



The complete guide to digital identity



Contents

01 The crisis of traditional identity verification

02 What is digital identity?

03 The enrollment journey

04 When identity becomes an asset

05 Digital identity changes the math

06 One identity layer, every use case

The complete guide to digital identity

Every time a person verifies their identity online, they start from scratch. New form. New selfie. New photo of the same driver's license that has been photographed a dozen times before. Identity verification today is a sequence of disconnected moments, each one treating the user as a stranger regardless of how many times they've proven themselves before.

That friction has real costs: businesses absorbing the expense of repeated checks, customers abandoning processes that feel like obstruction, and a verification model that creates new attack surfaces every time it runs. And as AI-generated synthetic identities, deepfakes, and document forgeries grow more sophisticated, the old logic of "seeing is believing" has stopped being reliable.

Digital identity changes the model. A [persistent, cryptographically secured credential](#) that a person establishes once and carries forward across every subsequent interaction. A foundation built for the world as it actually is.

This guide covers what digital identity is, how it works, why it is categorically different from traditional identity verification, and what it makes possible for the organizations building on it.

The crisis of traditional identity verification

The core problem with traditional IDV is structural: it treats every verification as a first-time event.

A user opens a bank account and gets verified.

They apply for a loan at the same institution and get verified again.

They sign a closing document and go through the process once more.

Each checkpoint is self-contained, isolated from every prior interaction, with no memory and no compounding value. The investment in verifying that person the first time earns nothing on the second or third transaction.

The operational cost of this model is significant. [Fenergo's 2025 survey of financial institutions](#) found that organizations now spend an average of \$72.9 million annually on AML and KYC operations, with no natural ceiling as transaction volume grows.

The same study found that 70% of institutions lost clients in the past year due to slow or overly complex onboarding, up from 48% just two years prior.

Consumers asked to prove themselves repeatedly lose confidence in the organizations demanding it, and many abandon the process before it's complete.

Fraud exposure compounds alongside the cost. Every new verification event creates a fresh opportunity for synthetic identity fraud, document forgery, or biometric spoofing, so the model does not get safer with repetition. It just adds to the attack surface.

The "do nothing" response is common, with organizations absorbing per-transaction costs, accepting the drop-off, and treating verification as the price of doing business. The problem is that costs scale linearly with volume while security does not scale at all.

What is digital identity?

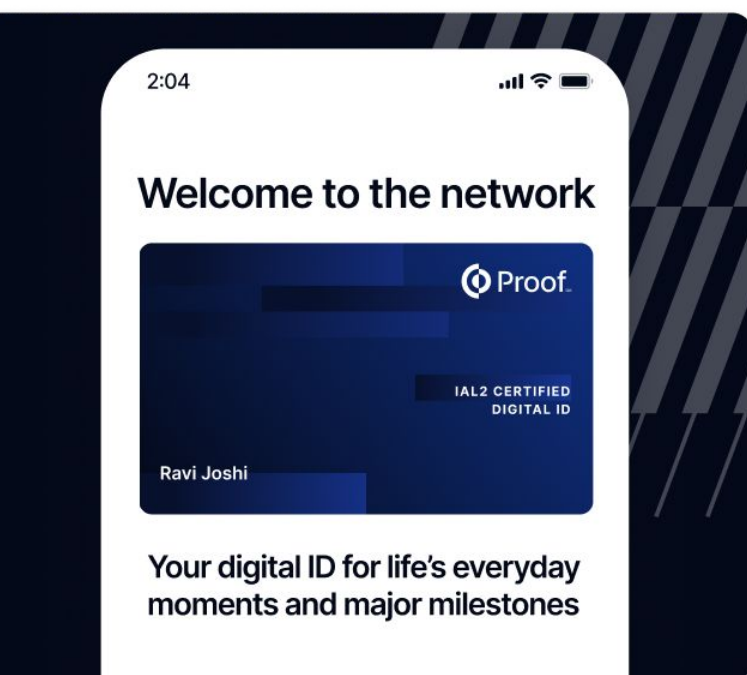
Unlike a database record, which stores information about someone, a digital identity is mathematically bound to the verification event that created it, and that distinction has become increasingly consequential.

A stored record is a snapshot: your name, your date of birth, your ID number. Those are strings of characters that can be copied from one system and presented in another. Data breaches happen precisely because stored information is separable from the person it describes, and whoever holds the

data can impersonate the person.

A digital identity credential works differently. It is cryptographically tied to a live biometric, so re-authentication requires the same person confirmed in real time, not just a matching set of records.

The credential cannot be separated from the person it represents, which means it cannot be stolen and replayed the way data records can. This architecture is increasingly essential as the threat landscape shifts.



