What Is People Verification? Cryptographic Person-to-Person Identity, Explained

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

> **Status (June 2026):** Early access. The People verification family is live with early-access customers and isn't generally available yet. This article describes the shipped design as it stands today; talk to your ScrambleID account team about access and timelines.

In one sentence: People verification is a class of authentication where two humans cryptographically verify each other's identity directly, without an intermediary call center or helpdesk, using hardware-bound private keys on each party's device, with a default 60-second single-use artifact (QR code, Type Code, or SMS deep link) carrying the verification context.

TL;DR (canonical)

- **Definition:** Direct human-to-human identity verification using cryptographic round-trip authentication, with no third-party call center, helpdesk, or notary in the middle.
- **Why it exists:** AI-generated voice and video have made every traditional human-to-human verification signal probabilistic and increasingly defeatable. People verification shifts the question from "does this person sound or look like the legitimate user?" to "does this person possess the private key bound to that identity?"
- **The artifact options:** A QR code (QID) for in-person scanning, a Type Code for use over a voice call, or an SMS deep link for distant verification. All three share a single-use Dynamic Identifier with a default 60-second TTL.
- **The consent and attribute model:** The presenter selects a profile (Work, Personal, or Custom) and sees a live preview of exactly which attributes will be shared. The verifier sees provenance marks (verified source vs self-asserted) on each attribute.
- **The differentiator:** AI quality does not affect the result. No AI, regardless of how convincing the voice or face, can produce a cryptographic signature without holding the matching hardware-bound private key.
- **Fast and deterministic:** verification completes in a few seconds, versus the 30 to 90 seconds typical of knowledge-based questions. Replay attempts that yield a success target zero.

Why people verification matters now

For most of the history of business, humans verified each other by recognition, deference, and shared context. You knew the executive's voice. You recognized the vendor's face. You knew the building's security guard. When you didn't, you called someone who did, or you checked a badge, or you signed a paper.

Generative AI broke every signal in that chain.

Voice cloning from 30 seconds of audio is now commodity capability available in consumer products. Deepfake video on consumer hardware is real-time. Behavioral patterns can be learned and replayed by an LLM. The Arup Hong Kong incident in early 2024 made the new pattern public: a finance employee transferred $25.6 million after a video conference in which every other participant was an AI-generated deepfake. The voice was right. The face was right. The behavior was right. None of the participants existed.

The traditional defenses (call them back to verify, check the badge, "I recognize them") all assume signals an attacker cannot easily replicate. Those assumptions no longer hold.

people verification is built on a different assumption. It does not ask whether the person on the other side looks or sounds right. It asks whether they hold the cryptographic private key bound to the identity they claim. That is a binary question with a deterministic answer. Either the signature verifies or it does not. AI cannot produce a signature without the key.

The basic shape of a people verification

Two humans, each with the ScrambleID mobile app installed and identity-bound to the app:

1. **Presenter** opens the app and chooses what to share. They pick a profile (Work, Personal, or Custom) or toggle individual attributes. The ID card preview at the top of the screen updates live to mirror exactly what the verifier will see.
2. **Step-up if required.** If their profile or organizational policy requires it, the app invokes the platform authenticator (Face ID, Touch ID, Windows Hello, or device PIN) before issuing any artifacts.
3. **Artifact issued.** The app issues a Dynamic Identifier (DID) for the session and renders three options to the presenter: a QR code (a QID), a short Type Code, and an SMS deep link button.
4. **Verifier consumes.** The verifier opens their ScrambleID app and chooses how to consume the artifact. Scan the QR. Type the code. Tap the SMS link.
5. **Both see the same result.** On success, both parties see the presenter's ID card with a "Verified" success label. Either can review the event in Verification History. The verifier can save the presenter as a contact.

The whole flow is read-only by default and explicitly initiated on both sides. There is no push-to-approve. There is no flow where pressing accept on a notification grants verification. Both parties

must take action.

