PXL VISION

Der ultimative Einkaufsleitfaden zur Identitätsprüfung

Der ultimative Einkaufsleitfaden zur Identitäts-prüfung

Alles, was Sie schon immer über die passende Identitätsprüfung für Ihr Unternehmen wissen wollten.

Inhaltsverzeichnis

Willkommen

Es gibt keine Standardlösung für die Online-Identitätsprüfung. Darum haben wir diesen **Einkaufsleitfaden** geschrieben, um Unternehmen beim Kauf einer Identitätsprüfungslösung zu beraten.

Wir wissen, dass die Identitätsprüfungsbranche manchmal unübersichtlich sein kann, insbesondere dann, wenn Anbieter viele Versprechen zu ihren Produkten und Lösungen machen, von denen manche unbegründet sind. Deswegen möchten wir für Transparenz und Offenheit bei der Buyer Journey sorgen. Dieser Leitfaden führt Sie durch die einzelnen Schritte des Einkaufsprozesses. Sie erhalten Einblicke in alle Aspekte der Identitätsprüfung Ihrer Kunden.

Dieser Leitfaden enthält einen detaillierten Überblick über den Identitätsprüfungsprozess, die bewährten Technologien, die Sie kennen sollten, die relevanten Anwendungsfälle und die regulatorischen und gesetzlichen Vorgaben, die Ihr Unternehmen erfüllen muss.

Bei der Kaufentscheidung ist es wichtig, dass Sie sich darüber im Klaren sind, welche Softwarelösungen und Technologien für bestimmte Fälle am besten geeignet sind. Mit diesem Leitfaden können Sie eine fundierte Kaufentscheidung treffen, von der sowohl Ihr Unternehmen als auch Ihre Kunden profitieren.

Tipps zum Kauf

Im gesamten Leitfaden und in jedem einzelnen Abschnitt heben wir einige der bewährten Praktiken beim Einkauf hervor, damit Sie voll von Ihrer Wahl des Anbieters und der Lösung profitieren können.

1 Hintergrund

Betrug ist so alt wie die Menschheit selbst. In einem Sonderbericht aus dem Jahr 2018 bezeichnet die in London ansässige NGO Fraud Advisory Panel Betrug als eine der größten Bedrohungen für die Gesellschaft und definiert ihn als die „Absicht, zu täuschen, um sich finanzielle oder persönliche Vorteile zu verschaffen". Seit es Menschen gibt, existiert auch das sehr menschliche Bedürfnis, zu lügen und zu betrügen.

Der Bericht liefert eine kurze Geschichte des Betrugs

Der Bericht kommt zu dem Fazit, dass digitaler Betrug zu den höchsten betrugsbedingten Verlusten geführt hat, die je im 20. und 21. Jahrhundert verzeichnet wurden. „Betrüger wünschen drei Dinge: unbemerkt zu bleiben, die Tat schnell durchführen zu können und auf naive oder unaufmerksame Opfer zu stoßen. Im Internetzeitalter werden ihnen diese drei Dinge auf dem Silbertablett präsentiert", so die Autoren des Berichts.

„Für Betrüger sind drei Bereiche besonders wichtig: Unsichtbarkeit, Schnelligkeit und das Abzielen auf die Ahnungslosigkeit der Opfer."

Auf globaler Ebene sind die Prognosen besonders besorgniserregend. Das irische Beratungsunternehmen Crowe veröffentlicht regelmäßig einen der wenigen Berichte, mit dem versucht wird, die globalen Gesamtkosten durch Betrug zu berechnen. Der Bericht von 2019 (PDF) gibt eine Summe von 5 Billionen USD an, was etwa 6 % des gesamten weltweiten BIP entspricht. Noch besorgniserregender ist, dass in den Jahren 2009 bis 2019 die Einbußen durch Betrug um mehr als 50 % gestiegen sind.

Crowe weist auf eine Konstante in diesem zehnjährigen Zeitraum hin: Betrüger nutzen immer neue Technologien für ihre Machenschaften. Mit jedem neuen Tool, mit dem sich Unternehmen vor Betrug schützen, passen auch die Betrüger ihre Techniken an, um diesen Schutz zu umgehen. Der Bericht gibt auch einen der Hauptgründe für die kontinuierlich zunehmende Zahl an Betrugsfällen an: Geschäftsführer verfolgen für gewöhnlich eine *reaktive* Herangehensweise an Betrug, wobei sie hoffen, dass es sie nicht erwischt. Tritt der Fall doch ein, geht es um Schadensbegrenzung. Eine bessere Methode zur Betrugsbekämpfung ist die Nutzung einer Online-Identitätsprüfung. Es ist heute wichtiger denn je, Kunden-Onboarding-

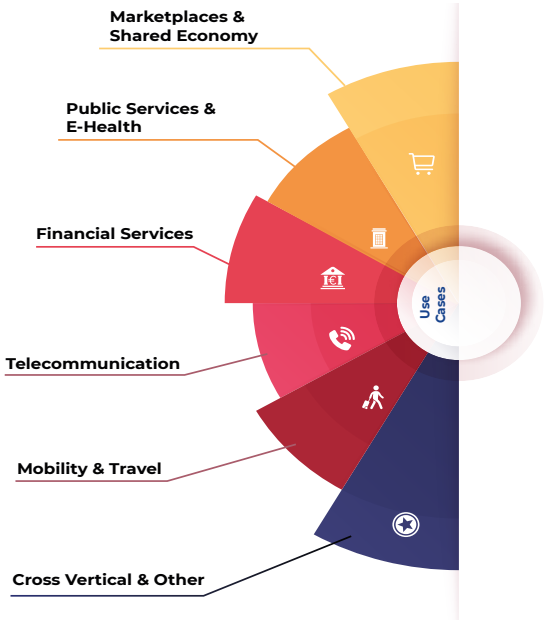
Prozesse zu verbessern und weiterzuentwickeln. Die Digitalisierung greift immer weiter um sich und Sektoren wie das Gesundheitswesen, die Telekommunikation und das Finanzwesen werden immer mehr dadurch beeinflusst, wie Kunden auf der gesamten Welt Online-Transaktionen durchführen. Besonders die wirtschaftlichen Verwerfungen durch die COVID-19-Pandemie haben erhebliche Auswirkungen auf alle Bereiche der Gesellschaft.

Angesichts der wachsenden Gefahr durch Betrug und andere Arten von Cyberkriminalität für Ihre bestehenden und zukünftigen Kunden ist es wahrscheinlich, dass auch Onboarding-Prozesse die negativen Auswirkungen zu spüren bekommen, wenn nicht bewährte Praktiken zur Identitätsprüfung angewendet werden. Wir werden auf diese Praktiken weiter unten zurückkommen. Das Wachstum einer jeden Online-Plattform sowie der Erfolg von digitalen Produkten und Dienstleistungen hängt von der erfolgreichen Verifizierung aller Benutzeridentitäten ab. Dieser Prozess, der als Identitätsprüfung bezeichnet wird, bestätigt, dass sich hinter einzelnen Benutzern eine reale Person verbirgt. So lassen sich Angriffe von Scammern und Betrügern abwehren, die bei der Verwendung gefälschter und gestohlener Identitäten immer raffinierter werden.

Stellen Sie bei der Implementierung einer Identitätsprüfungslösung sicher, dass Sie einen bewährten Anbieter mit Erfahrung in Sachen Betrugsprävention und Datensicherheit wählen. Durch die Verifizierung und Authentifizierung Ihrer Kunden können Sie die Genauigkeit und Sicherheit des Onboarding-Prozesses verbessern.

Branchen

Zahlreiche Branchen können von einer Online-Identitätsprüfungslösung profitieren. Auf unserem PXL Vision Blog finden Sie einige Beispiele. Einen kurzen Überblick bietet folgende Branchengrafik:



Wie Sie sehen können, profitieren viele verschiedene Branchen von einer Online-Identitätsprüfung. Es wird ein bedeutendes Wachstum bei Online-Marktplätzen und Finanzdienstleistungen verzeichnet, die viele relevante Anwendungsfälle für die Identitätsprüfung bieten. Gleichzeitig bietet die kontinuierliche Entwicklung des Telekommunikationsbereichs und weiterer wichtiger Branchen umfassende Möglichkeiten zur Online-Identitätsprüfung, die für Vertrauen und Sicherheit in der digitalen Welt sorgt.

Es gibt aktuell zahlreiche unterschiedliche Lösungen und Herangehensweisen für Identitätsprüfungssoftware (IDV) auf dem

Markt. Oft scheinen sie einander stark zu ähneln. Wenn ein Unternehmen eine IDV-Lösung kaufen möchte, ist es jedoch wichtig, dass die Zielsetzung dabei sehr klar formuliert ist. Eine zielgerichtete Einkaufsplanung kann den Unterschied zwischen einer erfolgreichen Implementierung und einem negativen Anwendererlebnis machen.

Die Wahl der richtigen Lösung

Zu Beginn des Einkaufsprozesses haben Unternehmen häufig eine ganze Reihe von Fragen. Darum sollten Unternehmen die unterschiedlichen Ansätze der Anbieter kennen und diesen folgende nützliche Fragen stellen:

Fragen, die vor der Kaufentscheidung beantwortet werden sollten.

- Wo werden die Daten nach der Verifizierung der einzelnen Kundentransaktionen gespeichert?
- Wie benutzerfreundlich ist die Lösung? Wie wird sich das auf die Konversionsrate auswirken?
- Wie genau ist die Lösung?
- Welche Zertifizierungen muss die Lösung im Hinblick auf Datensicherheit (DSGVO) und Branchenauflagen erfüllen? Werden sie von der Lösung erfüllt?
- Wie sieht das Provisionsmodell der Lösung aus?

Da viele Plattformen zur Online-Identitätsprüfung nicht flexibel genug sind, um an jedes Unternehmen und jedes Kunden-Onboarding-Modell angepasst zu werden, hilft unser Leitfaden dabei, die Fachsprache zu verstehen und die besten Lösungen für Ihre Branche, Ihr Unternehmen und Ihre Bedürfnisse zu identifizieren. Ganz gleich, ob Sie ein kleines oder großes Unternehmen sind oder sich einfach damit schwertun, sich zwischen einer Vielzahl von Anbietern und ähnlich klingenden Produkten zu entscheiden: Unser Leitfaden hilft Ihnen dabei, die kleinen (aber dennoch wichtigen) Unterschiede zwischen den verschiedenen Anbietern in der Branche zu erfassen.

Bei der Analyse der geeigneten Lösungen, die Ihre Anforderungen an eine automatisierte Identitätsprüfung erfüllen, müssen Sie zunächst wissen, welche Kriterien ein Verifizierungsverfahren in Ihrem Fall erfüllen muss. Zwar sind Sicherheit und Zuverlässigkeit wichtige Eigenschaften für eine Lösung, doch andere weniger wichtige Faktoren sollten nicht unterschätzt werden. Unabhängig von der jeweiligen Lösung raten wir dazu, folgende zusätzliche Eigenschaften des Anbieters zu berücksichtigen, bevor Sie sich für eine Partnerschaft entscheiden.

Es gibt keine Softwarelösung zur Identitätsprüfung, die alle Bedürfnisse aller Organisationen vollständig erfüllt. Bei unserer Zusammenarbeit mit einem großen und vielfältigen Kundenstamm aus zahlreichen unterschiedlichen Branchen mit einer Vielzahl von Anwendungsfällen haben wir festgestellt, dass jede Organisation ihre ganz eigenen Anforderungen und Präferenzen bei der Gestaltung ihrer geschäftskritischen Prozesse hat.

Bei IDV-Software müssen für gewöhnlich Kompromisse zwischen Sicherheit, Benutzererlebnis, Performance und anderen wichtigen Faktoren gemacht werden. Wir beobachten bei unseren Kunden allgemeine Muster in Sachen Anforderungen, die von der jeweiligen Branche und dem Anwendungsfall des Unternehmens abhängen.

Transparenz ist wichtig

So ergibt sich zwar ein Überblick über die Unterschiede zwischen den Branchen, doch konnten wir auch feststellen, dass selbst innerhalb desselben Marktsegments jede Organisation einzigartige Bedürfnisse hat, die sich nach der Größe, dem Ansprechpartner, der Unternehmenskultur und anderen Faktoren richten.

Damit Sie Antworten auf diese Fragen erhalten und das Thema besser verstehen können, erklären wir Ihnen in diesem Leitfaden, wie die Identitätsprüfung funktioniert, welche Betrugsarten die häufigsten sind und worauf Sie bei der idealen Lösung für Ihre einzigartigen Anforderungen achten sollten.

Wenn Sie die Lösung eines Anbieters untersuchen, versuchen Sie, folgende Fragen zu beantworten. Legen Sie dabei besonderen Fokus auf die Faktoren, die Ihnen am wichtigsten sind.

Einige dieser wichtigen Fragen sind:

- Wie groß ist Ihr Unternehmen?
- Wie viele Verifizierungen müssen Sie monatlich durchführen?
- Wünschen Sie eine plattformbasierte/ mobile App oder eine plattformunabhängige Weblösung?
- Benötigen Sie eine Cloud- oder eine On-Premise-Lösung?
- Welches Maß an Sicherheit ist für Ihr Unternehmen das richtige?
- Gibt es bestimmte regulatorische Auflagen, die Sie in Ihrer Branche beachten müssen?
- Welche Art von Benutzererlebnis (User Experience, UX) erwarten Ihre Kunden?
- Wie stellt der Anbieter eine hohe Kundenkonversionsrate sicher?
- Wie flexibel ist die Lösung bei unternehmensspezifischem Branding?
- Wie viel Erfahrung hat der Anbieter mit Projekten in Ihrer Branche?
- Wie äußern sich die Kunden des Anbieters zum Preis-Leistungs-Verhältnis, zur Zuverlässigkeit und zur Flexibilität der Lösung?
- Vertraut eine Regierung oder eine bedeutende Institution dem Anbieter?
- Gibt es einen angemessenen Entwickler-Support?
- Wo werden die Daten gespeichert?
- Über welche Art von Aftersales-Support verfügt der Anbieter?

Dieser Leitfaden soll Ihnen eine Hilfestellung bieten, damit Sie den besten Anbieter für Ihre individuellen Bedürfnisse finden, ohne Kompromisse eingehen zu müssen.

2 Wie funktioniert KI-basierte Identitätsprüfung?

In diesem Abschnitt sehen wir uns die unterschiedlichen Methoden zur Identitätsprüfung von Benutzern, die wichtigsten bewährten Praktiken der Branche und die erforderlichen Informationen vor einer Kaufentscheidung etwas genauer an.

Ältere Methoden zur Online-Identitätsprüfung basierten größtenteils auf einem unzureichenden Prozess, bei dem Menschen die von Benutzern hochgeladenen Bilder und Ausweisdokumente prüften und verglichen. Für diese Aufgabe nutzen die besten Online-Identitätsprüfungslösungen heute die neuesten Technologien in den Bereichen optische Zeichenerkennung, Computer Vision und maschinelles Lernen.

Algorithmen für maschinelles Lernen analysieren deren Output und nutzen das Ergebnis als Input für die nächste Operation. Sie lernen aus diesen Daten und lösen Probleme, die zu komplex für die Berechnung mit herkömmlicher Programmierung sind, so etwa der Abgleich des „Live-Gesichts“ einer Person mit einem Foto.

Um die Identität einer Person und deren Ausweisdokumente zu verifizieren, muss die Lösung folgende Schritte durchführen: 1) Authentizität des Ausweisdokuments verifizieren; 2) Anwesenheit einer realen Person verifizieren; 3) Zugehörigkeit des eingereichten Dokuments zu dieser Person verifizieren.

