White Paper

Digital Identity Proofing

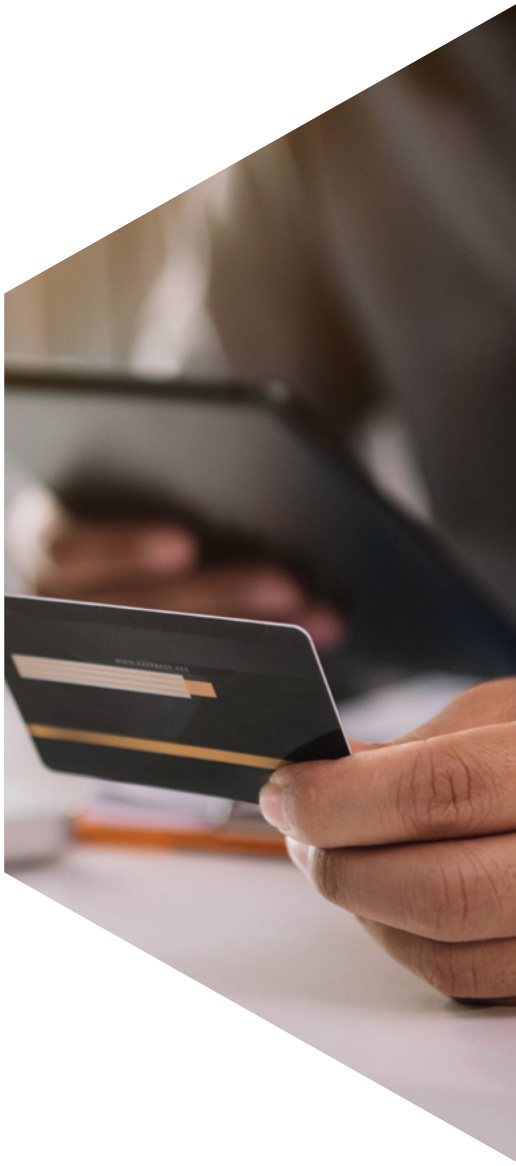
How to verify identities remotely and securely

Game-changing customer experience meets high-assurance security

ENTRUST

SECURING A WORLD IN MOTION

Trusted Identity in the Spotlight



The coronavirus global pandemic is expanding the already burgeoning population of remote workers and consumers. Almost every enterprise is facing a surge in the volume of identities they need to verify online, as millions more people work, shop, and conduct transactions from home. An effective identity proofing solution brings a combination of strong security and engaging user experiences to almost every remote use case. Now is a good time for enterprises, consumer marketers, financial institutions, and government agencies to explore modern identity proofing.

The volume of identities you need to manage and verify will increase as we move through this health crisis — and the population of remote users will continue to expand after the pandemic subsides, as people become more comfortable with ubiquitous connectivity.

Identity Proofing: Balancing Security and User Experience

If you ask the question, "What is identity proofing?" you'll get a range of answers. In broad terms, the methodology has existed in some form for decades. Most of us remember providing our mother's maiden name or similar bits of personal trivia to "prove" our identities. This practice is often referred to as static PII (personally identifiable information), and it's far from secure, given the proliferation of hacking, malware, and social engineering.

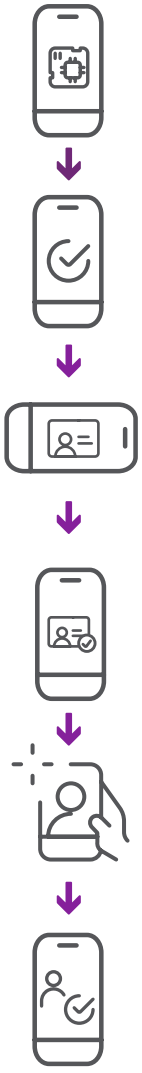
The problem with these approaches is that they present a terrible combination of poor user experience (aka friction) and flimsy security. Consumers often get frustrated during onboarding and abandon important processes like opening new accounts or signing up for new products and services. When technology providers offer solutions to remove some of that friction, they sometimes inadvertently provide enticing new opportunities for hackers.

These early methodologies have evolved somewhat, but many of the ID proofing solutions on the market today are only slightly refined versions of those high-friction/low-security methodologies. So, a better question to ask is, "How does identity proofing with low friction and strong security work?"

Onboarding in 60 Seconds or Less

Banks, government agencies, corporations, and other organizations that need to onboard a large number of users quickly and securely require a modern identity proofing solution. And these organizations should ensure that the ID proofing solution they select can be easily integrated with their own apps, websites, or other digital properties for a seamless user experience.

