People Trust Checks: Cryptographic Person-to-Person Verification With Consent and Data Minimization

People & In-Person / Last updated 2026-06-11 / https://www.scrambleid.com/learn/people-trust-check

> **Status (June 2026):** Early access. People Trust Checks and the wider People verification family are live with early-access customers and aren'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: A People Trust Check is a **verifier-initiated, consent-based session** where the presenter shares a **time-limited Unified ID Card view** (Work/Personal/Minimal/Anonymous or custom) that clearly distinguishes **verified attributes** from **self-asserted** ones, so verification is fast, privacy-preserving, and resistant to replay.

TL;DR (canonical)

- Trust Checks replace "screenshot theater" with a **live session** and a **freshness indicator**.
- The verifier can declare a requirement ("Need: Work / Minimal / Anonymous / None"); the presenter retains autonomy but must remain compliant.
- The presenter always sees a **preview** of what will be shared before accepting.
- Attributes carry **provenance** (verified check ✓ vs self-asserted dot •) to reduce spoofing.
- Trust Checks can be launched in-person (QR / code) or via messaging links.

Why is most identity verification replayable?

Common patterns today:

- "Text me a photo of your badge."
- "Send me a screenshot of the app."
- "Forward me the email."

These fail because they are:

- replayable and easy to forge,
- detached from a live session,
- hard to audit,
- prone to oversharing.

Trust Checks are designed around the opposite assumptions: **freshness**, **consent**, **minimization**, and **provenance**.

What is a People Trust Check?

A People Trust Check is a short-lived, verifier-initiated session where a presenter consents to share a time-limited, provenance-marked ID Card view. It has two roles:

- **Verifier (initiator):** requests a Trust Check and (optionally) declares required fields.
- **Presenter (receiver):** reviews and consents to share a compliant ID Card view.

A Trust Check does **not** mean "this person is safe". It means: *"The presenter is the holder of a bound identity and is sharing a controlled card view right now."*

How do you launch a Trust Check?

1) Face-to-face (QR or short code)

- Verifier shows a QR.
- Presenter scans or types a short code.
- Presenter previews, chooses a compliant profile, and shares.

2) Smart link (messaging)

- Verifier sends a link (e.g., via iMessage, SMS, chat).
- Presenter taps, previews, and shares.

The key property is consistent: the share is **time-limited** and the renderer displays **freshness** and **provenance**.

What is the Trust Check flow?

1. Verifier initiates a Trust Check and chooses a requirement pill:
    - **Need: None** (full picker)
    - **Need: Work** (must include mandatory Work fields)
    - **Need: Minimal**

- **Need: Anonymous**

2. Presenter opens the request and sees a **preview** of what will be shared.
3. Presenter selects a profile:
   - Work
   - Personal
   - Minimal
   - Anonymous
   - Custom (bounded)
4. Presenter taps **Accept & Share**.
5. Verifier receives a **one-time ID Card view** and a trust summary:
   - Human-verified ring + freshness
   - Attribute provenance markers (✓ vs •)
   - Optional social proof (mutual trusted contacts)

How do profiles and requirement pills work?

The requirement pill is a design constraint that prevents under-sharing while preserving consent.

If no requirement is set: the presenter sees the full picker.

If a requirement is set: the UI adapts:

- **Accept/Reject sheet** when the last-used profile already complies (fast path)
- **Filtered picker** when the last-used profile is non-compliant (compliance enforced)

Requirement contract (concept)

```
{
  "requiredProfile": {
    "level": "WORK",
    "mandatoryFields": ["legalName", "companyName", "title"]
  }
}
```

How does data minimization work in Trust Checks?

ScrambleID treats oversharing as a security problem.

The Unified ID Card carries provenance metadata:

- ✓ **Verified** attribute (solid check)
- • **Self-asserted** attribute (dot)
- ☁̸ **Temporarily unavailable** (offline/pointer-stale)

Example (Work card):

- Work Email: alice.j@company.com ✓
- Work Phone: +1-404-555-0199 •

This is the core differentiator versus traditional "profile" sharing: the verifier can see what is verified vs merely claimed.

What replay resistance do Trust Checks provide?

Trust Checks make replay meaningfully harder by providing:

- **Freshness** (time-bounded sessions)
- **One-time views** (session-scoped)
- **Consent at the moment of share**

No system can stop someone from taking a photo of a screen. The goal is to make screenshots **obviously stale** and **less useful** by:

- displaying freshness context,
- showing provenance badges,
- making the share tied to a session and a specific moment.

Where are Trust Checks used?

- Field operations (technicians, deliveries, on-site work)
- In-person customer interactions (branch, retail, events)
- Executive verification for high-risk communications ("Is this really the CFO?")
- "Verify-me" moments during suspected social engineering

What metrics should you publish for Trust Checks?

- Trust Check completion rate
- Time-to-verified view (median / p95)
- Receiver UI state distribution (S0 full picker / S1 accept-reject / S2 filtered)
- Overshare anomaly rate (if you instrument picker overrides)

(See Metrics + ROI Playbook.)

Key Takeaway

Person-to-person identity verification (People Trust Checks) enables humans to cryptographically verify each other's identity with explicit consent and data minimization. Unlike showing a screenshot or badge, Trust Checks are live, session-bound, and cannot be replayed. This prevents social engineering, exec impersonation, and "CEO fraud" attacks.

FAQ

What is people verification?

People verification is a real-time identity confirmation between two people, one person (the verifier) initiates a check, and the other (the presenter) shares verified identity attributes through a trusted channel. Unlike document checks or database lookups, people verification produces live, session-bound proof that cannot be replayed or forwarded.

What problem does people verification solve?

People verification stops impersonation attacks where someone claims to be a colleague, vendor, or authority figure. Common scenarios include: verifying IT support callers, confirming delivery personnel, validating visitors at secure facilities, and stopping "CEO fraud" where attackers impersonate executives.

How is a People Trust Check different from showing an ID badge?

ID badges can be forged, borrowed, or photographed. A People Trust Check produces cryptographic proof that the presenter controls a registered ScrambleID identity, with verified attributes from authoritative sources (employer directory, government ID). The verification is live and session-bound.

Can the verification link be forwarded to someone else?

Links can be forwarded, but verification requires the ScrambleID app bound to the presenter's device; a forwarded link does not produce a valid verified share. Concretely, the binding is a hardware-backed private key (Secure Enclave on iOS, TEE or StrongBox on Android) that signs the session-bound challenge. The biometric only unlocks the local key material and never leaves the device, so the attacker would need the victim's enrolled device and biometric.

What attributes can be shared in a Trust Check?

The presenter chooses which attributes to share: Work profile (name, title, employer), Minimal (name only), Anonymous (membership verification without name), or custom selections. Verified attributes show provenance; self-asserted attributes are clearly marked.

What is the verification time-to-live (TTL)?

Verification results are time-bounded. Policy controls how long a verification remains valid before the verifier must re-check. This prevents replay of stale verifications.

References (public)

- NIST Digital Identity Guidelines overview (assurance concepts): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf

---

Related reading

- People Verification Implementation Guide
- Unified ID Card: Attribute Provenance
- ID Card Picker: Consent UX