Es gibt zwar mehrere Anbieter für die Online-Identitätsprüfung auf dem Markt, doch jeder Anbieter liefert eine technologisch einzigartige Lösung. Um einen Online-Identitätsprüfungsanbieter zu bewerten, ist es wichtig, zunächst das Verfahren der Online-Identitätsprüfung verstehen.

Viele Anbieter bieten zusätzlich optionale Funktionen, um die Identität noch sicherer zu verifizieren. Auf diese Weise ermöglichen sie es den Kunden, möglichst einfach zusätzliche Schritte in ihren Prozess zu integrieren. Dazu gehören die manuelle Verifizierung, Prüfungen des Wohnsitzes, Prüfungen zu politisch exponierten Personen (PEP), die Anwendung offizieller Sanktionslisten und vieles mehr.

Der große Unterschied liegt darin, wie die einzelnen Anbieter die genannten Schritte durchführen und welche Auswirkungen die Methode auf die vorgegebenen Entscheidungsfaktoren hat, denn es gibt erhebliche Unterschiede in Sachen Sicherheit, Genauigkeit und Benutzererlebnis.

Verifizierung von Dokumenten

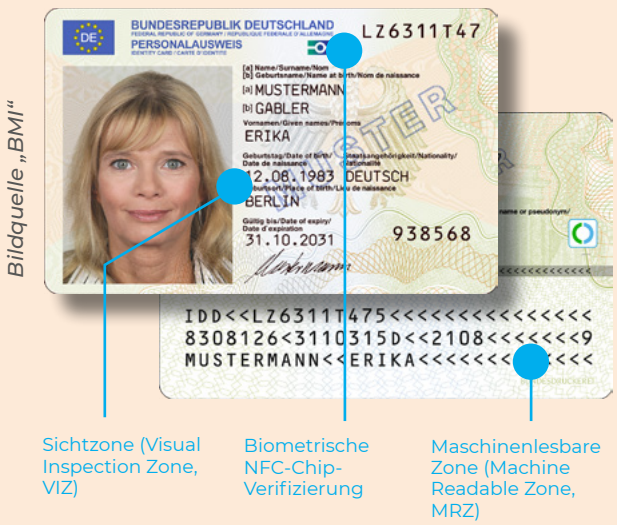
Das Herzstück aller Identitätslösungen ist die Verifizierung der Authentizität von Ausweisdokumenten.
Ein modernes Ausweisdokument verfügt über zahlreiche integrierte Sicherheitsmerkmale, die eine Identitätsprüfungslösung erfassen und verifizieren kann.

Dennoch gibt es bei der Verifizierung von Ausweisdokumenten mehrere Herausforderungen. Nehmen wir als Beispiel Reisepässe. Obwohl die Internationale Zivile Luftfahrtorganisation (ICAO), eine Sonderorganisation der Vereinten Nationen, einen Standard für die Struktur internationaler Reisedokumente (sprich Reisepässe) festgelegt hat, gibt es immer noch Hunderte unterschiedliche Reisepässe und Tausende Dokumentarten auf der ganzen Welt.

Zwar folgen viele international verwendete Ausweisdokumente dem ICAO-Standard, doch gibt es daneben zahlreiche nationale Ausweisdokumente, die eine eigene Struktur haben. Und selbst wenn die Dokumente den ICAO-Standard erfüllen, verfolgt jedes Land einen eigenen Ansatz in Sachen Design und Anwendung der physischen Sicherheitsmerkmale.

Die meisten Dokumente haben folgenden Aufbau:

- **Maschinenlesbare Zone (MRZ):** Die maschinenlesbare Zone befindet sich am unteren Rand eines Ausweisdokuments und besteht aus einigen standardisierten Zeilen mit alphanumerischen Zeichen, die die wichtigsten Identitätsinformationen wie Vorname, Nachname, Geburtsdatum usw. enthalten.
- Sichtzone (VIZ): Der Großteil des restlichen Dokuments stellt die Sichtzone dar. Sie enthält die biografischen Informationen des Passinhabers, das Foto, die Unterschrift, visuelle Sicherheitsmerkmale wie Hologramme und Lentikularbilder sowie einige Informationen über das Dokument selbst.
- Biometrischer NFC-Chip: Viele moderne Ausweisdokumente verfügen über einen integrierten digitalen Chip. Dieser Chip speichert biometrische Informationen (Fingerabdrücke, Gesichtsscans usw.) sowie zusätzliche Daten, die sich in der VIZ und in der MRZ befinden.



⚠ Um eine geeignete Identitätsprüfungslösung zu finden, ist es zunächst wichtig, die Verhaltensmuster von Betrügern und die häufigsten Betrugsmaschen zu identifizieren.

Betrug und KI-gestützte Verifizierung von Dokumenten

Bei der Betrugserkennung können sich die Lösungen im Bereich der Identitätsprüfung erheblich unterscheiden.

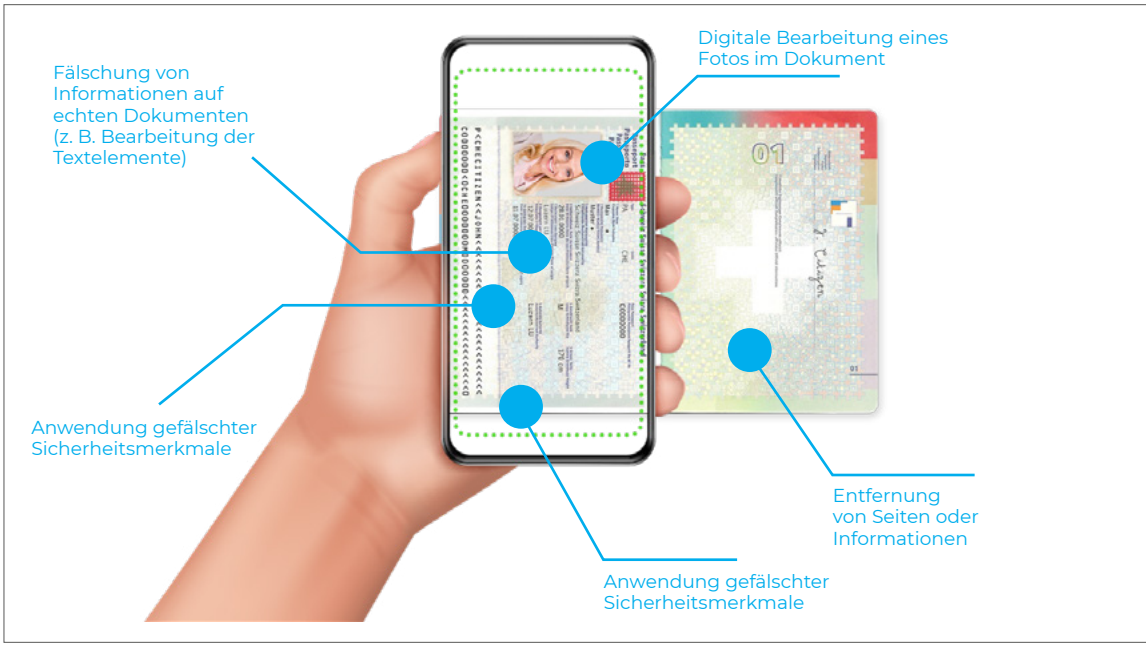
Der Großteil des Identitätsbetrugs im Internet erfolgt mittels einfacher Dokumentenfälschung oder amateurhafter Versuche (Verwendung gefälschter Dokumente oder einfacher Fälschungen mit aufgeklebten Elementen). Manche hochwertige Fälschungen werden jedoch nur von qualifizierten forensischen Experten erkannt.

Es gibt auch raffinierte Betrugsversuche mit Dokumentvorlagen und echten Dokumenten mit falschen Informationen, die kaum als solche zu erkennen sind; selbst Experten und spezialisierte Maschinen tun sich dabei schwer.

Während ein menschlicher Prüfer den Authentizitätstest in vielen dieser Fälle nicht bestehen würde, sieht es bei einer KI-gestützten Identitäts-prüfungslösung ganz anders aus.

Die bei der KI-gestützten Prüfung von Ausweisdokumenten am häufigsten festgestellten Betrugsmaschen sind:

- Fälschung von Informationen auf echten Dokumenten (z. B. Bearbeitung der Textelemente)
- Verwendung von Seiten aus zwei verschiedenen Dokumenten
- Entfernung von Seiten oder Informationen
- Anwendung gefälschter Sicherheitsmerkmale
- Digitale Bearbeitung eines Ausweisfotos
- Austausch des Ausweisfotos
- Vollständig gefälschte Dokumente
- Gestohlene Dokumentvorlagen
- Gestohlene echte Dokumente
- Fiktive Dokumente von fiktiven Behörden



Die häufigsten Betrugsversuche, die die maschinenbasierte Prüfung von Ausweisdokumenten als Ziel haben.

⚠ Wie kann man ein Ausweisdokument korrekt verifizieren? Aus Erfahrung wissen wir, dass eine Lösung fünf wichtige Bereiche berücksichtigen muss, um eine korrekte Verifizierung durchführen zu können:

1. Bilderfassung des Dokuments

Einer der wichtigsten Faktoren bei der Verifizierung ist die Art der Bilderfassung des Dokuments.

Viele Lösungen akzeptieren ein digitales Bild aus einer beliebigen Quelle. Sie bitten ihre Benutzer, ein gescanntes Dokument hochzuladen oder per E-Mail zu schicken. Dieses Bild wird anschließend verarbeitet, wobei jedoch die Wahrscheinlichkeit einer fehlgeschlagenen Verifizierung hoch ist, denn die Qualität des bereitgestellten Bildes lässt sich nicht beeinflussen.

Sie erhalten möglicherweise Bilder von schlechter Qualität oder gar Bilder, die gar keine Dokumente zeigen, was zu Abbrüchen oder einer Wiederholung des Vorgangs führt. Darum ist es wichtig, den Prozess der Bilderfassung zu kontrollieren und mehrere Echtzeitprüfungen während des Scans von Dokumenten durchführen zu können.

2. Validierung der Datenintegrität

Ein effektiver Prozess zur Dokumentenerfassung ist eine Voraussetzung für einen zuverlässigen und sicheren Identitätsprüfungsprozess.

Mit hochwertigen Dokumentenscans lassen sich die Dokumentendaten genau erfassen und auf Integrität prüfen. Die Prüfung der Dokumentenintegrität ist einer der komplexesten Bereiche bei der Verifizierung von Dokumenten und stellt eines der wichtigsten Unterscheidungsmerkmale zwischen den

Tipps zum Kauf:

- Es ist keine zuverlässige Prüfung der Sicherheitsmerkmale möglich, wenn ein Dokument mit einem einzigen Foto erfasst wird. Die Erfassung einer Videosequenz ist der bessere Ansatz. Eine Videosequenz erfasst mehrere Frames, wodurch eine zuverlässige Prüfung der Sicherheitsmerkmale des Dokuments möglich ist.
- Entscheiden Sie sich für eine Lösung, die eine Live-Erfassung von Dokumenten während des Identitätsprüfungsprozesses ermöglicht. Bilder und Videos, die außerhalb des Identitätsprüfungsprozesses erfasst werden, sind nicht zuverlässig.
- Die Lösung sollte verhindern, dass das Dokument während der Videoerfassung aus dem Blickfeld der Kamera entfernt und möglicherweise gegen ein anderes Dokument ausgetauscht wird.
- Die Lösung sollte eine Erfassung mit hoher Auflösung ermöglichen, um sicherzustellen, dass alle erforderlichen Prüfungen ausgeführt werden können.
- Die Lösung sollte sicherstellen, dass das erfasste Bild/Video nicht verschwommen ist. Das gesamte Dokument muss sichtbar sein – seine Kanten dürfen nicht abgeschnitten sein.
- Bei einer guten Lösung wird eine Benutzeroberfläche eingesetzt, die den Benutzer über Verbesserungsmöglichkeiten bei Auflösung und Aufnahmebedingungen informiert.

Lösungen dar, die aktuell auf dem Markt verfügbar sind. Es gibt Lösungen, die einfach die Informationen aus der MRZ extrahieren – ein ziemlich unkomplizierter Vorgang. Obwohl die MRZ über eine Prüfsumme verfügt, die validiert werden kann, sind nicht alle Felder (auch nicht der Vor- und Nachname des Passinhabers) in der Prüfsumme enthalten. Es gibt außerdem viele Dokumente, die den ICAO-Standard für die MRZ nicht erfüllen. Da es recht einfach ist, eine gefälschte MRZ zu erstellen, kann die korrekte Verifizierung der Dokumentenauthentizität sich nicht nur auf die Integrität der MRZ-Prüfsumme stützen. Eine fortschrittlichere Lösung extrahiert ebenfalls Informationen aus der VIZ und führt zusätzliche Prüfungen durch.

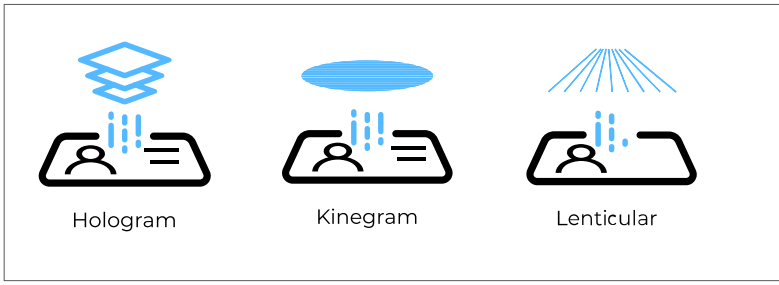
Bei der Extrahierung der VIZ gibt es jedoch ebenfalls mehrere Herausforderungen. Fast jeder Dokumententyp ist einzigartig im Hinblick auf die enthaltenen Informationen, seine Struktur, die Schriftart und Schriftgröße. Darum müssen ML-Algorithmen speziell für die genaue Extrahierung von Informationen trainiert werden. Wenn ein Anbieter eine Lösung mit hoher Genauigkeit anpreist, ist es wichtig, dass auch definiert wird, wie diese Genauigkeit zu verstehen ist.

3. Visuelle Authentizitätsprüfungen

Die Verifizierung des biometrischen NFC-Chips sorgt aktuell für die höchste Sicherheit bei der Identitätsprüfung.

Allerdings können nicht alle Benutzergeräte diesen Chip erfassen, und die meisten nationalen Ausweisdokumente wie Führerscheine oder Personalausweise verfügen noch nicht über integrierte Chips. Darum muss die Lösung des Anbieters die Authentizitätsprüfung auf Grundlage der visuellen Informationen auf dem erfassten Dokument durchführen.

Visuelle Authentizitätsprüfungen sind komplex. Dabei sind fortschrittliche Technologien in den Bereichen Computer Vision und maschinelles Lernen erforderlich, um visuelle Eigenschaften, Anomalien und Hinweise auf eine Fälschung zu erfassen. Zusätzlich ist der Abgleich des erfassten Dokuments mit einer bekannten Referenzvorlage des spezifischen Dokumententyps erforderlich. Dies reicht vom einfachen Vorlagenabgleich, bei dem die allgemeinen Merkmale des Dokuments verglichen und Datenfelder wie die VIZ zur Extrahierung von Informationen erfasst werden, bis hin zu hochkomplexen Vorgängen, bei denen Hunderte wichtiger visueller Merkmale mit der Vorlage verglichen werden.



Validierung der physischen Eigenschaften eines Dokuments

Manche Lösungen gehen sogar noch einen Schritt weiter, indem die strukturelle Integrität spezifischer physischer Sicherheitsmerkmale wie Hologramme, Kinegramme und Lentikularbilder geprüft wird.