Here's how it works:



1. **App download.** Consumers, employees, citizens, or other users typically download your app, which has identity proofing embedded into it, onto a mobile device equipped with a high-resolution camera.

2. **Device reputation check.** In-app artificial intelligence (AI) tools verify that the device being used is not stolen and doesn't have a reputation for being involved in fraudulent transactions. This prevents the compromise of valid credentials.

3. **Photo of an official ID.** Users are prompted to snap a photo of their official government-issued identity document such as a passport, license, or national ID card. Much of the user's personal information, like name and address, are pre-populated to the customer application form.

4. **Document verification.** The app then assesses the document's authenticity in near real time with global coverage of 6,000+ official government identity document types. Depending on document specifics, 50 or more forensic tests are conducted to determine document authenticity.

5. **Snap a selfie.** AI tools ensure that it's a "live" image and not a photo of a photo. An important privacy note: The best solutions do not store user photos or any other PII.

6. **Identity verification.** This is the critical final step. Effective solutions leverage AI to match the image on the identity document with the selfie to verify user identity.

Even for the most methodical user, this process should take less than a minute. The right combination of biometrics, AI tools, and real-time access to a global library of government document types makes the process far more secure than traditional approaches — even though users are less taxed.

Perfect Places for Identity Proofing

Your users expect you to protect their identity, and they're holding you responsible. Whether users are accessing banking services, government programs, company VPNs, or e-commerce sites, they increasingly believe you are responsible for protecting their identity and liable for any implications of a breach. From that perspective, creating layers of the highest assurance security measures would make sense. Unfortunately, consumers will abandon account opening processes and employees will work around security measures if the identity proofing process is too onerous. The key is finding a modern solution that provides both high-assurance security and low friction for users.

Here are some examples of use cases and key considerations for each:

Account opening: Consumers increasingly are willing to work with banks and other service providers that don't have physical locations nearby. This makes it easy for them to compare a wider range of offerings. This is an opportunity for banks and other consumer marketers that can make the account opening experience quick, easy, and secure. It's also a competitive threat for companies that fail to make that transition.

Customer onboarding: Banks, retailers, and other consumer marketers have robust digital business portfolios. Connectivity with customers is only going to increase — and so is the field of competitive offerings. Streamlining the onboarding process is key to successful cross-selling and up-selling strategies.

Employee onboarding: The right identity proofing solution will rapidly pay for itself by automating the onboarding of new employees or registration of existing employees for access to apps, networks, and websites. Studies show the process is 8x more efficient with the right identity proofing system.

Other common use cases:

Student registration
Loyalty program registration
Online/mobile application forms
Visitor management
Mobile driver's license programs
e-Passport programs
Age verification
Card or card-not-present transactions
Security checks and watchlists
Physical and logical access control
CRM management
Sharing-economy app management

Incredibly Strong and Nearly Invisible Security

Do consumers want frictionless onboarding experiences or strong security for personal data and transactions? There may have been a time when they had to choose. But now they want it all — and someone in your market is going to give it to them.

There's ample evidence to support that theory, as multiple studies show that up to 70% of consumers will abandon a mobile or online registration process if it presents too much friction. If they don't like the experience, they'll move on to another brand, but they're more and more likely to be savvy about a provider's security posture.

70% of consumers will abandon a mobile or online registration process if it presents too much friction.

Why Identity Proofing Feels Invisible:

DEVICE REPUTATION	DOCUMENT VERIFICATION	FACIAL MATCH
In background	**5.5 seconds**	**1 second**
Tech lovers may find this interesting — factors here include account creation velocity, access velocity, TOR browser history, credit/debit fraud checks, and rooted or jailbroken device detection. From the user perspective, this takes no time.	AI is driving modern identity proofing systems with tight integration to databases of government document types. Key elements of identity documents are scanned, document type is confirmed, and validation results are delivered in seconds.	That same AI and validation engine that authenticates documents compares selfies to images on the IDs and ensures the subject is "live" and not a photo of a photo — in one second or less.

Automating Compliance on Multiple Fronts

The regulation landscape for any organization that uses identity proofing is constantly changing. As hackers evolve, so must the regulators who are intent on protecting consumers, as well as the interests of financial institutions, corporations, healthcare providers, government agencies, and other organizations.

When it comes to protecting consumers and their privacy, the European Union's General Data Protection Regulation (GDPR) set a benchmark in many respects. One of the most identity-specific parts of the regulation reads: "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures." While the regulation pertains to European consumers, other regulatory agencies are using it as a benchmark.

