What Is Identity Proofing? How You Prove a Person Is Who They Claim to Be at Registration

Definitions / Last updated 2026-06-11 / https://www.scrambleid.com/learn/what-is-identity-proofing

In one sentence: Identity proofing is the process of establishing that a person is who they claim to be at registration, distinct from authentication (which verifies that a returning user is the same person who was proofed), and it is the foundation on which every downstream authentication ceremony rests.

TL;DR (canonical)

- **Definition:** Establishing that a person is who they claim to be at the moment they register for a service.
- **Distinct from authentication.** Proofing is the registration-time question ("who is this?"); authentication is the access-time question ("is this the same person?").
- **NIST IAL framework.** NIST SP 800-63A-4 defines IAL1 (lightweight proofing with lower-friction evidence requirements), IAL2 (verified evidence), and IAL3 (in-person or supervised with strict evidence); self-asserted identity counts as no proofing at all under Revision 4. Finalized July 2025 as part of the SP 800-63 Revision 4 family.
- **Proofing methods include:** document verification (government ID with security feature checks), biometric matching (live selfie compared to ID photo with liveness detection), authoritative-source validation (address, SSN, business records), in-person verification, and supervised remote verification.
- **Knowledge-based verification (KBV) is no longer sufficient on its own.** Public-records and breached-data leaks have made KBV a weak proofing signal.
- **The proofing-to-binding handoff is critical.** Bind a phishing-resistant credential at the moment of proofing, while the proofed identity is still verified.
- **Where proofing matters most:** financial-services KYC, healthcare patient registration, government benefits, federal employment, regulated CIAM, high-value enterprise customer onboarding.

Identity proofing vs identity authentication

These are different operations and they answer different questions.

Property	Identity proofing	Identity authentication
When	Once, at registration	Every time the user accesses
Question answered	Is this person who they claim to be?	Is this the same person who was proofed?
NIST framework	IAL (Identity Assurance Level)	AAL (Authenticator Assurance Level)
Evidence	Government ID, biometric, authoritative-source validation	Cryptographic credential ceremony
Defined in	NIST SP 800-63A	NIST SP 800-63B
Failure mode	Synthetic identity, document fraud	Credential theft, phishing

Both are required for a strong identity system. A system with strong authentication but weak proofing produces an authenticated nobody (a fabricated identity that can be re-authenticated cleanly forever). A system with strong proofing but weak authentication wastes the proofing investment because the authenticated user is not necessarily the proofed person.

NIST IAL levels

NIST SP 800-63A-4 (Revision 4) restructured the assurance ladder. Self-asserted identity is no longer an IAL: it's simply "no identity proofing." IAL1 is now a real proofing level with lower-friction evidence requirements, sitting below IAL2.

No identity proofing: self-asserted

The user provides their identity information and the relying party records what was provided. No verification is performed beyond rudimentary checks (e.g., the email address resolves). Under Revision 4 this isn't an IAL at all.

Appropriate for: Low-stakes scenarios where the relying party does not need to know who the user actually is. Newsletter subscriptions, anonymous-equivalent commenting, free trial signups.

Not appropriate for: Anything involving payments, PII, regulated services, or privileged access.

IAL1: Lightweight proofing

The entry proofing level under Revision 4. The user presents identity evidence and the relying party validates and verifies it, with lower-friction evidence requirements and more flexible processes than IAL2. It exists for services that need some confidence in a real-world identity without the cost and friction of full IAL2 verification.

IAL2: Verified evidence

The user provides identity evidence that is verified to be genuine and matched to the user. NIST SP 800-63A specifies what counts.

Typical evidence requirements:

- Two pieces of identity evidence with at least one "strong" (government-issued ID with photo and machine-readable features), or
- One piece of "superior" evidence.

Verification activities:

- Confirming evidence is genuine: security features, machine-readable zone (MRZ) consistency, document templates, hologram verification.
- Validating data against authoritative sources where available: SSN to SSA, address to USPS, business name to state registry.
- Binding evidence to the presenter: biometric matching of a live selfie to the ID photo, with liveness detection to defeat presentation attacks.

Modes:

- **Remote IAL2:** Verification performed online, often via a vendor (Persona, Stripe Identity, Onfido, Jumio, ID.me, others) using document upload, selfie, and liveness.
- **In-person IAL2:** Verification performed in person by trained staff (notary, bank branch, federal facility).

Appropriate for: Banking KYC, healthcare patient registration, mid-stakes employment, most regulated CIAM, federal benefits.

IAL3: In-person or supervised remote verification with strict evidence

The strongest tier. Requirements are stricter than IAL2 across evidence collection, verification, and binding.

Typical requirements:

- Multiple pieces of strong evidence.
- In-person verification with trained staff, OR supervised remote verification (live video with the verifier).
- Strong biometric binding to the credential.
- Stronger audit and recordkeeping.