Diese fortschrittlichen Prüfungen sind noch nicht weit verbreitet, da besondere technische Anforderungen erfüllt werden müssen.
Eine geeignete Lösung muss für jeden Dokumententyp mit tatsächlichen physischen Exemplaren manuell trainiert werden. Zum einen ist diese Herangehensweise somit weniger skalierbar. Zum anderen ist sie besonders wertvoll bei speziellen Dokumententypen für individuelle Anwendungsfälle und solche mit besonders hohen Sicherheitsanforderungen.

Tipps zum Kauf:

- Wählen Sie eine Lösung aus, die Daten sowohl aus der MRZ als auch aus der VIZ extrahiert.
- Stellen Sie sicher, dass die Lösung nicht nur die MRZ-Prüfsumme validiert, sondern auch Syntax und Logik prüft, und das auch bei Dokumenten, die nicht den ICAO-Standard erfüllen.
- Bestimmte Informationen aus der MRZ (z. B. Dokumentnummer, Geburtstag, Ablaufjahr) werden mit den Informationen aus der VIZ abgeglichen.
- Falls vorhanden, sollten Daten von biometrischen NFC-Chips extrahiert, verifiziert und mit den MRZ- und VIZ-Daten abgeglichen werden.

Tipps zum Kauf:

- Stellen Sie sicher, dass die Lösung des Anbieters das sogenannte Key Feature Template Matching verwendet, bei dem zahlreiche wichtige visuelle Merkmale (z. B. Ecken, Kanten, Datenfelder, Hintergrundmuster, Flaggen) identifiziert und mit Referenzmaterial verglichen werden, um die größtmögliche Übereinstimmung zu erzielen.
- Auch wenn es für Ihre eigenen Zwecke nicht erforderlich ist, sollten Sie dennoch einen Anbieter auswählen, der die Authentizität der physischen Sicherheitsmerkmale wie Hologramme und Lentikularbilder verifizieren kann. Stellen Sie sicher, dass eine Lösung, die über diese Funktion verfügt, sich nicht leicht von einem glänzenden, reflektierenden Material wie Alufolie täuschen lässt. Stellen Sie sicher, dass die Lösung die Struktur, den Farbverlauf und das Verhalten der Reflexion in unterschiedlichen Winkeln anhand des Referenzdokuments prüfen kann.
- Im Fall von Lentikularbildern können darin gespeicherte Informationen (z. B. die Ausweisnummer oder Dokumentennummer und das Gültigkeitsdatum bei bestimmten Dokumenten) ebenfalls extrahiert und mit den Informationen aus der MRZ verglichen werden. Vermeiden Sie Lösungen, von denen der Anbieter behauptet, dass sie diese spezifischen Merkmale auf Grundlage eines einzigen Bildes prüfen können. Bei diesen Prüfungen muss das Dokument bewegt und aus verschiedenen Winkeln analysiert werden, um ein zuverlässiges Ergebnis zu liefern.
- Weitere Prüfungen wie die Erkennung von Anomalien bei Schriftart und Schriftgröße, der korrekten Rundung der Dokumentecken, der Druckfarben usw. sind nicht zuverlässig genug.* Wenn eine Lösung behauptet, derartige Prüfungen durchzuführen, dann sollten Sie sicher sein können, dass diese Prüfungen einen Einfluss auf das Ergebnis der Dokumentenverifikation haben.
- Nutzen Sie lieber einen Anbieter, der langjährige Erfahrung im Bereich der Identitätsprüfung hat. Der Aufbau einer zuverlässigen Lösung erfordert viel Zeit und eine große Anzahl von Datensätzen, um die Machine-Learning-Algorithmen zu trainieren.
- Zahlen können täuschen: Verlassen Sie sich nicht nur auf die Anzahl an Dokumenten, die eine Lösung unterstützt. Es gibt Lösungen, die vorgeben, eine globale Abdeckung von Tausenden Dokumenten zu bieten. Versuchen Sie bei Ihren Nachforschungen zu verstehen, in welchem Umfang diese Dokumente unterstützt, welche Prüfungen durchgeführt und welche Felder extrahiert werden.
- Eine Lösung unterstützt möglicherweise 3000 Dokumententypen, kann die Authentizität aber nur bei fünf genau verifizieren. Das wäre natürlich akzeptabel, wenn diese fünf Dokumententypen genau diejenigen sind, die in Ihrem Land verwendet werden. Suchen Sie nach einer Lösung mit hoher technischer Leistung bei den wichtigsten Dokumenten für Ihren Anwendungsfall. Berücksichtigen Sie eher Lösungen, die sich leichter auf Ihre spezifischen Anforderungen ausweiten lasen.

*Quelle: interne Tests von PXL Vision mit über 100.000 Dokumenten.

4. Lebenderkennung

Alle Online-Identitätsprüfungslösungen sind für bestimmte raffinierte Arten von Presentation Attacks (Präsentationsangriffen) oder Betrug anfällig.

Identitätsprüfungslösungen müssen verifizieren, ob es sich tatsächlich um eine wirkliche Person handelt, die Zugriff wünscht. Durch die Lebenderkennung lässt sich bestimmen, ob dies der Fall ist. Sie ist unerlässlich, um Ihren Kunden eine sichere und genaue Identitätsprüfung bieten zu können.

In den letzten Jahren haben Betrüger immer neue ausgeklügelte Methoden gefunden, um biometrische Gesichtsmerkmale nachzuahmen („Spoofing“). Wir unterscheiden hier zwischen zwei Arten von Angriffen: solchen vor der Kamera und solchen hinter der Kamera.

Maskenattacke Bildschirmattacke Druckattacke

Spoofing-Angriffe vor der Kamera

Bei Angriffen vor der Kamera versucht der Angreifer, das System mithilfe einer sogenannten Presentation Attack zu täuschen. Die häufigsten Methoden bei einer Presentation Attack sind das Tragen professionell gestalteter Masken oder das Platzieren eines ausgedruckten Fotos oder eines Videoausschnitts (oder eines gerenderten Videos) einer anderen Person vor der Kamera.

Angriffe hinter der Kamera umfassen für gewöhnlich einen Angriff auf einen Server, auf dem die Lebenderkennungssoftware ausgeführt wird. Angriffe hinter der Kamera werden mit den höchsten Standards in Sachen IT-Sicherheit, Datenverschlüsselung und Kommunikation abgewehrt.

Heute entwickeln Hacker ständig neue Technologien und innovative Methoden, um Identitätsprüfungsplattformen zu überlisten. Lösungen mit einer robusten Lebenderkennung reduzieren das Risiko von Spoofing oder Presentation Attacks durch Kriminelle.

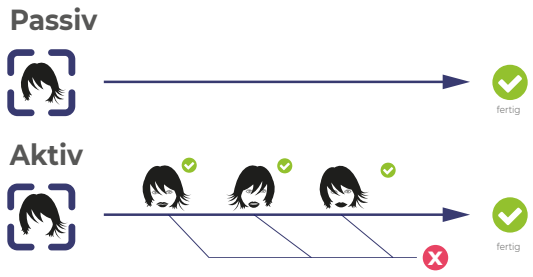
Die meisten Lösungen bieten ein Lebenderkennungstool als eine der wichtigsten Technologien ihrer Identitätsprüfungsplattform an. Die Anbieter sollten transparente Angaben zu der von ihnen genutzten Lebenderkennung machen. Informieren Sie sich diesbezüglich, bevor Sie eine Verifizierungsplattform nutzen.

Heutzutage gibt es hauptsächlich zwei Technologien für Lebenderkennung auf dem Markt: aktive und passive Lebenderkennung. Allerdings bestehen zwischen den beiden Optionen einige bedeutende technologische Unterschiede:

Bei der aktiven Lebenderkennung kommt eine „Challenger Response“-Methode zum Einsatz, bei der der Endbenutzer Anweisungen befolgen soll, bis sichergestellt ist, dass ein echter Mensch vor der Kamera sitzt. Es ist erwiesen, dass „Challenger Response“-Anweisungen zu Benutzerermüdung führen. Beispielsweise kann eine aktive Lebenderkennung Benutzer dazu auffordern, den Kopf in eine bestimmte Richtung zu drehen, zu blinzeln, zu nicken oder andere komplexere Bewegungen auszuführen, damit die Software den Benutzer verifizieren kann.

Manche Kunden brechen den Prozess ab, besonders, wenn sich wiederholende Schritte erforderlich sind. Bei passiver Lebenderkennung werden hingegen sogenannte Convolutional Neural Networks verwendet, die über eine verbesserte Tiefenanalyse verfügen, bei der die Textur und das Gesicht analysiert werden.

Bei passiver Lebenderkennung wird der Prozess für den Benutzer vereinfacht. So wird die Konversationsrate gesteigert und das Risiko von Abbrüchen reduziert. Es sind keine Interaktionen erforderlich, und der Benutzer muss nur einige Sekunden in die Kamera schauen, ohne bestimmte Anweisungen zu befolgen. Ähnlich wie bei der Authentizitätsprüfung von Dokumenten reicht ein einziges Bild für eine zuverlässige Lebenderkennung nicht aus. Ein „Selfie-Video“ ist die bevorzugte Methode für konsistente und präzise Ergebnisse bei der Lebenderkennung.



Leider sind weiterhin Lösungen auf dem Markt, bei denen die veraltete und weniger genaue aktive Lebenderkennung zum Einsatz kommt. Bevor Sie eine Kaufentscheidung treffen, stellen Sie sicher, dass die sicherere und fortschrittlichere passive Lebenderkennung zum Einsatz kommt.

5. Biometrische Verifizierung des Gesichts

Biometrische Verfahren werden seit vielen Jahren verwendet, um Menschen zu identifizieren und zu verifizieren. Die Technologie kann auf Fingerabdrücke, die menschliche Iris, Stimmfrequenzen und sogar das Gangbild angewendet werden.

Seit einiger Zeit liegt der Fokus auf Gesichtsbiometrie. Gesichtsscans lassen sich leicht durchführen. Jeder, der schon einmal ein Selfie aufgenommen hat, kann das Verfahren nutzen.Bei der Technologie zur Gesichtserkennung wird das Gesicht im Foto des Dokuments mit dem Gesicht der Person im Selfie-Video verglichen. Allerdings gibt es verschiedene Herausforderungen, die die Ergebnisse der Verifizierung beeinträchtigen können. Dazu gehören: schlechte Beleuchtung, schlechte Aufnahmequalität, minderwertige Fotos, Alterung der Person, Brillen, Bärte und sogar Stereotype im Hinblick auf die ethnische Herkunft.

Tipps zum Kauf:

- Wir empfehlen die passive Lebenderkennung für höhere Sicherheit und geringere Abbruchraten. Stellen Sie jedoch sicher, die Lösung zunächst zu testen. Lösungen, die eine passive, auf einem einzigen Bild oder auf andere Weise erbrachte Lebenderkennung anbieten, können möglicherweise nicht halten, was sie versprechen.
- Fallen Sie nicht auf falsche Werbeversprechen herein. Es gibt Anbieter (z. B. iBeta, IDIAP, TÜV IT), die Lebenderkennungstests durchführen, doch existiert keine offizielle Zertifizierung für Lebenderkennung.

Bei der Auswahl eines Anbieters sollten Sie nach einer Lösung suchen, die spezifisch für Datensätze programmiert und mit diesen trainiert und getestet wurde, die Ihrem Anwendungsfall entsprechen. Zwar gibt es keine eigentliche Zertifizierung der Gesichtserkennung, doch Organisationen wie das National Institute of Standards and Technology (NIST) in den USA führen Prüfungen und Vergleichstests von Algorithmen für die Gesichtsbiometrie durch.

Das NIST testet Algorithmen anhand mehrerer großer Datensätze von Gesichtern und stellt einen Testbericht für eine weitere Analyse bereit. Das NIST verfügt jedoch nicht über einen Datensatz zum Testen von Dokumentfotos anhand von Smartphone-Selfies, sodass das Ergebnis die Realität nicht genau abbildet. Während die daraus hervorgehenden Ergebnisse Ihnen keine Zusicherung zur Genauigkeit einer Lösung für Ihren Anwendungsfall bieten (ein Experte ist notwendig, um diese Ergebnisse verstehen und analysieren zu können), sind sie ein sehr guter Ausgangspunkt, einen Anbieter auszuwählen, der wenigsten die Vergleichstests durchlaufen hat und die nötigen Schlussfolgerungen aus den Ergebnissen zieht.

Tipps zum Kauf:

- Wählen Sie einen Anbieter, der einen Algorithmus nutzt, der spezifisch auf Ihren Anwendungsfall ausgelegt ist.
- Wählen Sie eine Lösung, die an Ihre Sicherheitsbedürfnisse angepasst werden kann.
- Wählen Sie gegebenenfalls eine Anbieterlösung, die so flexibel ist, dass ihr Modul für die Gesichtsbiometrie auch für andere Anwendungsfälle in Ihrem Unternehmen eingesetzt werden kann, z. B. für die Gesichtserkennung oder die mobile Authentifizierung.
- Fragen Sie die Anbieter, ob sie an einem Vergleichstest, beispielsweise von NIST, teilgenommen haben. Wenn das der Fall ist, fordern Sie den entsprechenden Bericht an. Lassen Sie sich von den vielen Informationen nicht einschüchtern. Mit der Art und Weise, wie der Anbieter die Ergebnisse erklärt, können Sie seine Kompetenz einschätzen.

Die Eignung einer Lösung für Ihr eigenes Unternehmen hängt von einer Vielzahl von Faktoren ab, wobei die wichtigsten der Algorithmus und die zu dessen Training verwendeten Datensätze sind. Zur Veranschaulichung dient dieses Beispiel: Wenn sich Ihr Unternehmenssitz in Asien befindet, Sie jedoch eine europäische Lösung nutzen, die speziell für die Gesichter von Europäern trainiert wurde, können die Ergebnisse beim Einsatz in Asien ernüchternd sein.

Andere Eignungsfaktoren sind:

Leistung

Einsatzmöglichkeiten

Unterstützung mehrerer Anwendungsfälle bei der Gesichtserkennung

Dynamische Konfiguration des Sicherheitslevels passend zu Ihren Anforderungen

3 Genauigkeit und Automatisierung

Oft erhalten wir die Frage: Wie akkurat arbeitet Ihre Lösung? Wir verstehen das Motiv hinter dieser Frage, doch eine einfache Antwort darauf gibt es nicht.

Das heißt nicht, dass wir nicht stolz sind auf unsere Ergebnisse; es ist einfach unmöglich, eine ehrliche, transparente Antwort zu geben, ohne mindestens einen halbtägigen Workshop durchgeführt zu haben, bei dem erläutert wurde, was Genauigkeit im Kontext von Echtzeit-Anwendungen bedeutet und wie sie gemessen wird.

Zunächst ist es wichtig, den Unterschied zwischen Genauigkeit und dem gesamten Automatisierungsgrad zu verstehen. Die Genauigkeit muss als eine Ausprägung der Verifikationsgenauigkeit jeder einzelnen Komponente oder Funktion innerhalb einer Identitätsprüfungsplattform betrachtet werden. Der gesamte Automatisierungsgrad ist der Prozentsatz der erfolgreichen Verifizierungen, die Ihren Prozess automatisch durchlaufen, ohne dass eine manuelle Prüfung oder Ablehnung der Identität erforderlich ist.

Genauigkeit

Genauigkeit muss bei jeder Funktion der Identitätsprüfung einzeln betrachtet werden. Im Verifizierungsprozess von Dokumenten gibt es unterschiedliche Genauigkeiten bei der Extraktion von Informationen aus der MRZ und der VIZ sowie bei jeder einzelnen Authentizitätsprüfung.