A digital identity is a persistent, cryptographically secured credential that represents a verified person.

Generative AI has made it easy to produce convincing synthetic identities, forged documents, and deepfaked selfies, and the fraud numbers reflect it.

Cryptographic proof creates a verification that cannot be faked, because it requires a live biometric matched to a mathematically bound credential issued at a specific, auditable moment in time.

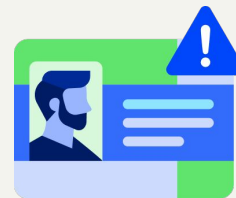
The strength of that cryptographic binding depends on who issues the credential. The most secure digital identities are issued by a certificate authority, an organization with the infrastructure to issue PKI (public key infrastructure) certificates directly to verified individuals.

The critical question is whether the same organization that verifies the identity also issues the certificate. Many digital identity platforms verify the person and then hand off to a third-party certificate infrastructure to

The scary stats



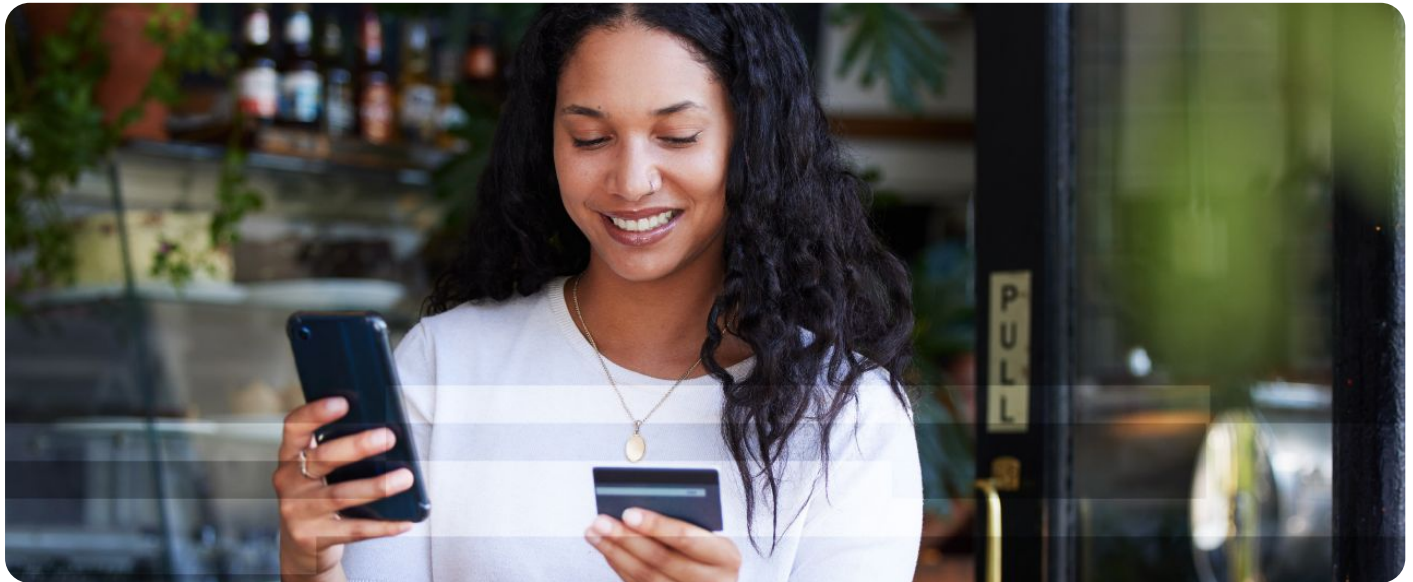
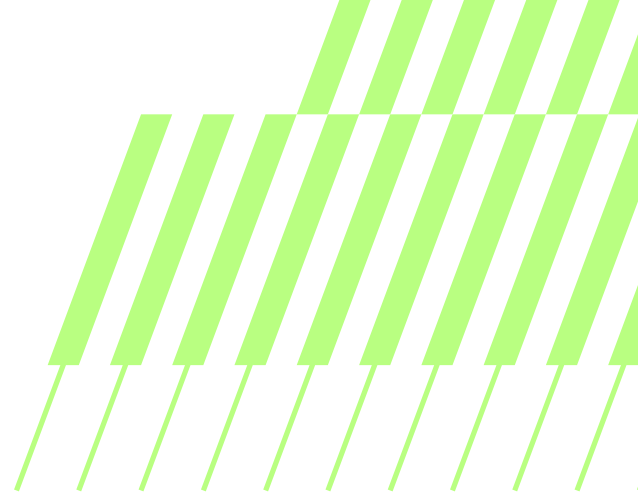
Deepfake related fraud losses reached [\\$1.1B in 2025](#), tripling from \$360M just a year earlier.