The three artifact channels and when to use each

Artifact	When to use	Default TTL	Notes
QR code (QID)	In person, screen-to-screen	60 seconds	Most common pattern. Carries the DID, organizational context, signature, and certificate thumbprint.
Type Code	Over a voice call or when scanning is impractical	60 seconds	Short alphanumeric code. Spoken aloud by presenter, typed by verifier. Single-use.
SMS deep link	Distant verification when both parties are not co-located	60 seconds	Single-use link that opens the verifier's app. Organizational policy can disable this channel entirely.

All three artifacts carry the same Dynamic Identifier with the same single-use semantics, the same 60-second default TTL, and the same cryptographic guarantees. The choice of channel is operational, not a security trade-off.

What makes the cryptography deterministic

The signature on the QID payload is produced with a ScrambleID private key for the environment, and the QR carries the certificate thumbprint that identifies the corresponding public certificate. Any verifying device can confirm the QID came from the expected environment.

On each user's device, a separate hardware-bound private key (Apple Secure Enclave, Android StrongBox, Windows TPM, or equivalent) is the cryptographic root. That key is generated on the device, never leaves it, and cannot be extracted by any software, including jailbreak tooling. Cryptographic operations require device user verification (Face ID, Touch ID, PIN) per WebAuthn semantics.

The Dynamic Identifier is server-issued, single-use, and short-TTL. The ScrambleID service invalidates the DID on first use and purges it on expiry. A captured DID cannot be replayed. A relay attacker who somehow intercepts the DID cannot redirect the result, because the WebSocket channel is bound to the issued DID and messages are only delivered on the bound connection.

Origin binding is enforced via the certificate thumbprint embedded in the QID. Any signature must validate to the current environment. Wrong-origin attempts are rejected. The audit trail records every event including method (QR/Code/SMS), outcome, TTL expiries, the device IDs (ZIDs) involved, and the attribute set shared.

Attributes and provenance: what gets shared

The presenter does not share a fixed identity. They share a contextually-scoped subset of verified or self-asserted attributes. The catalog (version 2025-07) includes:

Attribute	Default profile	Source	Provenance mark
Avatar / photo	All	Liveness check on device	Verified
Handle (@user#)	All	System checksum	Verified
Human-Verified ring + freshness	All	Device key + biometric/PIN	Verified
Legal name	Work, Personal	HR/KYC or government-ID scan	Verified or self-asserted
Company / employer	Work	HR	Verified or self-asserted
Job title	Work	HR	Verified or self-asserted
Department	Work	HR	Verified or self-asserted
Work email	Work	MX/domain proof	Verified or self-asserted
Work phone	Work	HR or OTP	Verified or self-asserted
Personal email	Personal	OTP link	Verified
Mobile / personal phone	Personal	SMS OTP	Verified
LinkedIn URL	Work / Personal	OAuth proof	Verified or self-asserted
Location (city, country)	Custom	IP / self	Verified
Custom (≤ 3 fields)	All	Self-attested	Self-asserted

Each attribute carries a provenance mark in the verifier's view. A check mark indicates a verified source. A dot indicates self-asserted. Tooltips explain provenance. The verifier can make trust decisions on the basis of source quality, and People verification does not pretend self-asserted data is verified.

What people verification is not

Not a session-establishment protocol. People verification does not establish an online session for a relying party. It establishes that two humans have cryptographically verified each other in a specific moment, with a specific attribute set, recorded in audit. Session-bearing protocols (OIDC, SAML) are separate.

Not a substitute for identity proofing. People verification verifies that the presenter holds the cryptographic credential bound to a previously-proofed identity. The proofing happened at enrollment. People verification exercises the binding. (See What Is Identity Proofing?.)

Not a replacement for in-band MFA. Workforce SSO, customer logins, and admin consoles still use FIDO2/WebAuthn passkeys, PIV/CAC, or other web-channel authentication. People verification is the human-to-human channel that complements those, particularly where AI-generated impersonation has eroded traditional human-verification practices.

Not a video-recognition or voice-print system. People verification deliberately does not authenticate by face match, voice match, or behavioral biometric. Those signals are increasingly probabilistic and increasingly defeatable. People verification uses cryptography because cryptography survives AI capability progression.