Wie kann also Genauigkeit gemessen und definiert werden? Üblicherweise wird eine Lösung anhand eines großen Datensatzes aus Dokumenten geprüft, zu denen bereits Grundwissen vorhanden ist. Bei jedem Feld der einzelnen Dokumente ist bekannt, wofür die einzelnen Zeichen stehen. Beim Testen einer Lösung werden Algorithmen auf diese Bilder angewendet und mit dem Grundwissen abgeglichen. Anschließend werden die Ergebnisse ausgewertet.

Die Genauigkeit lässt sich auf unterschiedliche Weise berechnen: Sie können die Anzahl der fehlerhaft extrahierten Zeichen durch die Gesamtzahl der Zeichen dividieren, um eine Fehlerrate zu erhalten, oder Sie können die Anzahl der fehlerhaft extrahierten Felder (wenn ein oder mehrere Zeichen falsch waren) durch die Gesamtzahl der Felder dividieren. Sie können alternativ festlegen, dass die gesamte Verifizierung des Dokuments fehlgeschlagen ist, auch wenn nur ein Zeichen falsch war, und die Anzahl der fehlerhaft extrahierten Dokumente durch die Gesamtzahl der Dokumente teilen. Somit kann man drei unterschiedliche Genauigkeitsergebnisse für dieselben Dokumente und dieselbe Lösung erhalten, die drei unterschiedliche Botschaften vermitteln. Zusammenfassend hängt das Genauigkeitsergebnis von der Herangehensweise und von der Definition einer fehlgeschlagenen Verifizierung ab.

Obwohl es bei der Gesichtserkennung und der Lebenderkennung einfacher scheint, da es sich jeweils nur um ein einziges Merkmal handelt,

ist dies nicht ganz zutreffend. Tatsächlich ist es etwas klarer und standardisierter. Dasselbe gilt für die Genauigkeit einer Lösung, wenn man einen Algorithmus auf einen großen Datensatz aus Bildern oder Videos anwendet. Je mehr diese Datensätze zu unserem spezifischen Anwendungsfall passen (Dokumentbild gegen Selfie-Video), desto zuverlässiger wird das Ergebnis.

Um diese Ergebnisse zu verstehen, müsste man einen technischen Workshop besuchen. Im Wesentlichen wird das Ergebnis von einem Konfidenzwert und einem Übereinstimmungsschwellenwert bestimmt. Bei der Gesichtserkennung bestimmt der Konfidenzwert, wie ähnlich zwei erfasste Gesichter sind. Unterschiedliche Algorithmen haben unterschiedliche Ansätze zur Messung und Quantifizierung von Konfidenzwerten. Beispielsweise kann der Wert zwischen 0 und 1 liegen, wobei 0 die geringste Ähnlichkeit und 1 die größte Ähnlichkeit darstellt. Der Konfidenzwert wird anschließend mit einem voreingestellten Übereinstimmungsschwellenwert abgeglichen. Das System gibt an, dass ein Gesicht einem anderen entspricht, wenn der Konfidenzwert über dem Schwellenwert liegt. Der Konfidenzwert ist nicht einem Prozentwert gleichzusetzen und drückt keine „Wahrscheinlichkeit“ und kein „Vertrauen“ in die angezeigten Ergebnisse aus. Beispielsweise garantiert ein Konfidenzwert von 1 auf einer Skala von 0 bis 1 nicht, dass zwei Gesichter zur selben Person gehören. Er sagt vielmehr aus, dass das System auf der Grundlage seiner Auslegung und seines Trainings voraussagt, dass die Bilder mit sehr hoher Wahrscheinlichkeit derselben Person zuzuordnen sind.

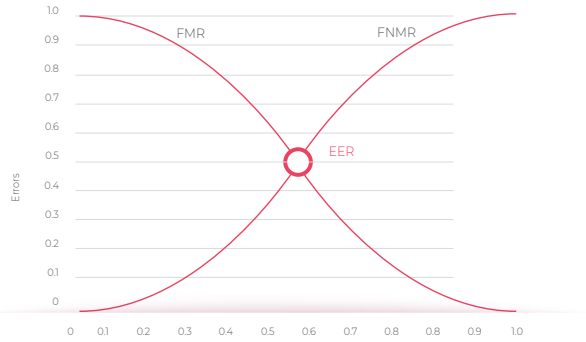
Die Konfidenzwerte werden vom Algorithmus automatisch ermittelt, während die Schwellenwerte von Menschen (Entwicklern und/oder Benutzern) eingestellt werden. Der Schwellenwert bestimmt, welche Bilder/Videos das System für eine mögliche Übereinstimmung akzeptiert. Ein höherer Schwellenwert ergibt somit weniger akzeptierte Ergebnisse und es besteht die Möglichkeit, dass eine potenzielle Übereinstimmung nicht berücksichtigt wurde. Auf der anderen Seite werden bei einem geringeren Schwellenwert mehr Bilder als Übereinstimmungen akzeptiert, wobei eine größere Wahrscheinlichkeit besteht, dass falsche Vorhersagen getroffen werden.

Da die Schwellenwerte anpassbar sind, haben sie für sich genommen keine Aussagekraft und bieten keinen Rückschluss auf die Genauigkeit eines Systems. Wenn der Übereinstimmungsschwellenwert z. B. hoch eingestellt wird, bedeutet dies noch lange nicht, dass die Ergebnisse genauer werden. Vielmehr bestimmen der spezifische Anwendungsfall und Ihre Anforderungen an das System, wie der Übereinstimmungsschwellenwert eingestellt werden sollte. Diese Entscheidung beinhaltet komplexe, praxisbezogene Kompromisse.

Vergleichstests

Bei der Identitätsprüfung kann ein geringer Übereinstimmungsschwellenwert ein False Positive ergeben und eine Person irrtümlicherweise verifizieren. Das könnte dazu führen, dass eine unautorisierte Person Zugang zu Waren, Dienstleistungen oder einem Gebäude erhält.

Wenn der Übereinstimmungsschwellenwert zu hoch eingestellt wird, kann dies zu False Negatives führen und verhindern, dass sich jemand verifizieren lassen kann. Dies führt zu Abbrüchen im Onboarding-Prozess.



FMR = Falschakzeptanzrate, FNMR = Falschzurückweisungsrate, EER = Gleichfehlerrate

Wenn Sie sich für einen Anbieter digitaler Identitätsprüfungslösungen entscheiden, sollten Sie auch wissen, wie Gesichtserkennungsalgorithmen funktionieren und weshalb es bei dieser Technologie bestimmte Einschränkungen geben kann. Genauso wie Menschen können auch Computer Fehler machen – beispielsweise durch falsche Akzeptanz oder falsche Zurückweisung während der Identitätsprüfung.

Falsche Akzeptanz tritt auf, wenn der Algorithmus irrtümlicherweise eine Übereinstimmung zwischen zwei unterschiedlichen Gesichtern feststellt. Das Gegenteil tritt bei der falschen Zurückweisung auf. Bei einer falschen Zurückweisung wird KEINE Übereinstimmung zwischen zwei Bildern festgestellt, obwohl es sich um dieselbe Person handelt.

Fehlgeschlagene Gesichtserkennung

Wenn biometrische Algorithmen irrtümlicherweise zwei Bilder ein und derselben Person zwei verschiedenen Personen zuordnen, schlägt sich das in der Falschzurückweisungsrate nieder, die den Anteil der falschen Zurückweisungen oder False Negatives misst. Genauso steht die Falschakzeptanzrate direkt mit dem Anteil der falschen Übereinstimmungen oder False Positives im Verhältnis.

Einige wichtige Bezeichnungen:
FMR = Falschakzeptanzrate
FNMR = Falschzurückweisungsrate
EER = Gleichfehlerrate

Bei Vergleichstests einer Gesichtserkennungslösung mit einer spezifischen Bilddatenbank wird der Konfidenzwert für gewöhnlich auf einer Grenzwertoptimierungskurve oder auch ROC-

Kurve dargestellt. Die Kurve stellt eine Vorhersage dar, wie viele False Positives und False Negatives beim ausgewählten Schwellenwert an jedem Punkt der Kurve zu erwarten sind. Die Ergebnisse hängen stark von der Bilddatenbank ab, mit der die Algorithmen trainiert werden, sowie von der Bilddatenbank, auf die sie angewendet werden. Wenn Sie denselben Datensatz für den Test verwenden, den Sie bereits für das Training verwendet haben, erhalten Sie immer gute Ergebnisse. Das entspricht jedoch nicht den realen Bedingungen. Eine Lösung etwa, die vor allem mit den Bildern von Europäern trainiert wurde, tut sich bei Gesichtern dunkelhäutiger Menschen schwer. Dasselbe gilt auch für die Lebenderkennung.

Wenn Ihnen ein Anbieter auf Ihre Frage sagt, dass er eine Genauigkeit von 99,9 % erzielt, ist das äußerst fragwürdig, es sei denn, er kann Ihnen im Detail erklären, wie er zu diesen Ergebnissen gekommen ist. Es ist leicht, einen Testdatensatz zu erzeugen, mit dem sich eine Genauigkeit von 100 % erzielen lässt, doch das bedeutet nicht, dass die Ergebnisse in der Realität in der Nähe von 100 % liegen werden. Die richtige Antwort auf die Frage nach der Genauigkeit ist darum „das hängt von verschiedenen Faktoren ab“, gefolgt von einer genaueren Erklärung.

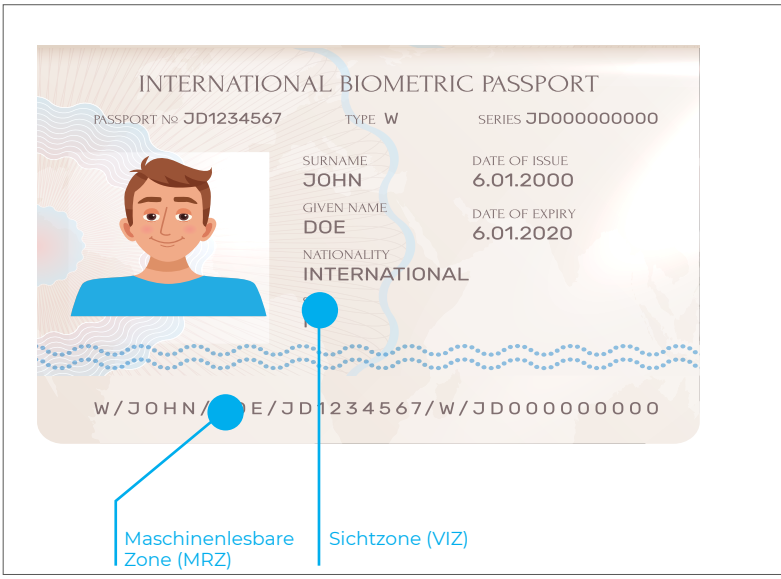
Automatisierung

Was letztlich ausschlaggebend ist, ist der allgemeine Automatisierungsgrad Ihres Anwendungsfalls. Sie möchten erfahren, wie viele Identitätsprüfungen den gesamten Prozess automatisch durchlaufen können und wie viele False Positives und False Negatives es über alle Prüfungsschritte hinweg gibt.

Der Automatisierungsgrad hängt tatsächlich von einer Vielzahl von Faktoren ab, etwa von der Konfiguration der Unternehmensregeln und den Anforderungen Ihres spezifischen Anwendungsfalls.

Wenn Sie aber beispielsweise darauf bestehen, dass bei jedem Dokumententyp jedes einzelne Zeichen aus der MRZ mit jedem einzelnen Zeichen in der VIZ übereinstimmt, wird Ihr Automatisierungsgrad deutlich sinken. Betrachten wir den Namen einer Person in einem offiziellen Ausweisdokument. Der Name in der MRZ wird nicht von der Prüfsumme abgedeckt und die verwendete OCR-B-Schriftart lässt keine Sonderzeichen zu. Hinzu kommt, dass längere Namen in der MRZ verkürzt werden. Wenn Sie also diese äußerst strenge Regel anwenden, werden alle Dokumentinhaber mit einem langen Namen oder einem Namen mit Sonderzeichen aus dem automatisierten Prozess geworfen. Als Folge steigt Ihre Falschzurückweisungsrate.

Wenn Ihnen zusätzliche Sicherheit jedoch nicht so wichtig ist und Sie nur eine einfache Altersverifizierung durchführen möchten, können Sie den allgemeinen Automatisierungsgrad steigern, indem Sie sich nur auf die MRZ konzentrieren und die VIZ überhaupt nicht prüfen.



Wenn Sie darauf bestehen, dass bei jedem Dokumententyp jedes einzelne Zeichen aus der MRZ mit jedem einzelnen Zeichen in der VIZ übereinstimmt, wird Ihr Automatisierungsgrad deutlich sinken.

Tipps zum Kauf:

- Fragen Sie die Anbieter in Ihrer engeren Auswahl, wie genau ihre Lösung ist. Wenn sie mit einer einfachen Zahl wie 99 % oder gar 100 % antworten, liefern sie entweder falsche Informationen oder haben nicht das nötige Know-how, um die Frage zu beantworten.
- Arbeiten Sie bevorzugt mit einem Anbieter zusammen, der transparent mit den verschiedenen Vor- und Nachteilen sowie Abhängigkeiten bei der Identitätsprüfung umgeht. Die Erklärung des technischen Zusammenhangs und Einblicke in den Prozess sorgen für Vertrauen und Transparenz.
- Wählen Sie einen Anbieter, der die Genauigkeit und Automatisierung an Ihre individuellen Anwendungsfälle anpassen kann.

4 Benutzererlebnis (User Experience, UX)

Wir haben bereits die Sicherheit, Genauigkeit und Zuverlässigkeit von Identitätsprüfungslösungen behandelt. Jedoch ist die beste Lösung wertlos, wenn Ihre Kunden den Identifizierungsprozess nicht abschließen können.

Darum ist ein bequemer und optimierter Online-Identitätsprüfungsprozess erforderlich. Die erfolgreichsten digitalen Onboarding-Plattformen wurden alle mit dem Hauptaugen-merk auf die UX entwickelt, denn eine bessere UX führt zu höheren Kundenkonversionsraten.

Die Benutzererwartungen an den digitalen Onboarding-Prozess zu erfüllen ist die größte Hürde. Beispielsweise sind bei E-Commerce-Plattformen die beiden Hauptkriterien für eine Identitätsprüfungsplattform Geschwindigkeit und Benutzerfreundlichkeit. Wenn der Prozess zu zeitaufwendig oder zu kompliziert ist, besteht das Risiko des Abbruchs und sinkender Umsatzzahlen. Hohe Abbruchraten bei Online-Identitätsprüfungslösungen lassen sich häufig auf eine schwache UX zurückführen. Bei manchen Identitätsprüfungslösungen auf dem europäischen Markt wird sogar von Abbruchraten zwischen 40 und 50 Prozent berichtet. Mithilfe der folgenden Punkte können Sie die Identitätsprüfungsplattform finden, die die Anforderungen Ihres Unternehmens erfüllt:

Weniger ist mehr

Für eine gute UX sollte es im Laufe des Onboarding-Prozesses so wenige Einzelbildschirme geben wie möglich, da diese sich direkt auf die Dauer des Onboardings auswirken. Die Anzeige der Bildschirmanzahl, bei der die Nummer des aktuellen Bildschirms und die Zahl der noch verbleibenden Bildschirme angegeben wird, ist eine bewährte Praxis. Im Allgemeinen sollten Sie die erforderliche Benutzerinteraktion so weit wie möglich reduzieren: Jeder Klick und jede Bewegung, die der Benutzer ausführen muss, erhöht die Wahrscheinlichkeit eines Abbruchs.

Außerdem fühlen sich die meisten Menschen nicht sofort wohl damit, ihre Identität über ein mit dem Internet verbundenes Gerät zu verifizieren; darum helfen eindeutige Anleitungen.