Gartner predicts that by 2026, [30% of enterprises](#) will no longer consider standalone IDV solutions reliable in isolation.



A basic [deepfake fraud incident](#) now costs businesses an average of \$500k, not counting reputational damage..



generate the credential, creating a gap in the chain of trust from the moment of enrollment.

Proof operates as a certificate authority, so the organization verifying a user's identity is the same one issuing their PKI certificate. The chain of trust is unbroken from enrollment through every subsequent use.

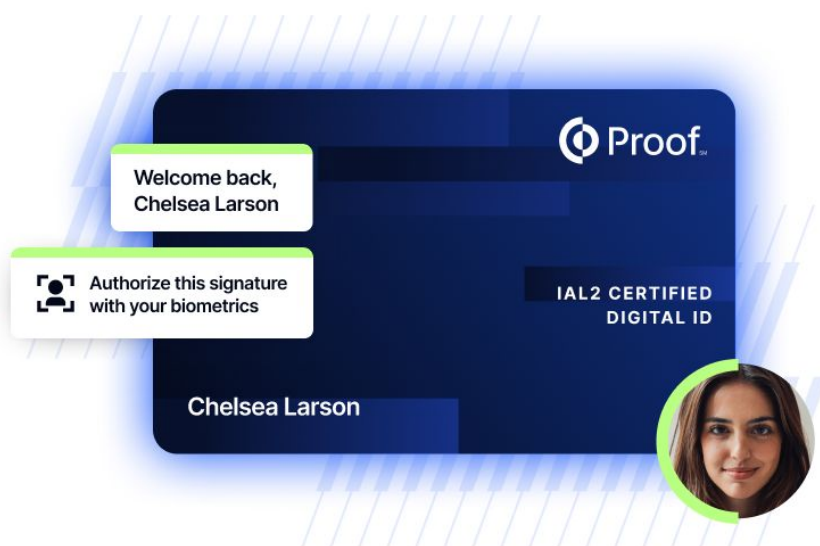
At Proof, we see digital identity as a persistent asset: something a user establishes once, at a high level of assurance, and carries forward across subsequent interactions. A single verified credential that travels with the user across products, organizations, and use cases, because it is issued to the person, not stored in any one company's database.

The enrollment journey

Establishing a digital identity happens through a structured, standards-compliant process designed to meet IAL2 (Identity Assurance Level 2) requirements. The process is built to be thorough without being burdensome, completing in minutes for most users.

Enrollment is a one-time investment, and everything that follows draws from it.

From this point forward, re-verification across any Proof-enabled service requires only a biometric check against the saved credential, with no new documents and no repeated data entry.



Step 1: Start

The user initiates verification within a Proof-enabled workflow, triggered from any product or service in the Proof network.

Step 2: ID Capture

The user captures a government issued identity document. The system extracts and validates the document data, checking for authenticity signals that distinguish genuine documents from forgeries.

Step 3: Selfie

A live selfie compares against the identity document photograph using biometric matching. This step is a liveness check that defeats static image attacks.

Step 4: Human-in-the-loop

Human-in-the-loop review is available for edge cases where signals are inconclusive, providing a fallback that protects against threats automated systems miss.

Step 5: Save ID

The verified credential is issued and stored, transforming a transaction record into a persistent asset that belongs to the user.

When identity becomes an asset

Most identity verification systems answer one question: is this person who they say they are? Proof's digital identity answers a second question that the first one makes possible: what can this person now do?

A Proof identity is an active credential, not a passive record, and it unlocks real-world capabilities across the full range of interactions where verified identity matters.



Document signing

Every signature is cryptographically tied to the verified identity, creating a legally binding, tamper-evident record where the identity is embedded in the action rather than attached after the fact.



Notarization

Proof enables fully remote online notarization, with the verified identity serving as the foundation for notarial acts that carry legal weight across jurisdictions without requiring an in-person appearance.



Physical access

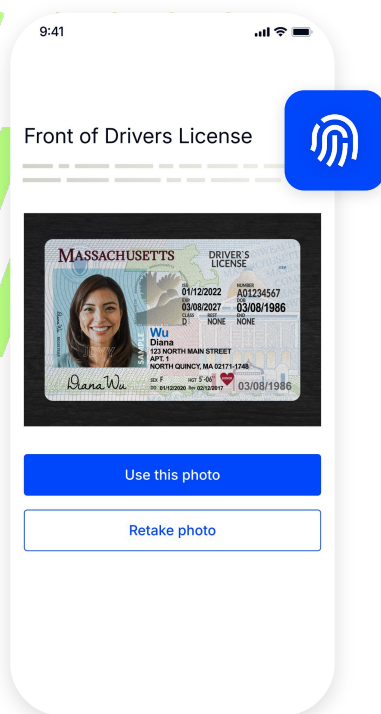
A verified Proof identity can extend beyond digital transactions to physical access controls, enabling organizations to unify digital and in-person identity assurance under a single credential.

