and effort involved. A vendor offering on-premise solutions will very likely also help realizing more complex integration projects and closely support its customers. So even if you choose to go for a cloud solution, working with a vendor who also offers on-premise solutions is the preferred option.

Depending on the use case, you may find a vendor who is already integrated with a system you are using – like your ERP, CRM or similar software. The best vendors can offer integrations with SAP modules or other commonly used core systems, so you won't need to do any further integrations.

6 Compliance: Why it matters

Compliance has essentially been the torchbearer for online identity verification as some of the earliest implementations of the service were used to assist financial companies (esp. fintech companies) with Anti-Money-Laundering (AML) and Know Your Customer (KYC) regulations.

A major factor behind the growth of the online identity verification industry is the shifting tides of how people access their banking. More people are switching to online or mobile banks while other first-time bankers are opening their bank accounts through online-only banks.

This trend is mainly driven by the rapid closing down of brick-and-mortar bank branches around the world - at least in wealthier developed nations. As governments around the world begin to hold financial institutions to ever higher standards, these institutions are in turn requiring the companies they do business with to also be more accountable.

KYC / AML

These two terms are often used interchangeably, as KYC (Know Your Customer) legislation belongs to the AML (Anti-Money Laundering) initiatives that are partial to the regulatory framework used throughout the global financial system. The submission of KYC documents and their processing is legislated under the AML framework which banks and financial institutions are obliged to follow. The overarching goal of AML is to verify with a high degree of certainty that customers are who they say they are and that they are not likely to be engaged in criminal activity.

GDPR

A special regulatory framework that comes into play for all citizens and residents of Europe, implemented in 2018. This regulation brought individual data protection issues to the forefront. Regardless of where your business is located, if you are offering your product or service to someone residing in the EU, then you are obliged to comply with the GDPR.

PSD2

The revised EU Payments Services Directive (PSD2) introduced the requirement for secure customer authentication (SCA) and requires a combination of knowledge, possession and inherent-to-the-customer based tools to verify a consumer‘s identity before a transaction may be completed.

Buyer’s Tips:

- Look for vendors that have knowledge of the various regulatory frameworks affecting their product, e.g., AML, GDPR and PSD2 regulations.
- Work with vendors, who are eager to share their expertise and support you in understanding the relevant regulatory requirements for your use case.

7 Market proven & future-proof

A number of different factors can be used to determine whether or not the vendor you choose is the best for your business needs.

No single factor in this section should stand alone, but each should be weighted to the needs of your business.

Own technology & control over product

Many companies in the digital identity space build their product/service using outsourced components.

While this is probably cheaper overall for the ID company, given that they can save on research and development costs, it can lead to various issues down the road. The aforementioned jurisdictional requirements of your product or service, for example. The GDPR requires that EU companies keep EU data in the EU. A problem would arise if the frontend of a platform (which receives the uploaded ID document scans) is located in a non-EU country.

There are of course other benefits to a company having its own technology & full control over their product, as they would be entirely responsible in the event of a business disaster such as a hacker infiltrating a vendor's network. In such a scenario, a vendor offering a hodge-podge solution would have to sync with all the other vendors whose components make up their product. This could coalesce into a series of 'whataboutisms' and other companies not accepting responsibility for their part in the disaster.

One of the main advantages of vendors that own their technology, is that they would typically share their product roadmap and involve you in the definition and priorization of new features to improve the solution over time in a way it benefits you most. In this way, your project needs and requirements are better addressed than a vendor which does not own their own technology and is unable to provide flexibility

Certifications and Standards

Certification agencies provide a mutual framework to test the quality of a product or service.

There are a number of standards and certifications that a product in the online identity verification space could attain.

ISO 27001: The ISO 27001 certification is an internationally recognised best practice framework for an Information Security Management System (ISMS).

If you are a business that wants to secure its information assets and avoid regulatory headaches (under GDPR laws for example), working with a vendor that is ISO 27001 certified should be at the top of your certification wish-list.

When a vendor holds the ISO 27001 certification, you can trust that they will be more likely to act diligently regarding where and how your data is stored and accessed.