Um besser beurteilen zu können, wie stark die Benutzerfreundlichkeit bei einem Anbieter von ID-Verifizierungslösungen berücksichtigt wird, sollten Sie sich für ein Unternehmen entscheiden, das über UX-Spezialisten verfügt, die das gesamte Kunden- und UX-Design maßgeblich mitgestalten.

Idealerweise wird der Benutzer Schritt für Schritt durch den Onboarding-Prozess geführt. Bei der Zusammenstellung von Code für eine Identitätsprüfungsplattform verbringen Entwickler häufig zu viel Zeit mit Fragen der Funktionalität, da dies ihre Hauptaufgabe ist. Der UX wird dabei zu wenig Beachtung geschenkt.

Wenn Sie nach einer Lösung suchen, kann das Kürzel KISS* für „Keep It Simple Stupid“ helfen.

Das KISS-Prinzip geht davon aus, dass die meisten Systeme dann am besten funktionieren, wenn sie möglichst einfach sind. Darum sollte Einfachheit eine wichtige Zielsetzung bei der Entwicklung sein und unnötige Komplexität vermieden werden. Ein übermäßig komplizierter Onboarding-Prozess führt dazu, dass viele potenzielle Neukunden ihn abbrechen.

Beim Erfassungsprozess etwa (den wir oben besprochen haben) übernehmen die besten Identitätsprüfungslösungen die volle Kontrolle über den Prozess, leiten den Benutzer an und liefern Feedback in Echtzeit. So wird sichergestellt, dass die Bildqualität hoch genug ist, um Wiederholungen zu vermeiden.

Manche Lösungen fragen den Benutzer auch nach dem Dokumententyp und dem Ursprungsland. Zwar können Algorithmen so bei den erwarteten Dokumententypen ein besseres Ergebnis erzielen, doch bereitet es ihnen Schwierigkeiten, wenn der Benutzer dann ein anderes Dokument scannt als das, was er ursprünglich ausgewählt hat. Auch wenn es sich hier um einen Bedienfehler handelt, muss der Schritt wiederholt werden, was zu Frustration und zu einem möglichen Abbruch führen kann.

Eine andere Schwachstelle vieler Lösungen ist das Lebenderkennungsmodul.

Die aktive Lebenderkennung verlangt vom Benutzer eine Reihe spezifischer Bewegungen, was zu einer höheren Abbruchrate bei Ihrem Onboarding-Prozess führen wird. Bei der passiven Lebenderkennung muss der Benutzer nur einige Sekunden vor der Kamera stillhalten – das schafft der Großteil der Benutzer.

Zuletzt sollten auch die Sprachen des Zielmarktes berücksichtigt werden. Als international gebräuchliche Geschäftssprache eignet sich Englisch für die meisten Endbenutzer, doch zusätzliche Sprachen machen den Onboarding-Prozess für Menschen, die nicht über umfangreiche Fremdsprachenkenntnisse verfügen, deutlich einfacher. Wenn man eine markenspezifische Standalone-Lösung verwendet, müssen alle erforderlichen Sprachen abgedeckt sein.

Es gibt auch Anbieter, die White-Label-Lösungen bereitstellen, bei denen Sie die UX komplett anpassen können, und das nicht nur in Sachen Branding, sondern auch bei der Sprache.

Workflow und Support für die Plattform

Der allgemeine Workflow und die Interaktion mit Ihren bestehenden Geschäftsprozessen ist genauso wichtig wie die tatsächliche Verifizierung. Ein stark in Ihre bestehenden Prozesse integrierter Workflow sorgt dafür, dass sich die Benutzer bei Ihrer Marke „zu Hause“ fühlen, wodurch die Wahrscheinlichkeit eines Abbruchs verringert wird.

Manche Anbieter haben sehr strikte Prozesse und begrenzte Integrationsmöglichkeiten. Wenn ein Benutzer zwingend eine externe mobile App herunterladen muss, um die Verifizierung durchzuführen, ist ein Abbruch quasi vorprogrammiert. Identitätsprüfungslösungen müssen in verschiedenen Plattformen eingesetzt werden können und sich an Ihre spezifischen Bedürfnisse und Workflows anpassen lassen.

Auch wenn die meisten Menschen einen PC oder einen Laptop als Hauptgerät verwenden, funktionieren die Identitätsprüfungsplattformen vieler Anbieter nur auf Smartphones. Smartphones

*Dieses Akronym wurde von einem Ingenieur der US Navy geprägt, als sein Team eine Jet-Turbine entwickelte, die von einem durchschnittlichen Mechaniker im Feld unter Gefechtsbedingungen gewartet werden konnte.

sind die wichtigsten Treiber hinter dem Wandel auf dem Markt für Identitätsprüfung. Der Grund dafür liegt in den verbesserten Kamerasensoren moderner Handys, die auch bei schlechten Lichtverhältnissen gut funktionieren und über leistungsstarke Betriebssysteme verfügen. Diese Aspekte haben die Entwicklungen auf dem Markt für Online-Identitätsprüfung in den letzten Jahren beschleunigt.

Der Leistungsunterschied zwischen PCs und Smartphones wird immer kleiner, weshalb der Trend einer stärkeren Smartphone-Nutzung bestehen bleiben wird.* Laut einem Bericht waren Ende 2017 4,3 Milliarden Smartphones in Nutzung – dreimal mehr als PCs. Die Zahl der Smartphone-Nutzer wird voraussichtlich jährlich um 9 Prozent wachsen und soll bis 2023 7,2 Milliarden Nutzer erreichen.

Jedoch gibt es immer noch viele Menschen, die einen PC bzw. einen Laptop als Hauptgerät verwenden, sodass manche Anbieter diese Plattformen ebenfalls unterstützen. Das Problem bei PCs ist zum einen die Komplexität und zum anderen sind es die nahezu unbegrenzten Kombinationsmöglichkeiten aus Kameras, Betriebssystemen und Treibern. Alle diese Kombinationen zu unterstützen und tatsächlich zu testen ist nahezu unmöglich, ganz zu schweigen davon, dass viele Systeme überhaupt nicht über eine Kamera verfügen. Selbst wenn eine Kamera vorhanden ist, sind die Bilder mancher Modelle spiegelverkehrt, sodass es schwierig ist, ein Dokument korrekt vor einer Kamera zu positionieren, besonders dann, wenn man dadurch den eigenen Blick auf den Bildschirm verdeckt.

Darum empfehlen wir, eine Smartphone-basierte Verifizierung mithilfe von QR-Code, E-Mail oder SMS-Link einzurichten.

*Samsungs Veröffentlichung „Insights“.

Tipps zum Kauf:

- Geschwindigkeit und Genauigkeit sind zwei Variablen, die häufig im Konflikt miteinander stehen. Das ist besonders der Fall, wenn bei Online-Identitätsprüfungsplattformen Geschwindigkeit gefordert ist, denn dies geschieht oft zu Ungunsten der Genauigkeit. Wir empfehlen Ihnen, nach Lösungen Ausschau zu halten, die Geschwindigkeit bei minimaler Interaktion mit dem Benutzer sowie eine optimierte UX bieten, und bei denen Genauigkeit dennoch einen hohen Stellenwert hat.
- Eine Spitzenlösung sollte nicht länger als 30 bis 60 Sekunden brauchen, um eine vollständige Identitätsprüfung durchzuführen.
- Entscheiden Sie sich für eine Lösung, die auf Ihre spezifischen UX- und Workflow-Bedürfnisse angepasst werden kann.
- Wählen Sie eine Lösung, die den Benutzer durch den Verifizierungsprozess führt und sofortiges Feedback liefert. Vermeiden Sie es, Benutzer fünf Minuten lang warten zu lassen, bis sie schließlich erfahren, dass sie den Prozess erneut starten müssen.
- Wählen Sie eine Lösung, die passive Lebenderkennung anstatt aktiver Lebenderkennung verwendet und bei der die Benutzer nicht zuerst den Dokumententyp auswählen oder Bilder manuell erfassen und hochladen müssen.

5 Flexibilität und Konfigurierbarkeit

Je größer und erfolgreicher ein Unternehmen wird, desto mehr Einfluss hat ein Identitätsprüfungsprozess auf sein Geschäft.

Kleine, mittelständische und große Unternehmen haben abhängig von ihren Anwendungsfällen unterschiedliche Anforderungen. Selbst bei demselben Anwendungsfall in derselben Branche haben zwei Unternehmen ähnlicher Größe ganz einzigartige Anforderungen und Präferenzen in Sachen Identitätsprüfung. Identitätsprüfung ist selten eine Anforderung, die mit einer Standalone-Lösung umgesetzt werden kann, da sie in die bestehenden Prozesse der Organisation integriert werden muss. Dazu gehören die vorhandenen IT-Umgebungen und Unternehmensregeln.

Auf der Suche nach einem Partner im Bereich der Identitätsprüfung sollten Sie sich für eine Lösung oder Plattform entscheiden, die maximale Flexibilität und Konfigurierbarkeit bietet und mit Ihrem Unternehmen wachsen kann. Mit Flexibilität und Konfigurierbarkeit meinen wir in erster Linie die Möglichkeit, die angewendeten Unternehmensregeln und die Verifizierungslogik zur Akzeptanz oder Zurückweisung einer Identität anzupassen und zu verfeinern. Hinzu kommen die unterschiedlichen Möglichkeiten der Integration und Bereitstellung einer Lösung innerhalb Ihrer IT-Umgebung und Ihrer Geschäftsprozesse.

Unternehmensregeln und Verifizierungslogik

Unternehmensregeln sind die einzigartigen Anforderungen oder Filter Ihres Unternehmens, die auf Ihren Anwendungsfall angewendet werden sollen.

Da wir Identitätsprüfungslösungen vollkommen neu entwickeln, haben wir gelernt, dass jedes Unternehmen einzigartig ist und eigene Ansätze fordert.

Identitätsprüfungsplattformen sollten so flexibel und konfigurierbar sein, dass sie an die Bedürfnisse Ihres

Beispiele für Filter, die dabei helfen, den effizientesten und genauesten Onboarding-Prozess zu schaffen:

Welche Dokumententypen und Nationalitäten sollten erlaubt, welche abgelehnt werden?

Welche Datenintegrationen und Validierungsprüfungen sind verpflichtend, welche optional?

Welche Authentizitätsprüfungen (z. B. NFC-Verifizierung) sind verpflichtend?

Wie oft sollte ein Nutzer den Prozess nach einem Fehlversuch wiederholen dürfen?

Welche Schwellenwerte sollten auf die Gesichtsverifizierung und die Lebenderkennung angewendet werden?

Wie sollte mit abgelaufenen Dokumenten umgegangen werden?

Unternehmens angepasst werden können. Unternehmensregeln lassen sich auf Menschen, Prozesse, Unternehmensverhalten und Computersysteme in einer Organisation anwenden. Ihre Aufgabe ist es, die Organisation beim Erreichen ihrer Ziele zu unterstützen. Im Wesentlichen definieren Unternehmensregeln die Kriterien, die zur Akzeptanz oder Zurückweisung einer Identität erfüllt werden müssen. Diese Kriterien werden nicht nur vom Identitätsprüfungsprozess bestimmt, sondern auch von gesetzlichen und regulatorischen Anforderungen, unternehmensinterner Compliance oder den Präferenzen der einzelnen Unternehmen. Die Entscheidung, ob eine Identität akzeptiert oder zurückgewiesen wird, sollte idealerweise bei Ihnen liegen – keine Lösung sollte Ihnen diese Entscheidung abnehmen.

Viele Lösungen liefern ein simples Ergebnis nach dem Schema „bestanden/nicht bestanden“. Für manche Unternehmen und Anwendungsfälle kann das ausreichen und grundlegende Anforderungen erfüllen, so etwa bei Fragen der Compliance. Jedoch lassen sich daraus keine Rückschlüsse auf den allgemeinen Erfolg oder die Verbesserungsmöglichkeiten für Ihre spezifischen Möglichkeiten ziehen.

Ein guter Anbieter liefert Ihnen alle erforderlichen Informationen, damit Sie auf Grundlage Ihrer Filterkriterien eine fundierte Entscheidung treffen können, ob eine Identität akzeptiert oder zurückgewiesen werden soll. Die besten Lösungen geben Ihnen außerdem die Flexibilität, Ihre Filterkriterien oder Unternehmensregeln als Teil des Prozesses direkt anzuwenden und diese mit der Zeit dynamisch anzupassen. Derartige Lösungen helfen Ihnen auch bei einer Vielzahl von Szenarien, etwa bei unerwarteten Zurückweisungen.

Die Anwendung der Unternehmensregeln als Teil des Prozesses hat weitreichende Auswirkungen auf die UX, den allgemeinen Automatisierungsrad Ihres Unternehmens sowie letztlich auf die Gesamtbetriebskosten. Wenn Sie als Einzelhändler beispielsweise Alkohol und Tabak online verkaufen möchten, unterliegen Sie höchstwahrscheinlich nicht denselben regulatorischen Auflagen wie eine Bank beim Onboarding neuer Kunden. Als Einzelhändler müssen Sie lediglich wissen, dass die Person mindestens 18 Jahre alt ist. Dazu reicht möglicherweise selbst ein abgelaufenes Dokument. Darum würde ein sehr strenger Identitätsprüfungsprozess mit der Prüfung zahlreicher Details zu einer hohen Abbruchrate und Umsatzeinbußen führen. Eine Bank muss hingegen deutlich strengere Anforderungen erfüllen.

Es gibt Lösungen, die diese Anforderung an Flexibilität erfüllen, indem verschiedene Prüfungen durchgeführt werden können, die Fehlercodes ausgeben, auf die reagiert werden kann – entweder dynamisch während des Prüfungsprozesses oder später.

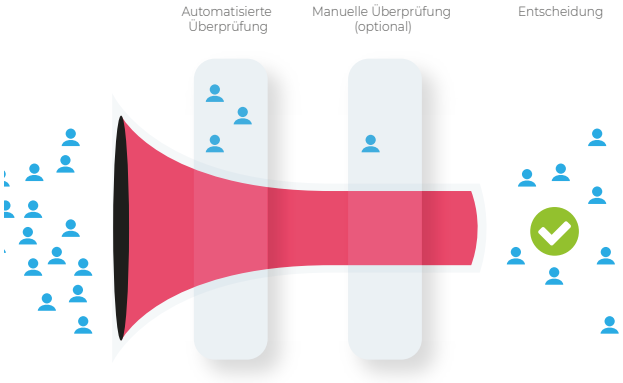
Es gibt Hunderte mögliche Fehlermeldungen, darunter:

- zu geringe Bildauflösung
- Dokument nicht erkannt
- Dokument abgelaufen
- Gesicht nicht erkannt
- spezifische MRZ-Felder ungültig
- Gesichtsverifikation fehlgeschlagen
- verschwommenes Bild

Die besten Lösungen nutzen derartige Fehlercodes in Echtzeit während des Prüfungsprozesses. Diese Fehler helfen auch dabei, eine Vielzahl von Onboarding-Anforderungen zu erfassen und zu bestimmen, ob diese als Blocking-Fehler oder als Non-Blocking-Fehler klassifiziert werden. Blocking-Fehler führen zum Abbruch oder zur Wiederholung des Prozesses; bei Non-Blocking-Fehlern erfolgt die Verifizierung trotz bestimmter Fehler.

Für Ihr Unternehmen ist es ausschlaggebend, zu wissen, welche Kriterien wichtig sind und wie sich die Lösung in verschiedenen Situationen verhält. Für Einzelhändler ist beispielsweise der mögliche finanzielle Schaden durch einen Betrüger deutlich niedriger als für eine Bank. Wenn die Sicherheitsanforderungen und die Regulierungen des Bankenwesens für Sie nicht von Bedeutung sind und Sie den Prozess so optimieren möchten, dass er eine möglichst hohe Konversionsrate erzielt, sollten Sie so viele Verifizierungen ermöglichen wie möglich, selbst wenn Sie dazu abgelaufene Dokumente und/oder unscharfe Bilder akzeptieren müssen.