The threats People verification defeats

Threat	How People verification addresses it
Voice cloning of executives, vendors, IT	Cryptographic round trip with the enrolled device. AI cannot sign without the private key.
Deepfake video on calls	Same. The deepfake on the call cannot complete the cryptographic ceremony.
AI-generated synthetic relationship building	Cryptographic verification at the moment of the ask. Weeks of charm do not produce a private key.
Phishing and adversary-in-the-middle	Out-of-band QR with signed payload, certificate thumbprint, short TTL, channel binding.
MFA fatigue / prompt bombing	No push-to-approve in people verification. Both sides explicitly act.
SIM swap / SMS interception	SMS link is single-use, short-lived, app-bound. Not a reusable OTP. Channel can be policy-disabled.
Token theft / replay	DID, QID, Type Code one-time. WebSocket channel binding. Server invalidates consumed artifacts.
Device compromise (jailbreak, root)	Mobile blocks crypto ops on failed posture checks. Keys remain in Secure Enclave/TEE.
Help-desk social engineering	No identity changes occur over phone support without a successful people verification first.
Coerced oversharing	Overshare Anomaly metric (z-score on attribute toggles vs baseline) can trigger step-up or block.

For the deepfake-resistance case in detail, see Deepfake-Resistant Identity Verification. For help-desk specifically, see Stopping Help-Desk Impersonation with People Verification.

Performance and reliability

These are design targets from the engineering spec, not published production measurements. Sanctioned production numbers will follow engineering sign-off:

- **End-to-end verification:** a few seconds after the verifier triggers consume, versus the 30 to 90 seconds typical of knowledge-based questions.
- **Verification completion rate:** ≥ 98.5% under healthy network conditions (design target).
- **Replay attempts that succeed:** target 0%, ceiling 0.05%.
- **Server-side biometric template storage:** zero. Device-bound keys only. ScrambleID never receives or stores biometrics.
- **Accessibility:** all critical steps operable via screen reader and large text.

How People Verification relates to the broader ScrambleID architecture

People verification is one of three non-traditional channels (alongside Agent and Machine-to-Machine) built on the same cryptographic foundation:

- **Hardware-bound private keys** held in Secure Enclave, StrongBox, TPM, or HSM.
- **Dynamic Identifiers (DIDs):** per-session, single-use, server-issued, short-TTL.
- **QR Identifiers (QIDs):** QR-encoded DIDs with environment-signed payloads and certificate thumbprints.
- **Canonical opaque identifiers:** SUID (System User ID) and ZID (Device ID). PII is never used as a key handle.
- **WebSocket channel binding:** results delivered only to the bound channel.

The same primitives that authenticate two humans in a people verification authenticate an AI agent calling a tools API or a backend service requesting a token. The surface adapts to the channel; the cryptographic guarantee is identical.

For architectural depth, see The ScrambleID Identity Fabric.

Standards alignment

- **W3C WebAuthn Level 2/3:** device user verification (UV) on the platform authenticator, no biometric template storage server-side.
- **FIDO2:** alignment of the on-device authenticator semantics.
- **NIST SP 800-63B:** People verification does not by itself establish an online session, but the authenticator posture (device-bound keys, WebAuthn UV) aligns with AAL2+ practices when combined with enterprise policy.
- **NIST SP 800-207 (Zero Trust):** out-of-band, short-lived, signed artifacts reduce the credential-theft surface; per-event audit supports continuous evaluation.
- **Privacy:** data minimization is structural. Presenters choose which attributes to share. Retention is in tenant-scoped tables with configurable history windows.

Key Takeaway

People verification is a class of authentication where two humans cryptographically verify each other's identity directly, without a central call center or helpdesk, using hardware-bound private keys on each party's device. ScrambleID People is the implementation, now live with early-access customers ahead of general availability: one party (presenter) selects which identity attributes to share, the other (verifier) consumes them through a single-use server-issued artifact (QR code/QID, Type Code, or SMS deep link) with a default 60-second time-to-live. Both parties see identical results. The cryptographic round trip cannot be defeated by AI-generated voice or video because no AI can produce a signature without the matching hardware-bound private key. People verification shifts authentication from probabilistic detection (which AI is winning) to deterministic cryptography (which AI cannot defeat). A verification completes in a few seconds, versus the 30 to 90 seconds typical of knowledge-based questions, with a replay-success target of 0%.