ETSI norms: An important organisation to be aware of in your buyer's journey should be the European Telecommunications Standards Institute (ETSI). ETSI is in charge of creating global standards around internet, mobile,

radio and broadcast technologies across the EU. By ensuring your vendor is knowlegable and up to date with ETSI standards, you are more likely to ensure your identity verification solution complies with legislative and regulatory standards across Europe.

ISO/IEC 30107: The purpose of this certification is to provide a foundation and process for presentation attack detection (PAD).

This ISO/IEC 30107 certification establishes a framework through which presentation attack events can be specified and detected, such that they can be categorized, detailed and communicated for subsequent decision making and performance assessment.

eIDAS: Another standard is the electronic Identification, Authentication and Trust Services (eIDAS), which is an EU regulation for electronic identification that aims to make national eID schemes interoperable across Europe.

Many vendors claim being compliant and having certifications. Taking a closer look is, however, very appropriate. We have seen cases, where only a small part of the advertised solution was certified. Some solutions we encountered were only partially compliant. Some solutions might miss the certification for your specific use case. In some instances, the certification is only valid for a part of the advertised solution/product.

Company location

Where the company is headquartered and where it has its offices is also an important yet often overlooked factor.

Does the country have unique qualities that make it a desirable location to do business? Think about the different ways political and financial stability has an impact on the storage of customer data and the impact of laws and regulations on how data is accessed, stored and controlled in that country. A vendor who is closer to you also suggests a more reactive support time. Additionally, the vendor can easily visit you when needed and there will be fewer challenges due to different time zones.

Track record and reputation

Reputation matters.

How mature is the company? Has it reliably provided its product or service over an extended period of time? Are existing online reviews about the company or its product positive or negative? The more questions that can be asked in this manner the better.

A company that deals with such highly sensitive information as online identities, has the responsibility to get things right. Perfection is not the goal, as mistakes are only natural. However, the way a company behaves when problems arise is highly demonstrative of its integrity.

Customer references & trust

One of the most important things to consider is customer references.

Who has the vendor worked with? In which industries? Which use cases? And with which customer sizes? A vendor who has only dealt with 100 small customers likely doesn't have the right set-up to deal with a very large organization. On the other hand, a vendor who only specializes in large enterprises may not be the right partner for a startup.

Has the vendor been used by a government agency? Government trust is public trust (not true

for every country of course) and that is a good indicator of a company's overall quality. Does the company know about building public trust? How might that be important for their particular business? What factors play a role in low levels of public trust in the company? Low public trust in a company is usually not the result of a single factor, but rather emerges from multiple causes.

Awards

Has the company been acknowledged by an outside institution and been nominated for or even won an award?

This is a good sign, as it is in every company's interest to be noticed and to make themselves notable on a national or even global stage. However, just like venture capital and seed funding, awards are helpful on a general level, but they do not tell you the more granular details, like for example, how effectively a platform converts customers.

One potential downside with awards is that some companies might overdo it to compensate for something else missing.

Academic partnerships

Companies that collaborate with academic institutions display an ability to bridge the gap between university and corporate culture.

A commitment to academia will ensure that the company remains on the cutting edge of technological research and discovery. Companies located near academic institutions benefit from the ability to easily meet face-to-face with thought leaders on technology.

Instead of just monitoring early-stage research at universities and throwing money at an opportunity as it emerges, a smart company will continuously seed money into areas of interest. Both industry and academia, as well as the greater society, stand to benefit from these long-term commitments. Check if any of the identity verification vendors that you are considering are partnering with any academic institutions and how they collaborate.

Buyer's Tips:

- Choose vendors who have worked with companies similar to yours.
- Ask vendors for customer references, customers will tell you exactly what worked well and how.
- Vendors who have worked with national digital ID schemes or government organizations are typically good for consideration.
- Be wary of companies which are defining themselves mostly by the awards they won. This might indicate a lack of focus in other key areas of their business.
- We recommend choosing a vendor that has developed its own technology and ideally retains full control over their product.
- Work with a vendor that understands regulations and certifications, and doesn't shy away from explaining them to you.
- Considerations such as business trustworthiness, geopolitical stability and ability to attract talented employees should not be underestimated.

8 Support

Pre-sale support

When looking for an identity verification solution, seek out the solution that offers the best support when designing the business process and business rules.

What does your business require? How will the product fit into your current business setup? How will the architecture and design of it look? How to synchronize the process with your current and future customer base?