Sie sollten auch toleranter bei den Schwellenwerten für die Gesichtserkennung und die Lebenderkennung sein. Als Bank sollten Sie jedoch streng sein und alle Auflagen erfüllen. Durch Fehlercodes, die bestimmte Fälle im Identitätsprüfungsprozess zurückweisen, können Sie den allgemeinen Automatisierungsgrad steigern und den Aufwand senken, sich durch Fehler und Verifizierungen kämpfen zu müssen, die an Ihr Backend weitergeleitet werden.



Ein weiterer Vorteil der dynamischen Anwendung von Unternehmensregeln und Fehlercodes ist die Behandlung unterschiedlicher Szenarien. Im Idealfall funktioniert alles bestens und Identitäten werden automatisch verifiziert. In vielen Fällen ist dies jedoch nicht so eindeutig, da die Lösung sich nicht ganz sicher ist und bestimmte Unternehmensregeln nicht erfüllt werden. Anstatt den Benutzer zurückzuweisen, können diese Informationen an einen Backoffice-Mitarbeiter weitergeleitet werden, der als Fallback-Option eine manuelle Verifizierung

durchführt. Wenngleich dieser Ansatz den Automatisierungsgrad senkt, hilft er dabei, potenzielle Kunden besser zu verwalten und die allgemeine Konversionsrate zu steigern.

Die meisten Identitätsprüfungslösungen, die heute auf dem Markt sind, sind auf einen größtmöglichen Automatisierungsgrad ausgelegt. In der Realität ist dies jedoch schwieriger umzusetzen.

Eine hochgradig konfigurierbare Verifizierungslösung ist der Schlüssel, damit Ihr Onboarding-Prozess auf Ihre Bedürfnisse in Sachen UX, Sicherheit, Compliance und Automatisierung ausgerichtet werden kann.

Ein gut aufgestellter Anbieter hilft Ihnen dabei, diese Anforderungen zu identifizieren, und definiert in Zusammenarbeit mit Ihrem Unternehmen die unterschiedlichen Filter (Unternehmensregeln), die im Identitätsprüfungsprozess angewendet werden sollen. Dank dieser Zusammenarbeit wird die Lösung auf Grundlage Ihrer Bedürfnisse für optimale Ergebnisse sorgen. Die besten Lösungen geben Ihnen die Möglichkeit, Unternehmensregeln selbst auf transaktionaler Basis zu definieren, wodurch sie sich abhängig von bestimmten Anwendereigenschaften dynamisch anpassen lassen. So kann nicht nur der allgemeine Automatisierungsgrad weiter gesteigert werden, Sie können so auch mehrere unterschiedliche Anwendungsfälle mit derselben Lösungsimplementierung abdecken, was die Gesamtkosten senkt.

Bei manchen Lösungen kommen standardmäßig auch menschliche Operatoren im Identitätsprüfungsprozess zum Einsatz. Allerdings gibt es wissenschaftliche Studien, dass bestimmte Vorurteile im Hinblick auf Geschlecht und Ethnie dazu führen können, dass menschliche Operatoren die Identität von Personen (möglicherweise unbewusst) inkorrekt verifizieren. Durch die Beteiligung von menschlichen Operatoren können auch regulatorische und datenschutzrechtliche Hürden auftreten.

Wenn Ihr Unternehmen in der EU ansässig ist, Ihr Anbieter jedoch menschliche Operatoren in Indien einsetzt, erfüllt die Lösung möglicherweise nicht die in Ihrem Land geltenden Datenschutzverordnungen. Je nach Ihren Anforderungen sollten Sie vielleicht ganz auf menschliche Operatoren verzichten oder zumindest auf die eigenen Mitarbeiter zurückgreifen können, wenn bestimmte Unternehmensregeln bei der Identitätsprüfung nicht erfüllt werden.

Integration und Einsatz

Jedes Unternehmen hat seine eigenen Präferenzen bei der Integration und dem Einsatz einer Lösung. Abhängig von der Komplexität der vorhandenen Prozesse eignen sich manche Ansätze besser als andere.

Zunächst sollten Sie sich die Frage stellen, ob eine Standalone-Komplettlösung für Ihre internen Anforderungen ausreicht oder ob eine tiefgreifendere Integration in Ihre bestehende IT-Umgebung und Ihre Geschäftsprozesse erforderlich ist. Eine Komplettlösung fasst alle Module einer Identitätsprüfungslösung in einem einzigen End-to-End-Prozess zusammen. Zusätzliche periphere Funktionen wie Datenbankprüfungen durch Drittanbieter, Sanktionslisten, PEP (politisch exponierte Personen) und optionale manuelle Prüfungen

sind manchmal mit eingeschlossen. Diese Lösungsarten ermöglichen für gewöhnlich eine einfache Integration, bieten jedoch nicht die Modularität, Flexibilität und Konfigurierbarkeit, die wir in den vorherigen Abschnitten besprochen haben.

Üblicherweise bevorzugen kleinere Unternehmen, darunter auch Start-ups, die keine eigene IT-Abteilung oder nicht genügend Technikressourcen haben und bei denen es keine strengen Anforderungen und Unternehmensregeln gibt, einfache Plug-and-play-Lösungen, die ein einfaches Ergebnis liefern. Wenn diese Unternehmen wachsen, kann aber auch die Anzahl der Anwendungsfälle zunehmen. Dann wird schnell klar, dass eine Komplettlösung die wachsende Komplexität nicht mehr bewältigen kann. Größere Unternehmen bevorzugen meist einen Ansatz mit einem höheren Modularisierungsgrad und einer besseren Konfigurierbarkeit, was es ihnen erlaubt, einzelne Module und Komponenten in unterschiedlichen Infrastrukturbereichen einzusetzen und diese tiefgreifend in den vorhandenen Geschäftsprozessen und IT-Umgebungen zu integrieren.

Eine weitere wichtige Frage in Sachen Plattformpräferenz ist die Differenzierung zwischen nativen mobilen Apps, mobilen browserbasierten Lösungen und Lösungen für PCs. Weiter oben haben wir dazu geraten, aus Sicherheits- und UX-Gründen auf PC- oder laptopbasierte Browser zu verzichten. Nun bleibt noch die Wahl zwischen mobilen Apps und mobilen Web-Anwendungen. Wenn Ihre gesamte User Journey im Browser abläuft, ist es möglicherweise nicht ratsam, eine mobile App einzusetzen, da Ihre Kunden diese herunterladen müssten, um die Verifizierung abzuschließen.

Wenn Sie bereits eine mobile App nutzen, liegt die Wahl einer nativen Integration möglicherweise auf der Hand. Bei dieser Wahl müssen jedoch einige Faktoren berücksichtigt werden, die einige Kompromisse fordern. Besonders zu beachten ist, dass die Verarbeitung von Identitätsprüfungen direkt auf einem Mobilgerät Vor- und Nachteile gegenüber der serverbasierten Verarbeitung mithilfe einer Web-Anwendung aufweist.

Tipps zum Kauf:

- Seien Sie sich Ihrer Anforderungen und der jeweiligen Vor- und Nachteile von mobilen Apps und Web-Anwendungen bewusst.
- Wählen Sie eine Lösung, die eine plattformübergreifende Herangehensweise bietet und alle relevanten Szenarien abdeckt.
- Flexibilität ist ausschlaggebend – wählen Sie eine Lösung, die Ihnen alle Optionen bei der technischen Architektur bietet (Cloud, On-Premise, Hybrid).
- Suchen Sie nach Anbietern, die bereits die notwendigen Integrationen bieten, oder fragen Sie sie, ob sie diese selbst bereitstellen könnten.
- Selbst wenn Sie eine einfache Cloud-Komplettlösung benötigen, empfehlen wir die Zusammenarbeit mit einem Anbieter, der auch komplexe On-Premise-Integrationen durchführt – das ist ein klares Zeichen für Kompetenz.

Mobile Apps

Die Ausführung von Software zur Identitätsprüfung direkt auf einem Mobilgerät bietet den Vorteil, dass Sie die lokale Rechenleistung des Geräts nutzen können.

Bilder lassen sich so schneller verarbeiten, wodurch Sie den Benutzer in Echtzeit anweisen können, um eine bessere Bild- und Extrahierungsqualität zu erzielen. Manche Funktionen wie die biometrische NFC-Chip-Verifizierung lassen sich (zumindest aktuell) nur mit einem Smartphone durchführen. Aber auch das kann sich in der Zukunft ändern.

Ein weiterer Vorteil einer nativen mobilen Implementierung ist die Möglichkeit, Fehler in Echtzeit zu handhaben, was letztlich zu einer besseren Leistung und einem höheren Gesamtautomatisierungsgrad führt. Außerdem kann die Verifizierung vollständig offline auf dem Gerät durchgeführt werden. Möglicherweise ist das jedoch nicht besonders relevant, da die meisten Anwendungsfälle ohnehin eine Internetverbindung erfordern.

Web-Anwendungen:

Web-Anwendungen haben einen großen Vorteil: Anwender können den Identifizierungsprozess durchlaufen, ohne zunächst eine mobile App herunterladen zu müssen.

Bei einer Web-Anwendung wird die Smartphone-Kamera über den Browser gesteuert, um alle erforderlichen Bild- bzw. Videoframes zu erfassen, die dann im Rahmen der Identitätsprüfung auf einem Server verarbeitet werden. Der große Nachteil hierbei ist, dass die Kamera im Browser nicht auf

Plattformen

Native App

+ Benutzerführung in Echtzeit
+ Höchste Bild- und Extraktionsqualität
+ Höhere Geschwindigkeit und bessere Leistung
+ Höhere Sicherheit mit NFC und Hologramm oder Lentikularbild
+ Verifizierung von Dokumenten vollständig offline auf dem Gerät möglich
+ Fehlerbehandlung in Echtzeit

VS

Web-Anwendung

– Keine Benutzerführung in Echtzeit
– Weniger Kontrolle über Kamera- und Bildqualität
+ Kein Download erforderlich
+ Schnellere Integration
+ Einfachere Aktualisierung und Wartung

dieselbe Weise bedient werden kann wie in einer Smartphone-App, da für gewöhnlich weniger Rechenleistung zur Verfügung steht. Dadurch entsteht eine weniger responsive UX und für gewöhnlich ein etwas geringerer Automatisierungsgrad. Auf der anderen Seite lässt sich eine Web-Anwendung deutlich einfacher und schneller integrieren und kann auch leichter aktualisiert und gewartet werden.

Einer der wichtigsten Faktoren ist die technische Architektur der Identitätsprüfungsplattform, wenn es um die Wahl zwischen einer Cloud-basierten Bereitstellung oder einer On-Premise-Implementierung in Ihrer eigenen Infrastruktur geht.

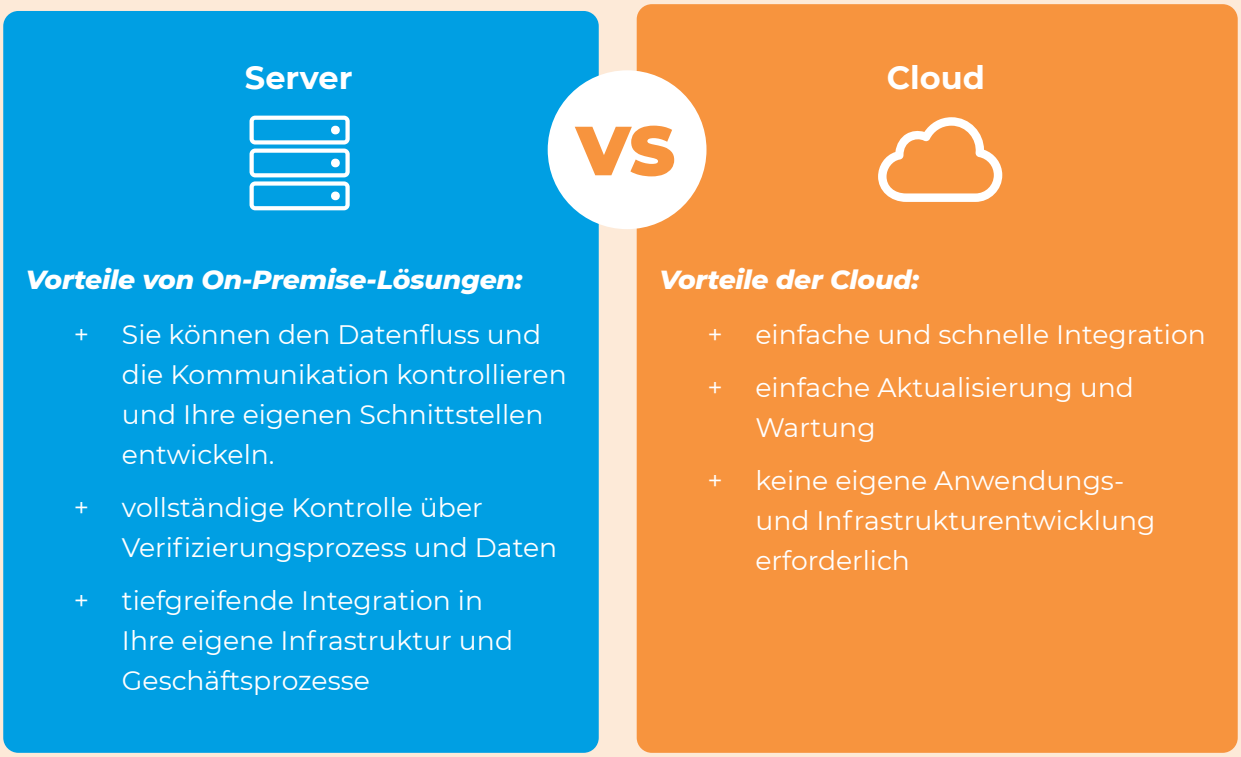
Die meisten Lösungen sind als Cloud-Lösungen verfügbar, auf die über eine Programmierschnittstelle (API) zugegriffen werden kann. Dies ist besonders nützlich, wenn Ihr Produkt oder Service bereits über eine App und/oder Website verfügt, jedoch zusätzlich eine Identitätsprüfungsplattform erforderlich ist. In diesem Fall kann die Plattform einfach mithilfe der API integriert werden. Bei einer Online-Identitätsplattform in der Cloud ist es nicht nötig, Software innerhalb der unternehmenseigenen Infrastruktur zu installieren. Jedoch ist „Cloud“ ein recht allgemeiner Begriff, der präzisiert werden muss.

Stellen Sie sicher, dass Sie verstehen, was für eine Art von Cloud Anbieter verwenden, und ob es sich um eine Public Cloud wie Google, Amazon oder Microsoft oder um eine eigene Private-Cloud-Infrastruktur handelt. Dies hat Auswirkungen auf die Compliance mit Datenschutzverordnungen und auf die Datensicherheit.

Eine wichtige Frage ist auch, wo die Daten Ihrer Kunden gespeichert werden. Bei Ihrer Online-Identitätsprüfungsplattform sollte Datensicherheit großgeschrieben werden. Das gilt auch für den Datenfluss und den Speicherort. Befindet sich die Cloud des Anbieters in einem fremden Land, bedeutet das, dass sensible Daten Ihrer Benutzer das Land verlassen und Sie keine Kontrolle mehr darüber haben, was mit ihnen geschieht. Das ist in den meisten Fällen nicht gesetzeskonform und bringt außerdem ein mögliches Sicherheitsrisiko mit sich.