As most security executives know, the financial penalties of violating GDPR are potentially massive. So, when considering identity proofing technology, it's important to choose a solution that simplifies compliance with GDPR specifically — and is likely to accommodate new regulations that emulate the EU statute.

GDPR COMPLIANCE TIPS:

Data retention practices: GDPR clearly states you can only collect the personal data you need for a specific business purpose; then only store a bare minimum of that data for the long term. Look for a solution that does not retain selfie images, PII, or other identity data.

Compliant algorithms: The platform you choose cannot be built to aggregate data from multiple customers and prospects to create machine learning algorithms used for decisioning. In the case of financial service applications, machine learning tools must focus only on individuals and not build aggregate models.

KYC and AML for Financial Institutions

Know Your Customer (KYC) regulations require banks and other institutions to verify the identity of customers before they are given access to financial products and services. The regulation also covers identity verification practices used to determine and monitor associated risks, often in regard to illegal activities such as money laundering.

Complying with KYC is a high-assurance requirement. Relying on older methodologies and PII will not suffice. Look for a solution that leverages biometrics, live facial recognition, and AI-based device reputation analysis. These modern, high-assurance security technologies are indicators of a KYC-compliant platform.

Anti-Money Laundering (AML) regulations are designed to enable institutions to prevent, detect, and report money laundering activities. The regulation is intended partly to prevent institutions from making money through illegal activities, but mostly to protect institutions from being used unknowingly for money laundering.

Because AML and KYC are closely linked, you'll want to look for many of the same attributes when choosing an identity proofing technology. As with KYC, this includes biometrics, live facial recognition, and device reputation analysis. These attributes will help you limit application and onboarding friction for legitimate customers, while providing a strong line of defense against fraudulent behaviors.

Integrating Transaction Security and Continuous Monitoring

Leveraging identity proofing technology to create engaging user experiences and deploy high-assurance security measures is a great way to modernize your digital business efforts. But like your digital business, the best identity proofing platforms are going to continue to evolve. They're going to become smarter and more intuitive, and they are going to expand to include new capabilities.

As a result, it's important to choose an identity proofing solution that works seamlessly within a larger authentication platform. This approach gives you the power and flexibility to expand, add use cases, and implement additional security measures as your world changes. The combination of identity proofing and a broader authentication platform also provides optimal protection for your customers and your enterprise throughout the customer journey. Here are some things to look for if you're interested in finding an identity platform that will expand and scale up to include these new capabilities:

IDENTITY PROOFING	TRANSACTION SECURITY	CONTINUOUS MONITORING
Modern UX and strong security in the application and onboarding process.	Safeguard against man-in-the-middle attacks and other threats.	Ensure authenticated identities aren't compromised.

Choosing the Right Technology for Your Enterprise

We all know that mobility and connectivity have changed both the definition and value of identity. Without trusted identity, nothing in the modern context works. Customers accessing offerings on smartphones, employees working anywhere, and other critical ecosystems rely on trusted identities to function. A key challenge in these ecosystems is that consumer expectations for convenience and the sophistication of cyberattacks are both racing ahead at the same incredible pace. Previous definitions of identity and the methodologies we used to authenticate identities no longer work because of all this change.

So, as your enterprise sets out to evaluate and select an identity proofing solution, it will be important to keep some of these best practices in mind:

Build a truly cross-functional search team	This decision is equally influenced by the need for exceptional customer engagement and strong enterprise security. Include members that represent both interests.
Start by recalibrating your definition of identity	The old definition and old methodologies no longer apply. Explore how concepts like decentralized and distributed are reshaping "identity."
Conduct grassroots research into customer preferences	Your customers — or employees, citizens, or other users — have preferences being shaped by their experiences with other brands. What they want changes rapidly; keep an up-to-date understanding.
Identify the most pressing cybersecurity threats	Just like consumer preferences, hacker methodologies evolve and become more sophisticated every day. Work with your security teams to understand current and emerging threats.
Explore the elements of modern identity and authentication	Biometrics, encryption, device reputation, AI, and machine learning are the new components of trusted identity. Reach out to trusted partners to develop a deeper understanding of these technologies.
Determine the impact of key regulatory requirements	Regulatory bodies are trying to keep up with privacy issues, cyber threats, and other key issues. Regulations change fast and present entirely new challenges.

RESOURCES FOR YOUR SEARCH

If you're looking for information and insights to help with your evaluation of identity-proofing technology — or if you'd like to see a demonstration of our platform — you can visit entrust.com/proof.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com