Similar to when you make a major purchase at an electronics store, you would usually reach out to a sales support person if you require more information about a product. The same logic applies to the acquiring of an ID platform for your business. Though it may be true that purchasing a software solution for your business is much more complicated than purchasing a flat-screen TV, there should still be a highly-qualified and dedicated sales support to guide you through the process.

Post-sales support

The post-sales support of your chosen online identity verification product is also an important consideration.

Because online identity platforms are primarily sold as a subscription service, they should automatically be packaged with post-sales support that guides you and helps improve the performance for your business throughout the entire lifecycle.

Integration & technical support

Developer support and technical support are key to expertly integrating the identity verification platform into your current business setup.

Look for a solution that offers technical support and dedicated project management on an ongoing basis. This is key to successful product implementation.

Change management & business continuity

Business needs change over time which is why you should look for a product that has a change management protocol.

This protocol will allow you to configure or modify the product at a later date so the product continues to fit your business' changing needs. It will also ensure that you are only paying for the modules that you require. Business continuity and disaster management support provide additional assurances that your business will be able to continue in the event of a disaster.

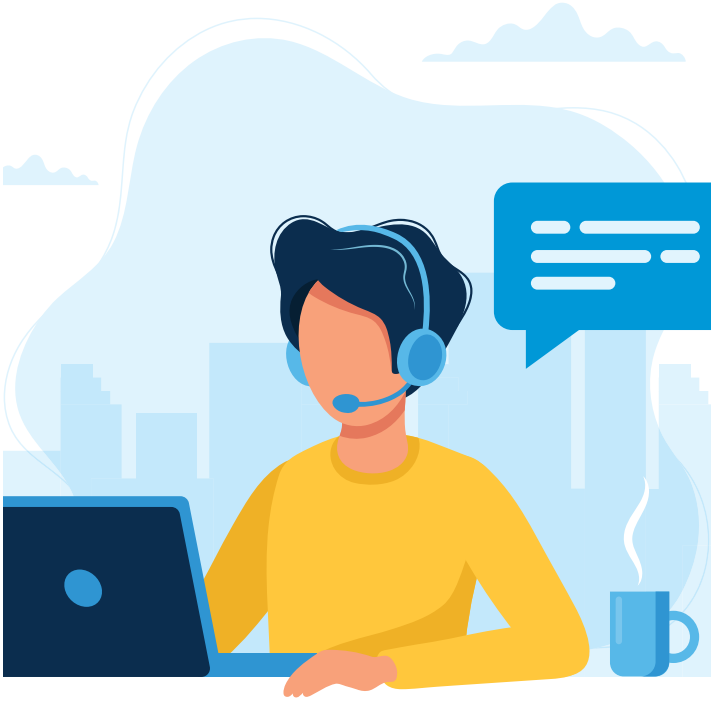
In some ways, identity verification can be compared to search engine marketing (SEM). In SEM you set your keyword strategy, start with some low key campaigns, take your learnings out of it and continue to improve your ads on an ongoing basis for the optimal result. With identity verification, you first tune it (e.g. for high security) and analyze the results, then you start adapting and tuning the business rules and thresholds over time to reach the optimal conversion rate for your business. Having a vendor who understands

that identity verification isn't just simple inputs and outputs and supports you in optimizing your processes on an ongoing basis is key.

Service level agreements (SLAs)

These are the commitments that the vendor makes to you.

In general, the more critical a service is to a company's operations, the stronger the SLA will need to be, in order to satisfy customer needs. SLAs may include service uptime commitments, response times, target fixing times and sometimes penalties in case of non-compliance. Choose a vendor that offers a rigorous SLA or at least lets you choose from different SLA levels. This is often an indication of a stronger commitment to ensure a flawless service.



Buyer's Tips:

- Choose a vendor that offers a dedicated and expert-orientated support team to help you make the most of any product solution you purchase.
- The best vendors offer pre-support and post-support services by default.
- Technical support should not be overlooked in the integration of an identity verification solution. Proper documentation is critical to maintaining and reaching successful outcomes.
- Try and select a vendor that offers rigorous change management protocols in their solution. These protocols are particularly important as your business requirements may vary over time.

9 Cost

As is the case with most products and services, the cheapest solution is not always the best, nor the most flexible or secure.