The value of the credential compounds with every use, as each transaction adds to an auditable record of verified activity tied to the same verified person, building a history that strengthens trust over time. This is what distinguishes digital identity from a more sophisticated login.

Why reusable digital identity changes the math

Traditional IDV operates on a per-transaction model where each verification is complete and self-contained: documents submitted, data checked, decision made, and then the process resets. Three problems compound with this structure:

- Cost scales linearly with volume, since every new transaction carries a new verification expense regardless of prior history.
- Fraud risk increases with each new submission, as each event creates a fresh opportunity for document forgery or identity spoofing.
- The data collected is siloed, living in one organization's systems and invisible to any other context where the same person needs to be verified.

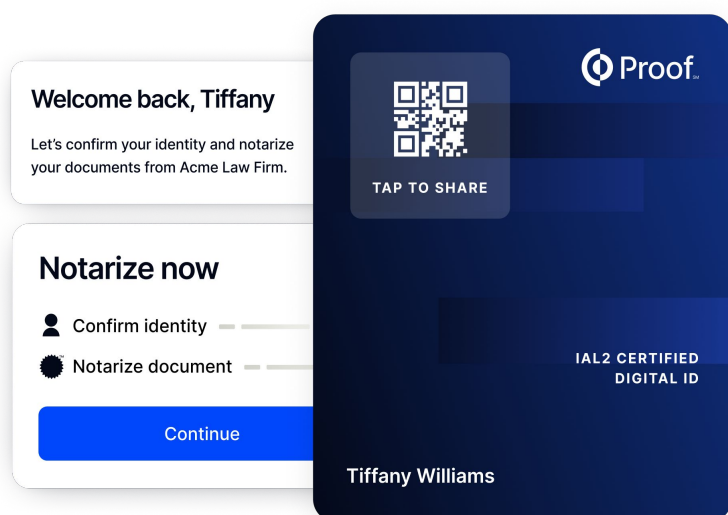


The comparison between traditional IDV and reusable digital identity is a difference in kind, not degree.

The fraud exposure embedded in this model is significant and growing. The [FTC reported that consumers lost \\$12.5 billion to fraud in 2024](#), a 25% jump from the prior year, with identity fraud as a primary driver. Additionally, McKinsey identifies synthetic identity fraud as [the fastest-growing financial crime in the United States](#), accounting for 10 to 15% of charge-offs in a typical unsecured lending portfolio.

The reason these schemes are so effective against traditional IDV is that each new check evaluates submitted documents in isolation, with no memory of what has been seen before.

Reusable digital identity operates on a fundamentally different architecture, and the contrast with "just saving information" is worth making explicit because the two are often conflated.



When an organization stores a user's name, ID number, and date of birth in a database, that is a data record: static, copyable, and vulnerable to the same breaches that affect any stored data.

If that database is compromised, so is every identity in it. The saved information model also has a hard boundary, living within one organization's infrastructure and unable to travel with the user anywhere else.