Appropriate for: Federal high-assurance contexts (PIV issuance), the highest-value financial transactions, regulated environments where in-person verification is the norm.

For deeper coverage of how IAL relates to AAL and FAL, see What Are NIST AAL Levels?.

Proofing methods (technical detail)

Document verification

The user uploads or scans a government ID. The verification system:

1. Identifies the document type and country.
2. Extracts data from the visual zone (name, DOB, expiration) and machine-readable zone (MRZ) for documents that have one.
3. Verifies the document's security features: holograms, microprint, UV-reactive elements, kinegrams, ICAO MRZ checksums.
4. Compares the document image against templates of known good documents to detect tampering or counterfeits.
5. Checks expiration and (where available) revocation against authoritative sources.

Modern document verification typically achieves high accuracy on known document types, with vendor-specific accuracy varying by document quality and lighting.

Biometric matching with liveness

The user records a live selfie or video. The verification system:

1. Detects a face in the live capture and in the ID photo.
2. Computes a similarity score between the two faces.
3. Performs liveness detection to ensure the live capture is from a real present person, not a photo, video replay, or deepfake.

Liveness is the defending property against presentation attacks (PAD, Presentation Attack Detection). The most common attacks are printed photos, screen-replayed videos, and 3D masks. Modern liveness systems use combinations of:

- Active liveness (challenge-response: blink, turn head, follow a dot).
- Passive liveness (analyzing texture, depth, and motion in the capture without explicit challenges).
- Hardware-backed liveness (TrueDepth on iPhone, structured-light or ToF cameras).

NIST FRTE and FATE (Face Recognition Technology Evaluation, formerly FRVT) publish vendor accuracy and PAD performance.

Authoritative-source validation

The verification system queries authoritative sources to validate the user-provided data. Examples:

- SSN against SSA (with consent and where authorized).
- Address against USPS, AAMVA, or commercial address-verification services.
- Business name and EIN against state registries and IRS.

- Bank account ownership via micro-deposit or instant verification.

These checks add evidence that the identity exists and matches authoritative records, reducing synthetic-identity risk.

Knowledge-based verification (KBV)

KBV asks the user questions derived from public records or credit-bureau data: prior addresses, prior employers, mortgage details, vehicle ownership.

KBV is no longer sufficient on its own for IAL2. The questions and answers are widely available to attackers via breached data. NIST SP 800-63A discourages KBV as the sole proofing mechanism. KBV can serve as a supplementary signal but is not the path to IAL2 alone.

In-person verification

A trained verifier (bank staff, federal employee, notary, dedicated proofing kiosk operator) examines the user's identity evidence and the user themselves in person. This remains the strongest path for IAL3 and is part of the federal PIV issuance process.

Supervised remote verification

A live verifier observes the user via video call, requests document presentation, performs biometric matching, and asks challenge questions. This is recognized in SP 800-63A-4 as a path to IAL2 (and potentially IAL3 with stricter controls).

The proofing-to-binding handoff

The most consequential design decision in any identity system: at the moment of proofing, what credential is bound to the proofed identity?

Weak handoff: The user is proofed, and the system later sends them a username/password by email. The proofing investment is partially wasted because the future authentication is bound to the email account, not to the proofed person.

Strong handoff: At the moment of proofing, the user binds a phishing-resistant cryptographic credential (FIDO2/WebAuthn passkey, derived PIV, hardware key) to the proofed identity. Future authentication exercises the same binding.

The strong handoff preserves the proofing investment across every future authentication event. It also dramatically reduces fraud, because synthetic-identity-driven account takeover requires either fraudulent proofing or stealing the bound credential, not just guessing a password.

For the recovery side of this (when the bound credential is lost), see Recovery and Fallback Playbook.

Common identity proofing failure modes

1. **Proofing only at signup, with weak password issued afterward.** Throws away the proofing investment.
2. **KBV as primary proofing.** Defeated by breached data.
3. **Document verification without biometric binding.** A stolen ID without biometric matching does not prove the holder.
4. **Liveness detection that doesn't catch deepfakes.** Vendors vary; deepfake attacks are now a real production threat.
5. **No re-proofing on high-risk events.** Account takeover, large transactions, or device add events should trigger re-proofing.
6. **Binding the proofed identity to a phone number.** SIM swap defeats the binding.
7. **Treating IAL and AAL as the same thing.** A user can be proofed strongly and still authenticate weakly; both must be addressed.
8. **Building proofing in-house at scale.** Document fraud detection, deepfake-resistant liveness, and authoritative-source integrations are vendor-specialty problems for most enterprises.