Tipps zum Kauf:

- Seien Sie sich Ihrer Anforderungen und der jeweiligen Vor- und Nachteile von mobilen Apps und Web-Anwendungen bewusst.
- Wählen Sie eine Lösung, die eine plattformübergreifende Herangehensweise bietet und alle relevanten Szenarien abdeckt.
- Flexibilität ist ausschlaggebend – wählen Sie eine Lösung, die Ihnen alle Optionen bei der technischen Architektur bietet (Cloud, On-Premise, Hybrid).
- Suchen Sie nach Anbietern, die bereits die notwendigen Integrationen bieten, oder fragen Sie sie, ob sie diese selbst bereitstellen könnten.
- Selbst wenn Sie eine einfache Cloud-Komplettlösung benötigen, empfehlen wir die Zusammenarbeit mit einem Anbieter, der auch komplexe On-Premise-Integrationen durchführt – das ist ein klares Zeichen für Kompetenz.



Wenn Sie den Datenschutz schätzen, stellen Sie sicher, dass Sie einen Anbieter mit einer lokalen, idealerweisen privaten und zertifizierten Rechenzentrumsinfrastruktur nutzen.

Die Alternative ist eine On-Premise-Bereitstellung. In diesem Fall werden alle erforderlichen Komponenten für die Identitätsprüfung direkt auf Ihrer Hardware bzw. in Ihrer Infrastruktur oder in Ihrer Private Cloud installiert und ausgeführt. So haben Sie vollständige Kontrolle über den Identitätsprüfungsprozess sowie darüber, wie Benutzerdaten weitergeleitet werden und wie die Lösung mit Ihren übrigen Systemen integriert ist. Zudem tragen Sie die alleinige Verantwortung für die IT- und Datensicherheit. Trotz der vielen Vorteile gibt es nicht viele Anbieter mit vollständigen On-Premise-Lösungen. Grund dafür sind die zusätzliche Integrationskomplexität und der Arbeitsaufwand. Ein Anbieter mit On-Premise-Lösungen wird Ihnen höchstwahrscheinlich auch bei der Umsetzung komplexerer Integrationsprojekte helfen und einen umfassenden Kundensupport bieten. Selbst wenn Sie sich für eine Cloud-Lösung entscheiden, ist es ratsam, mit einem Anbieter zusammenzuarbeiten, der auch über On-Premise-Lösungen verfügt.

Abhängig vom Anwendungsfall finden Sie möglicherweise einen Anbieter, der eine Integration für ein System anbietet, das Sie bereits verwenden, etwa Ihre ERP-, CRM- oder ähnliche Software. Die besten Anwender bieten Integrationen mit SAP-Modulen oder anderen verbreiteten Kernsystemen, damit Sie keine weiteren Integrationen durchführen müssen.

6 Compliance und wieso sie wichtig ist

Compliance war eines der wichtigsten Motive hinter der Online-Identitätsprüfung, da einige ihrer ersten Implementierungen eingesetzt wurden, um Finanzdienstleister (insbesondere Fintech-Unternehmen) bei der Einhaltung von Auflagen zur Geldwäschebekämpfung (AML, Anti-Money-Laundering) und im Bereich Know Your Customer (KYC) zu unterstützen.

Ein wichtiger Faktor beim Wachstum der Online-Identitätsprüfung ist der Wandel im Bankenwesen. Immer mehr Menschen nutzen Mobile- oder Online-Banking und viele junge Menschen setzen beim Eröffnen ihres ersten Bankkontos direkt auf Online-Banken.

Dieser Trend wird vor allem durch die Schließung zahlreicher Bankfilialen auf der ganzen Welt verstärkt, zumindest in den Industrienationen. Immer mehr Regierungen stellen zunehmend hohe Anforderungen an Finanzinstitute, was dazu führt, dass diese Institute wiederum von ihren Unternehmenskunden ein höheres Maß an Verantwortung verlangen.

KYC/AML

Diese beiden Bezeichnungen werden häufig als Synonyme verwendet, da die Gesetzgebung im Bereich KYC (Know Your Customer) den Maßnahmen zur Geldwäschebekämpfung (AML, Anti-Money-Laundering) zuzuordnen ist, die einen wichtigen Aspekt des regulatorischen Rahmens des internationalen Finanzsystems darstellen. Die Einreichung von KYC-Dokumenten und ihre Verarbeitung wird vom AML-Rechtsrahmen bestimmt, an den sich Banken und Finanzinstitute halten müssen. Das übergeordnete Ziel von AML ist es, mit einem hohen Maß an Sicherheit zu verifizieren, dass Kunden auch tatsächlich die Personen sind, für die sie sich ausgeben, und dass sie wahrscheinlich nicht an kriminellen Machenschaften beteiligt sind.

DSGVO

Die Datenschutzgrundverordnung, ein spezieller Rechtsrahmen, trat im Jahr 2018 für alle Bürger und Einwohner der Europäischen Union in Kraft. Diese Verordnung rückte individuelle Datenschutzfragen in den Fokus. Unabhängig davon, wo Ihr Unternehmen seinen Sitz hat, müssen Sie die DSGVO erfüllen, wenn Sie Ihr Produkt oder Ihre Dienstleistung einer Person mit Wohnsitz in der EU anbieten.

PSD2

Die überarbeitete EU-Zahlungsdiensterichtlinie (PSD2) führte die Anforderung einer sicheren Kundenauthentifizierung (SCA) ein und verlangt eine Kombination aus Wissen, Besitz und kundeneigenen Tools, um die Identität eines Verbrauchers zu überprüfen, bevor eine Transaktion abgeschlossen werden kann.

Tipps zum Kauf:

- Suchen Sie nach Anbietern, die sich mit den unterschiedlichen regulatorischen Rahmenwerken auskennen, die für ihre Produkte gelten (z. B. AML – Anti-Money Laundering Act / GWG – Geldwäschegesetz, DSGVO, PSD2 – Zahlungsdiensterichtlinie).
- Arbeiten Sie mit einem Anbieter zusammen, der gerne sein Wissen weitergibt und Sie dabei unterstützt, die relevanten regulatorischen Anforderungen für Ihren Anwendungsfall zu verstehen.

7 Bewährt und zukunftssicher

Eine Reihe unterschiedlicher Faktoren kann Ihnen dabei helfen, zu entscheiden, ob der von Ihnen gewählte Anbieter zu Ihren Geschäftsanforderungen passt.

Kein Faktor in diesem Abschnitt sollte isoliert betrachtet werden; alle müssen vor dem Hintergrund Ihrer Unternehmensanforderungen analysiert werden.

Technologie-Ownership und Kontrolle über das Produkt

Viele Unternehmen im Bereich der Identitätsprüfung bauen ihre Produkte und Dienstleistungen auf outgesourcten Komponenten auf.

Dieser Ansatz ist zwar insgesamt billiger für die Anbieter, da sie Geld bei der Forschung und Entwicklung sparen können, doch kommt es dadurch zu einer Vielzahl von Problemen. Dazu gehören die gesetzlichen Anforderungen an Ihr Produkt oder Ihre Dienstleistung. Die DSGVO verlangt, dass Unternehmen aus der EU Daten aus der EU nur innerhalb der Europäischen Union verarbeiten. Es würde zu Problemen kommen, wenn das Frontend einer Plattform (das die hochgeladenen Scans von Ausweisdokumenten erfasst) sich in einem Land außerhalb der EU befände.

Es gibt natürlich noch weitere Vorteile, wenn ein Unternehmen seine eigene Technologie nutzt und vollständige Kontrolle über das Produkt hat. So trägt es die alleinige Verantwortung, wenn es zu einem schweren Vorfall wie einem Hackerangriff auf das Netzwerk des Anbieters kommt. In diesem Szenario müsste sich ein Anbieter, der eine zusammengestöpselte Lösung anbietet, mit allen anderen Anbietern kurzschließen, deren Komponenten er nutzt. Dies könnte dazu führen, dass andere Beteiligte ihre Verantwortung für den Vorfall von sich weisen.

Einer der Hauptvorteile von Anbietern, die über ihre eigene Technologie verfügen, ist, dass sie für gewöhnlich ihre Produkt-Roadmap mit Ihnen teilen und Sie bei der Festlegung und Priorisierung neuer Funktionen miteinbeziehen, um die Lösung mit der Zeit so zu verbessern, dass Sie am meisten davon profitieren. So werden Ihre projektspezifischen Bedürfnisse und Anforderungen besser erfüllt als durch einen Anbieter, der nicht Eigentümer der eigenen Technologie ist und keine Flexibilität bieten kann.

Zertifizierungen und Normen

Zertifizierungsstellen bieten einen allgemeinen Rahmen zur Qualitätsprüfung von Produkten und Dienstleistungen.

Es gibt eine Reihe von Normen und Zertifizierungen, die ein Produkt zur Online-Identitätsprüfung erfüllen kann.

ISO 27001: Die Zertifizierung nach ISO 27001 ist ein international anerkanntes Best-Practice-Rahmenwerk für ein Information Security Management System (ISMS).

Wenn Sie als Unternehmen Ihre Informationsgüter schützen und regulatorisches Kopfzerbrechen vermeiden möchten (siehe DSGVO), sollte die Zusammenarbeit mit einem nach ISO 27001

zertifizierten Anbieter ganz oben auf Ihrer Prioritätenliste in Sachen Zertifizierung stehen.

Verfügt ein Anbieter über eine ISO-27001-Zertifizierung, können Sie davon ausgehen, dass er gewissenhaft mit der Speicherung und dem Zugriff auf Ihre Daten umgeht.

ETSI-Normen: Eine wichtige Organisation, die Sie im Rahmen Ihrer Kaufentscheidung kennen sollten, ist das Europäische Institut für Telekommunikationsnormen (ETSI). Das ETSI ist verantwortlich für die Erstellung allgemeingültiger Normen zu Internet-, Mobilfunk-, Funk- und Rundfunktechnologien in der gesamten EU. Wenn Sie sich vergewissern, dass Ihr Anbieter sich mit ETSI-Normen auskennt und auf dem neuesten Stand ist, erhöhen Sie die Wahrscheinlichkeit, dass Ihre Identitätsprüfungslösung die gesetzlichen und regulatorischen Verordnungen in Europa erfüllt.

ISO/IEC 30107: Der Zweck dieser Zertifizierung ist die Schaffung einer Grundlage und eines Prozesses zur Erkennung von Presentation Attacks (Presentation Attack Detection, PAD).

Die ISO/IEC-30107-Zertifizierung schafft ein Framework, durch das Presentation-Attack-Ereignisse spezifiziert und erkannt werden können, damit sie sich kategorisieren, detaillieren und kommunizieren lassen, um anschließend Entscheidungen zu treffen und die Performance zu bewerten.

eIDAS: Eine weitere Norm ist die eIDAS-Verordnung der EU (auch IVT), die den europaweiten Einsatz von elektronischer Identifizierung und Vertrauensdiensten für elektronische Transaktionen regeln soll.

Viele Anbieter behaupten, die Verordnung zu erfüllen und entsprechend zertifiziert zu sein. Doch ein genauerer Blick lohnt sich. Wir haben Fälle gesehen, bei denen nur ein kleiner Teil der beworbenen Lösung zertifiziert war. Manche Lösungen waren nur teilweise gesetzeskonform. Einige Lösungen verfügen möglicherweise nicht über die Zertifizierung für Ihren konkreten Anwendungsfall. In manchen Fällen gilt die Zertifizierung nur für einen Teil der beworbenen Lösung.

Unternehmensstandort

Der Unternehmenssitz und der Standort der Niederlassungen sind ebenfalls ein wichtiger, aber häufig unbeachteter Faktor.

Bietet das Land besondere Vorteile, die es zu einem wünschenswerten Unternehmenssitz machen? Denken Sie daran, wie politische und finanzielle Stabilität in verschiedener Hinsicht eine Auswirkung auf die Speicherung von Kundendaten hat. Beachten Sie auch die Auswirkungen, die nationale Gesetze und Verordnungen auf Zugriff, Speicherung und Verarbeitung von Daten haben. Ein Anbieter in Ihrer Nähe ermöglicht auch eine schnellere Reaktionszeit im Support. Zudem kann der Anbieter Sie bei Bedarf leicht vor Ort aufsuchen und Hürden durch unterschiedliche Zeitzonen fallen weg.

Erfolgsbilanz und Unternehmensruf

Der Ruf ist wichtig.

Wie viel Erfahrung hat das Unternehmen? Hat es sein Produkt oder seine Dienstleistung zuverlässig über einen längeren Zeitpunkt hinweg bereitgestellt? Sind Kundenrezensionen zum Unternehmen oder zu seinen Produkten positiv oder negativ? Je mehr Fragen Sie stellen können, desto besser.

Ein Unternehmen, das sich mit so sensiblen Informationen wie Online-Identitäten befasst, trägt die Verantwortung, die Dinge richtig zu machen. Perfektion ist kein Ziel, denn Fehler sind menschlich. Doch die Art und Weise, wie ein Unternehmen mit Problemen umgeht, sagt viel über seine Integrität aus.

Kundenreferenzen und Vertrauen

Einer der wichtigsten Faktoren sind Kundenreferenzen.

Mit wem hat der Anbieter gearbeitet? In welchen Branchen? Zu welchen Anwendungsfällen? Und mit welchen Unternehmensgrößen? Ein Anbieter, der bislang nur 100 kleine Kunden betreut hat, bietet vermutlich nicht die richtige Lösung für eine sehr große Organisation. Ein Anbieter, der sich hingegen nur auf große Konzerne spezialisiert hat, ist möglicherweise nicht der richtige Partner für ein Start-up.

Nutzt eine Regierungsbehörde den Anbieter? Das Vertrauen der Regierung entspricht dem Vertrauen der Öffentlichkeit (das gilt natürlich nicht für jedes Land) und ist ein guter Gradmesser für die allgemeine Qualität, die das Unternehmen bietet. Versteht es das Unternehmen, das Vertrauen der Öffentlichkeit zu gewinnen? In welcher Hinsicht könnte das für sein Geschäft wichtig sein? Welche Faktoren spielen eine Rolle bei geringem öffentlichen Vertrauen in das Unternehmen? Geringes öffentliches Vertrauen in ein Unternehmen beruht üblicherweise nicht auf einem einzigen Faktor, sondern hat verschiedene Ursachen.

Auszeichnungen

Wurde das Unternehmen von einer externen Stelle akkreditiert und für einen Preis vorgeschlagen oder hat es diesen gar gewonnen?

Das ist ein gutes Zeichen, denn es ist im Interesse eines jeden Unternehmens, bemerkt zu werden und sich selbst auf nationaler oder gar internationaler Ebene einen hohen Bekanntheitsgrad zu verschaffen. Doch genau wie Risikokapital und Seed-Finanzierung sind Preise nur allgemeine Gradmesser, die Ihnen keine tieferen Einblicke verschaffen. Sie erfahren beispielsweise nicht, wie effektiv eine Plattform Kunden konvertiert.

Ein potenzieller Nachteil von Auszeichnungen ist, dass manche Unternehmen damit womöglich übertreiben, um einen anderen Mangel zu kompensieren.

Akademische Partnerschaften

Unternehmen, die mit wissenschaftlichen Einrichtungen zusammenarbeiten, zeigen, dass sie Brücken zwischen dem Hochschulwesen und der Unternehmenswelt bauen können.

Ein Engagement in der Wissenschaft stellt sicher, dass das Unternehmen mit den neuesten Forschungsergebnissen vertraut ist. Unternehmen, die in der Nähe von Hochschulen angesiedelt sind, profitieren davon, sich persönlich mit führenden Forschern austauschen zu können.