In identity verification, as with most other things, you get what you pay for. Since competition in identity verification has risen exponentially over the past years, so too has the pressure on pricing in the industry.

It's also helpful to understand that the best identity verification platforms are based on highly complex technologies such as sophisticated machine learning and computer-vision algorithms. This has required decades of experience and many years of development and continuous improvement, all of which costs money.

Do they own their technology?

Most identity vendors on the market don't own their proprietary technology.

Instead, many vendors license different components from various technology providers and then package them into a product or platform. Nothing speaks against using such a product if it fulfils your requirements.

If you need a basic all-in-one solution, this may indeed work. However, if you need a more dynamic, complex setup, chances are high that you will not get the required expertise and support from that vendor.

We have heard outrageous pricing examples, usually from new challengers, trying to get a share of the market by offering sub-market level pricing. These challengers often suddenly disappear from the market after a couple of years.

The main problem is that many vendors underestimate the complexity of identity verification and the importance of flexibility and guidance needed for the customers. We therefore recommend working with vendors who build and own proprietary technologies. These vendors may not have the shiniest website and marketing materials, but if you take the time to dig a little deeper, you will get much more substance out of their responses. Such vendors will have much deeper knowledge and expertise and can support you much better when defining your requirements and when implementing and deploying their product. Furthermore, having proprietary technology means flexibility on the product side and within the commercial arena; if you don't need to pay licenses to any suppliers, you can have total freedom on the pricing model.

Transaction-based pricing

The identity verification industry mainly operates on transaction-based pricing, resulting in a dollar amount being paid for each identity verification.

Standard all-in-one solutions typically work as a subscription model wherein the monthly or annual payments include a certain volume of transactions.

Typically speaking, the higher the volume of transactions, the lower the dollar amount per transaction. However, the more complex the implementations are the higher the costs should be. Vendors may charge a one-time setup fee for delivery and implementation of a solution and annual maintenance fees for ongoing support. Sometimes these extra efforts are packaged into a subscription model in order to simplify pricing; so be sure to always check what you are actually getting when noting the price.

Price flexibility

While any vendor can immediately point to their standard pricing, the best vendors will offer flexibility on the business model.

A vendor should be a partner that supports your business journey and enables you to become more successful than you already are. By offering to help you with pricing, a vendor demonstrates that you are essential to them, no matter how small you might be as a customer.

The best vendors will offer you lower-cost ramp-up periods, flat fees with unlimited usage and even enable you to grow your user base with free verifications - earning for themselves, then, an amount calculated on the revenues generated by your business. These are just a few examples of alternative business models - don't shy away from asking your vendor to support you. This, however, should not imply lower (discount) pricing - just different pricing models with various incentives and commitments.

Buyer's Tips:

- Choose a vendor with proprietary technologies.
- Don't base your choice on price alone.
- Choose a vendor which offers you flexibility on the pricing model and helps you to grow your business before saddling you with a massive sunk cost.

10 Next steps

We can help you define your most important requirement and get started with finding the ideal solution for your business.

After reading this guide, we usually get two simple questions:

What do we do next?
How soon can it be implemented?

At PXL Vision, we believe in transparency and as part of our commitment to being open and honest about the overall process, we are more than happy to help you make sense of the important information contained in this document. We look forward to having a conversation with you, so we can learn more about the problems you wish to solve for your business.

As we discussed in this guide, there is no one size fits all IDV solution or product for every business size and type.

Our team of experts have the knowledge to help your business find and implement an identity verification solution that works best for your own requirements.

We're here to answer your questions.

We hope that this Buyer's Guide has been helpful for your business and provided you with a deeper understanding of the broader online identity verification market and the many granular choices that can impact your customer onboarding experience.

Please reach out to us for a chat or a free demonstration of PXL Vision's award-winning technology and product solution today.

Have a chat
with our product experts.
pxl-vision.com/contactus/

About PXL Vision

PXL Vision is the Swiss market leader for highly secure and fully automated AI-based identity verification solutions. PXL Vision's flexible technology supports any customer requirement and business process worldwide.

Companies from industries as diverse as financial services, telecommunications, mobility, the sharing economy and retail as well as the public sector are already using PXL Vision's technology to verify their customers' identity.

PXL VISION