Where identity proofing is required

Domain	Requirement
Banking / financial services	KYC and CIP under USA PATRIOT Act, BSA; risk-based proofing under FFIEC
Healthcare	Patient registration; provider credentialing; controlled-substance prescribers
Government / federal	PIV issuance, citizen-facing benefits, federal contracting
Telecom	Subscriber identity verification under regulatory requirements
Crypto / digital assets	Travel rule, KYC under FinCEN guidance
Gambling / gaming	State licensing requirements
High-value e-commerce	Fraud prevention; some platform contractual requirements
Regulated employment (DoT, healthcare, financial)	Background-check-bound proofing
Voter registration	State-level requirements vary widely

Where proofing is not legally required, it may still be a fraud-economic question: at what spend level does proofing reduce loss enough to pay for itself?

Key Takeaway

Identity proofing is the process of establishing that a person is who they claim to be at registration, distinct from authentication (which verifies that a returning user is the same person who was proofed). NIST SP 800-63A defines three Identity Assurance Levels (IAL): IAL1 (lightweight proofing with lower-friction evidence requirements), IAL2 (verified evidence with biometric binding), IAL3 (in-person or supervised remote with strict evidence); under Revision 4, self-asserted identity is treated as no proofing rather than an IAL. Common methods are document verification with security-feature checks, biometric matching of live selfie to ID photo with liveness detection, and authoritative-source validation. Knowledge-based verification (KBV) is no longer sufficient on its own. The most consequential design decision is the proofing-to-binding handoff: bind a phishing-resistant cryptographic credential at the moment of proofing so future authentication exercises the same binding rather than wasting the proofing investment on a username/password.

FAQ

What is identity proofing?

Identity proofing is the process of establishing that a person is who they claim to be at the moment they register for a service. It typically involves collecting identity evidence (government ID, biographic data), verifying the evidence is genuine and unmodified, validating that the data matches authoritative sources, and confirming that the person presenting the evidence is the legitimate holder. NIST SP 800-63A defines the Identity Assurance Level (IAL) framework with three levels.

How is identity proofing different from authentication?

Identity proofing happens once at registration and answers "is this person who they claim to be?" Authentication happens at every access and answers "is this returning user the same person we proofed?" Proofing establishes the binding between a real person and an account; authentication exercises that binding. The two are independent: an account can be proofed at IAL2 and authenticated at AAL1, or the reverse. Both are needed for a strong identity system.

What are NIST IAL levels?

Under Revision 4, self-asserted identity is treated as no proofing rather than an assurance level. IAL1: lightweight proofing with lower-friction evidence requirements. IAL2: remote or in-person verification of strong identity evidence (government ID, biometric matching to ID photo, address verification). IAL3: in-person or supervised remote verification with strict evidence requirements and strong binding ceremonies. IAL is defined in NIST SP 800-63A and updated in SP 800-63-4.

What identity evidence qualifies for IAL2?

IAL2 typically requires either two pieces of identity evidence with at least one being strong (government-issued ID with photo and machine-readable features), or one piece of superior evidence. Verification includes confirming the evidence is genuine (security features, machine-readable zone consistency), validating the data against authoritative sources where possible, and binding the evidence to the person presenting it (typically biometric matching: a live selfie compared to the ID photo with liveness detection).

Is knowledge-based verification (KBV) sufficient for identity proofing?

No, not on its own. NIST SP 800-63A discourages KBV as the sole proofing mechanism because the knowledge-based questions (SSN, prior addresses, mortgage details) are typically derived from public records or breached data. KBV remains useful as a supplementary signal but cannot satisfy IAL2 alone. Document verification with biometric binding is the dominant IAL2 path.

What's the proofing-to-binding handoff?

Once a person is proofed, the relying party must bind the identity to a credential the person will use for future authentication. The strongest pattern is to bind a phishing-resistant cryptographic credential at the moment of proofing, while the proofed person is still verified. If proofing is performed and the user later receives a username/password by email, the proofing investment is partially wasted because the future authentication is not bound to the proofed identity. The proofing-to-binding handoff is one of the most consequential design decisions in any identity system.

References (public)

- NIST SP 800-63A (Identity Proofing and Enrollment): https://csrc.nist.gov/pubs/sp/800/63a/4/final
- NIST SP 800-63-4: https://csrc.nist.gov/pubs/sp/800/63/4/final
- NIST FRTE and FATE (formerly FRVT): https://www.nist.gov/programs-projects/face-technology-evaluations-frvt-fate
- Login.gov Identity Verification Overview: https://www.login.gov/help/verify-your-identity/overview/
- FinCEN Customer Identification Program (CIP): https://www.fincen.gov/resources/statutes-regulations/guidance/customer-identification-program-cip-rule

---

Related reading

- What Are NIST AAL Levels?
- What Is Phishing-Resistant MFA?

- What Are Passkeys?
- Recovery and Fallback Playbook
- Compliance Mapping: NIST and CISA