FAQ

What is people verification?

People verification is a class of authentication where two humans cryptographically verify each other's identity directly, without an intermediary call center or helpdesk. Each party holds a hardware-protected private key on their device. One party (the presenter) shares a selected subset of identity attributes; the other (the verifier) consumes them through a single-use, server-issued artifact (QR code, Type Code, or SMS deep link) with a short time-to-live. Both parties see identical results. The cryptographic round trip cannot be forged by AI-generated voice or video because no AI can produce a signature without the matching private key.

How is people verification different from showing a photo ID?

Photo ID verification is probabilistic: the verifier compares a photo on a card to the face in front of them and decides if they match. The card can be forged. The face the verifier has never seen before. people verification is deterministic: a cryptographic signature produced by the presenter's hardware-bound private key, validated against a public key registered to that identity. There is no probability to debate. Either the signature verifies or it does not. AI deepfake technology that defeats face-to-photo comparison cannot defeat signature verification because no AI can sign without the private key.

Is people verification just QR-based authentication?

QR is one of three artifact channels (QR code carrying a QID, a short Type Code, or an SMS deep link). The QR is the most common because it works in person without speaking aloud. Type Codes are useful when scanning is impractical (over a phone call, for example, where the presenter speaks the code and the verifier types it). SMS deep links are used for distant verification scenarios where

both parties are not co-located. All three artifact types carry the same single-use Dynamic Identifier with a default 60-second TTL and the same cryptographic guarantees.

What attributes does a presenter share?

The presenter selects a profile (Work, Personal, or Custom) before sharing. The catalog includes verified attributes (legal name, employer, job title, work email, work phone, personal email, mobile phone, LinkedIn URL, location) and self-asserted attributes (custom fields, photo). Each attribute carries a provenance mark in the verifier's view: a check mark for verified sources, a dot for self-asserted. The verifier can make trust decisions on the basis of source quality. The presenter sees a live preview of exactly what will be shared before pressing Continue.

Why can't AI deepfakes defeat people verification?

People verification does not authenticate by face match, voice match, or behavioral signal. It authenticates by cryptographic signature. The presenter's device produces a signature using a private key that lives in hardware-protected storage (Apple Secure Enclave, Android StrongBox, Windows TPM) and cannot be extracted, copied, or impersonated by any software. AI can clone a voice from 30 seconds of audio. AI can produce convincing real-time deepfake video. AI cannot produce a cryptographic signature without holding the matching private key. People verification shifts authentication from probabilistic detection (which AI is winning) to deterministic cryptography (which AI cannot defeat).

How long does a people verification take?

A few seconds end-to-end after the verifier triggers the consume step, versus the 30 to 90 seconds typical of knowledge-based questions. The artifact (QR/QID, Type Code, SMS link) has a default 60-second time-to-live with ±90 second clock-skew tolerance. Most of the wait is the network round trip and the mobile UI render; the cryptographic exchange itself is the fast part.

Does people verification work without internet?

The standard people verification flow is online: both parties' apps communicate with the ScrambleID service via REST and WebSocket. For the agent and machine-to-machine channels, ScrambleID supports an offline Dynamic Identifier handshake pattern (covered by US Patent 12,388,656 B2) that works in air-gapped environments. The same DID primitive is the foundation for both the online people verification flow and the offline machine handshake.

References (public)

- W3C WebAuthn Level 2: https://www.w3.org/TR/webauthn-2/
- FIDO Alliance, Passkeys: https://fidoalliance.org/passkeys/
- NIST SP 800-63B: https://csrc.nist.gov/pubs/sp/800/63b/4/final

- NIST SP 800-207 (Zero Trust): https://csrc.nist.gov/publications/detail/sp/800-207/final
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Related reading

- People Trust Checks
- People Verification Implementation Guide
- Deepfake-Resistant Identity Verification
- Stopping Help-Desk Impersonation with People Verification
- People Verification vs Photo ID, Video, Notary, and KBA
- What Is Phishing-Resistant MFA?
- The ScrambleID Identity Fabric