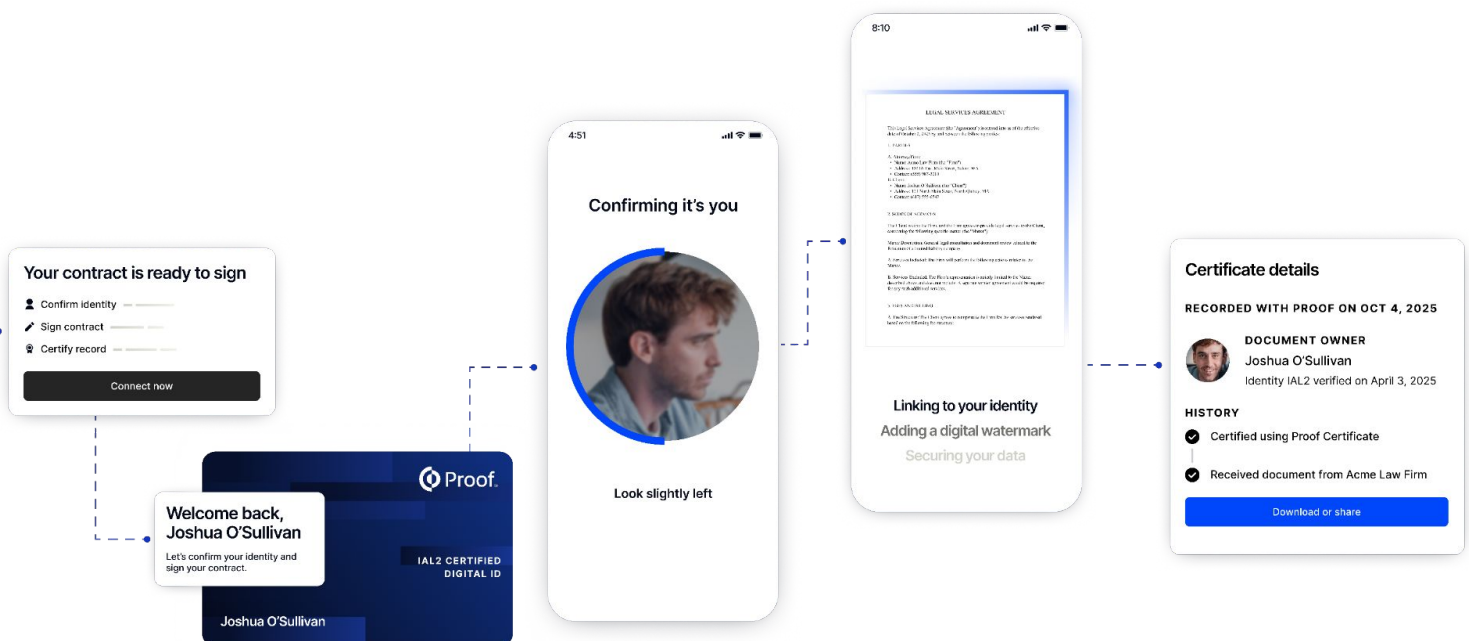
A Proof digital identity credential is architecturally different. It is cryptographically bound to the biometric of the verified person at the moment of enrollment, so re-authentication requires the live person confirmed through biometric check against a credential that was mathematically sealed at the time of issue. The credential is inseparable from the person it represents, which means it cannot be harvested from a breach and replayed elsewhere.

That binding is also what makes it genuinely portable. When a user enrolls in Proof's network, that verified identity is recognized across every Proof-enabled service, regardless of which organization or product the user is accessing:

- A user verified during account opening at one financial institution can use that same credential to complete a high-value transaction at another.
- A user verified for one product in a company's portfolio carries that verification into every other product in the same portfolio.
- A credential established during a real estate transaction can be reused for a subsequent notarization, a document signing, or an identity check at an entirely different organization.

This is identity issued to the person, not siloed in the company.

The practical outcomes follow from the architecture. Re-verification takes seconds rather than minutes, since a biometric check against an existing credential replaces document upload and identity matching from scratch. Fraud vectors collapse because a network of verified identities [sharing fraud signals across the platform](#) means an identity flagged in one context protects every other context in the network.



Integration and scalability

One identity layer, every use case

The economics of digital identity improve at scale, but only when identity infrastructure is treated as a shared layer rather than a per-product implementation.

Proof's architecture is built around a single identity layer that works across business units and markets, where the same credential that verifies a user for one product is recognized across all products built on the same infrastructure. Fraud signals discovered in one corner of the network inform decisions across the whole network, and compliance controls applied at the infrastructure level apply everywhere at once.

The difference is material



A financial services company with consumer banking, business accounts, and lending products no longer pays to re-verify the same customer across each one.



A real estate platform spanning listing, transaction, and closing workflows shares a single verified identity throughout.



A legal services provider covering document preparation, signing, and notarization operates from one identity foundation rather than three disconnected ones.

Verify once. Use everywhere.

Digital identity creates a unified audit trail, where every identity-linked action, document signing, account access, and transaction authorization, is recorded against the same verified identity. Compliance reporting that previously required stitching records across disparate systems becomes a function of querying a single log.

With digital identity deployed at this layer, a compliance checkbox becomes infrastructure: the kind that every other business capability builds on, that gets cheaper and more secure as it scales, and that compounds in value with every use.

[Learn more](#)



About Us

Proof is the trusted platform for the most important agreements that businesses and consumers sign. More than 7,000 businesses trust Proof to complete all types of transactions from online notarizations to identity-assured eSignatures. The platform combines strong identity verification with built-in fraud prevention to ensure that transactions are harder to forge. Proof also operates the Notarize Network, the largest on-demand network of trusted notaries that are available 24/7 to perform notarizations, witness transactions, or check identities. Learn more at proof.com.