Anstatt nur die frühe Forschungsphase zu überwachen und Geld in Chancen zu stecken, die sich gerade ergeben, wird ein intelligentes Unternehmen kontinuierlich Investitionen in seinen Interessensbereichen tätigen. Sowohl die

Industrie als auch die Forschung (und letztlich auch die Gesellschaft) profitieren von solch langfristigen Engagements. Finden Sie heraus, ob und wie einer der Identitätsprüfungsanbieter, die Sie im Auge haben, mit wissenschaftlichen Institutionen zusammenarbeitet.

Tipps zum Kauf:

- Wählen Sie einen Anbieter, der bereits mit ähnlichen Unternehmen zusammengearbeitet hat.
- Fragen Sie die Anbieter nach Kundenreferenzen. Die bestehenden Kunden können Ihnen genau sagen, was wie gut funktioniert hat.
- Anbieter, die mit nationalen digitalen ID-Systemen oder Regierungsbehörden zusammengearbeitet haben, sind für gewöhnlich eine gute Anlaufstelle.
- Seien Sie vorsichtig bei Unternehmen, die sich vor allem über ihre Preise definieren. Das kann ein Hinweis auf mangelnden Fokus in anderen wichtigen Geschäftsbereichen sein.
- Wir empfehlen die Wahl eines Anbieters, der seine eigene Technologie entwickelt hat und idealerweise die volle Kontrolle über sein Produkt beibehält.
- Arbeiten Sie mit einem Anbieter zusammen, der Verordnungen und Zertifizierungen versteht und der sich nicht scheut, Ihnen diese zu erklären.
- Aspekte wie Vertrauenswürdigkeit, geopolitische Stabilität und die Fähigkeit, talentierte Mitarbeiter anzuziehen, sollten nicht unterschätzt werden.

8 Unterstützung

Pre-Sales-Support

Wenn Sie sich nach einer Identitätsprüfungslösung umschauen, suchen Sie nach einer, die den besten Support für die Gestaltung Ihrer Geschäftsprozesse und der Unternehmensregeln bietet.

Was sind die Anforderungen Ihres Unternehmens? Wie passt das Produkt in Ihre jetzige Unternehmensstruktur? Wie sollen Architektur und Design aussehen? Wie soll der Prozess mit Ihrem bestehenden und zukünftigen Kundenstamm synchronisiert werden?

Genauso wie bei einem größeren Kauf im Elektrofachhandel würden Sie sich normalerweise an einen Ansprechpartner im Verkauf wenden, wenn Sie weitere Informationen zu einem Produkt benötigen. Dasselbe Muster gilt beim Kauf einer Identitätsprüfungsplattform für Ihr Unternehmen. Auch wenn es wohl wahr ist, dass der Kauf einer Softwarelösung für Ihr Unternehmen deutlich komplizierter ist als der Kauf eines Flachbildfernsehers, sollte es gerade in diesem Fall eine hoch qualifizierte und engagierte Vertriebsunterstützung geben, die Sie beim Einkaufsprozess begleitet.

Unterstützung nach dem Verkauf

Die Unterstützung nach dem Verkauf für das von Ihnen gewählte Online-Identitätsprüfungsprodukt ist ebenfalls ein wichtiger Faktor.

Da Online-Identitätsplattformen meist als Abonnement vertrieben werden, sollten diese selbstverständlich einen Post-Sales-Support anbieten, der Sie unterstützt und Ihnen hilft, die Leistung Ihres Unternehmens während des gesamten Lebenszyklus der Lösung zu verbessern.

Integration und technischer Support

Entwickler-Support und technischer Support sind wichtig, um die Identitätsprüfungsplattform professionell in Ihre aktuelle Unternehmensarchitektur zu integrieren.

Suchen Sie eine Lösung, die durchgehend technischen Support sowie ein dediziertes Projektmanagement bietet. Dies ist der Schlüssel zu einer erfolgreichen Produktimplementierung.

Change-Management und Geschäftskontinuität

Geschäftsanforderungen ändern sich mit der Zeit. Darum sollten Sie sich nach einem Produkt umsehen, das über ein Change-Management-Protokoll verfügt.

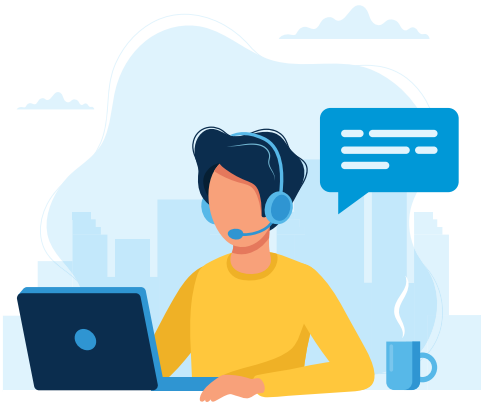
Dieses Protokoll erlaubt es Ihnen, das Produkt zu einem späteren Zeitpunkt zu konfigurieren oder zu modifizieren, damit es den sich verändernden Anforderungen Ihres Unternehmens gewachsen ist. So stellen Sie außerdem sicher, dass Sie nur für die Module zahlen, die Sie benötigen. Geschäftskontinuitäts- und Katastrophenmanagement-Support bieten zusätzlich Sicherheit, die Handlungsfähigkeit Ihres Unternehmens im Katastrophenfall zu gewährleisten.

In mancher Hinsicht lässt sich die Identitätsprüfung mit Suchmaschinenmarketing (SEM) vergleichen. Im SEM legen Sie Ihre Keyword-Strategie fest, beginnen mit einigen kleinen Kampagnen, ziehen Ihre Lehren daraus und verbessern Ihre Kampagnen kontinuierlich, um das optimale Ergebnis zu erzielen. Bei der Identitätsprüfung passen Sie die Lösung zunächst an (z. B. für hohe Sicherheit) und analysieren die Ergebnisse. Im nächsten Schritt beginnen Sie damit, Unternehmensregeln und Schwellenwerte anzuwenden und anzupassen, um die optimale Konversionsrate Ihres Geschäfts zu erreichen. Es ist wichtig, dass Ihr Anbieter versteht, dass es bei der Identitätsprüfung nicht nur um Input und Output geht, und er Sie bei der langfristigen Optimierung Ihrer Prozesse unterstützt.

Service Level Agreements (SLAs)

Dabei handelt es sich um die Verpflichtungen, die der Anbieter Ihnen gegenüber eingeht.

Im Allgemeinen gilt, dass die SLAs umso stärker sein müssen, je kritischer ein Service für den Betrieb eines Unternehmens ist. Nur so können die Bedürfnisse des Kunden erfüllt werden. SLAs können Verpflichtungen bezüglich der Betriebszeit, Reaktionszeiten, angestrebte Reparaturdauern und manchmal Strafen im Fall der Nichterfüllung enthalten. Wählen Sie einen Anbieter, der über ein stringentes SLA verfügt oder zumindest die Wahl zwischen unterschiedlich starken SLAs ermöglicht. Dies ist oft ein Hinweis darauf, wie wichtig es dem Anbieter ist, seinen Kunden einen reibungslosen Service bereitzustellen.



Tipps zum Kauf:

- Wählen Sie einen Anbieter, der über ein engagiertes und fachkundiges Supportteam verfügt, das Sie bei der optimalen Nutzung der von Ihnen erworbenen Produktlösung unterstützt.
- Die besten Anbieter verfügen standardmäßig über Pre-Support- und Post-Support-Dienstleistungen.
- Technischer Support sollte bei der Integration einer Identitätsprüfungslösung keine untergeordnete Rolle spielen. Die verständliche technische Dokumentation ist wichtig für erfolgreiche Ergebnisse.
- Achten Sie darauf, einen Anbieter zu wählen, der konsequente Change-Management-Protokolle in seiner Lösung anbietet. Diese Protokolle sind besonders wichtig, da sich die Anforderungen Ihres Unternehmens im Laufe der Zeit verändern können.

9 Kosten

Wie bei den meisten anderen Produkten und Dienstleistungen gilt auch hier, dass die billigste Lösung nicht in jedem Fall auch die beste, flexibelste oder sicherste ist.

Auch bei der Identitätsprüfung erhält man das, wofür man zahlt. Da der Konkurrenzkampf in der Identitätsprüfung in den letzten Jahren immer mehr zugenommen hat, ist auch der Preisdruck in der Branche gestiegen.

Die besten Identitätsprüfungsplattformen basieren auf hochkomplexen Technologien wie fortschrittlichen Machine-Learning- und Computer-Vision-Algorithmen. Deren Nutzung erfordert jahrzehntelange Erfahrung sowie viele Jahre der Entwicklung und der kontinuierlichen Verbesserung. All das kostet Geld.

Wem gehört die Technologie?

Die meisten Anbieter auf dem Markt für Identitätsprüfung besitzen keine proprietäre Technologie.

Stattdessen beziehen viele Anbieter Lizenzen für verschiedene Komponenten von mehreren Tech-Providern und führen sie anschließend zu einem Produkt oder einer Plattform zusammen. Es spricht nichts dagegen, ein solches Produkt zu verwenden, wenn es Ihre Anforderungen erfüllt.

Wenn Sie eine einfache All-in-One-Lösung benötigen, kann dies durchaus funktionieren. Wenn Sie jedoch ein dynamischeres, komplexeres Setup benötigen, stehen die Chancen gut, dass Sie das erforderliche Fachwissen und den Support des Anbieters benötigen Wir haben von unglaublich niedrigen Preisen gehört, meist von neuen Anbietern, die sich mit diesen Preisen unter Marktniveau einen Zugang zum Sektor verschaffen wollen. Diese Unternehmen verschwinden häufig nach einigen Jahren plötzlich vom Markt.

Das Hauptproblem dabei ist, dass viele Anbieter die Komplexität der Identitätsprüfung und die Bedeutung von Flexibilität und Support auf Kundenseite unterschätzen. Wir empfehlen daher die Zusammenarbeit mit Anbietern, die eigene Technologien entwickeln und besitzen. Diese Anbieter haben vielleicht nicht die glänzendste Website und das beste Marketingmaterial, aber wenn Sie sich die Zeit nehmen, genauer nachzuforschen, werden Sie viel mehr Substanz aus deren Antworten herausholen. Solche Anbieter haben meist ein viel umfassenderes Fachwissen und können Sie bei der Definierung Ihrer Anforderungen und bei der Implementierung und Bereitstellung des Produkts deutlich besser unterstützen. Darüber hinaus bedeutet eine proprietäre Technologie Flexibilität auf der Produktseite und im kommerziellen Bereich; wenn Sie keine Lizenzen an Lieferanten zahlen müssen, haben Sie völlige Freiheit bei der Preisgestaltung.

Transaktionsbasierte Preise

Die Identitätsprüfungsbranche verwendet vor allem ein transaktionsbasiertes Preismodell, wobei ein gewisser Betrag für jede Identitätsprüfung gezahlt wird.

Herkömmliche Komplettlösungen werden vor allem im Abonnementmodell angeboten. Dabei umfassen die monatlichen oder jährlichen Beträge eine bestimmte Menge an Transaktionen.

Für gewöhnlich gilt: Je größer die Menge der Transaktionen, desto geringer ist der Einzelpreis pro Transaktion. Jedoch sollten bei komplexeren Implementierungen auch die Kosten höher sein. Anbieter berechnen möglicherweise eine einmalige Einrichtungsgebühr für die Bereitstellung und Implementierung einer Lösung und jährliche Wartungsgebühren für fortlaufenden Support. Manchmal wird dieser Mehraufwand in einem Abo-Modell berücksichtigt, um die Preisgestaltung zu vereinfachen. Bringen Sie in jedem Fall in Erfahrung, was Sie für den angegebenen Preis tatsächlich erhalten.

Preisflexibilität

Zwar können alle Anbieter direkt ihre Standardpreise nennen, doch die besten Anbieter sind beim Geschäftsmodell flexibel.

Ein Anbieter sollte ein Geschäftspartner sein, der Ihr Unternehmen begleitet und es Ihnen ermöglicht, noch mehr Erfolg zu haben. Durch Entgegenkommen bei den Preisen zeigt ein Anbieter, dass Sie wichtig für ihn sind – unabhängig von Ihrer Größe als Kunde.

Die besten Anbieter bieten Ihnen kostengünstige Anlaufzeiten oder Pauschalgebühren mit unbegrenzter Nutzung oder ermöglichen es Ihnen sogar, Ihre Nutzerbasis mit kostenlosen Verifizierungen zu vergrößern – und verdienen dann an den Einnahmen, die Sie mit Ihrem Unternehmen erzielen. Dies sind nur einige Beispiele für alternative Geschäftsmodelle. Zögern Sie nicht, Ihren Anbieter um Unterstützung zu bitten. Das bedeutet nicht zwingend niedrigere Preise. Es handelt sich einfach um andere Preismodelle mit verschiedenen Anreizen und Verpflichtungen.

Tipps zum Kauf:

- Wählen Sie einen Anbieter mit herstellereigenen Technologien.
- Lassen Sie Ihre Entscheidung nicht allein vom Preis bestimmen.
- Entscheiden Sie sich für einen Anbieter, der Ihnen ein flexibles Preismodell bietet und Ihnen hilft, Ihr Geschäft auszubauen, anstatt Sie mit hohen versunkenen Kosten zu belasten.

10 Die nächsten Schritte

Wir können Ihnen dabei helfen, Ihre wichtigste Anforderung zu definieren und die ideale Lösung für Ihr Unternehmen zu finden.

Nachdem Kunden diesen Leitfaden gelesen haben, erhalten wir für gewöhnlich diese beiden einfachen Fragen:

Wie geht es weiter?
Wie schnell kann das Projekt umgesetzt werden?

Wir bei PXL Vision glauben an Transparenz und verpflichten uns zu Offenheit und Ehrlichkeit im gesamten Prozess. Darum helfen wir Ihnen sehr gerne dabei, die wichtigen Informationen in diesem Dokument besser zu verstehen. Wir freuen uns darauf, mit Ihnen zu sprechen, um mehr über die Probleme zu erfahren, die Sie in Ihrem Unternehmen lösen möchten.

Wie bereits gesagt gibt es keine Standardlösung zur Identitätsprüfung oder ein einziges Produkt, das zu jeder Unternehmensgröße und jedem Unternehmenstyp passt.

Unser Expertenteam verfügt über das Fachwissen, mit dem Ihr Unternehmen eine Identitätsprüfungslösung finden und implementieren kann, die sich am besten für Ihre Anforderungen eignet.

Wir stehen Ihnen für Ihre Fragen gerne zur Verfügung.

Wir hoffen, dass dieser Einkaufsleitfaden hilfreich für Ihr Unternehmen war und Ihnen ein tieferes Verständnis für die vielen verschiedenen Auswahlmöglichkeiten in der Online-Identitätsüberprüfung vermittelt hat. Jede Entscheidung hat einen Einfluss auf das Onboarding-Erlebnis Ihrer Kunden.

Kontaktieren Sie uns, um ein Gespräch oder eine kostenlose Vorführung der preisgekrönten Technologie und Produkte von PXL Vision zu vereinbaren.

Sprechen Sie mit unseren Produktexperten.
pxl-vision.com/kontakt/

Über PXL Vision

PXL Vision ist der Schweizer Marktführer für hochgradig sichere und vollständig automatisierte KI-basierte Identitätsverifikationslösungen. Die flexible Technologie von PXL Vision unterstützt alle Kundenanforderungen und Geschäftsprozesse auf der ganzen Welt.

Unternehmen aus so unterschiedlichen Branchen wie Finanzdienstleistungen, Telekommunikation, Mobilität, Sharing Economy und Einzelhandel sowie der öffentliche Sektor nutzen bereits die Technologie von PXL Vision, um die Identität ihrer Kunden zu überprüfen.

PXL
VISION