People Verification for Physical Sites: Contractor, Visitor, and In-Person Counterparty Verification

People & In-Person / Last updated 2026-06-11 / https://www.scrambleid.com/learn/people-verification-for-physical-sites

> **Status (June 2026):** Early access. The People verification family is live with early-access customers and isn't generally available yet. The walkthroughs below describe how the shipped flow works today, not deployments you can reference; talk to your ScrambleID account team about access and timelines.

In one sentence: Physical-site identity verification (contractors, vendors, visitors, in-person counterparties) has historically depended on physical badges, photo IDs, and phone trees that can be forged, cloned, and social-engineered; person-to-person cryptographic verification adds a deterministic identity gate at the physical access point in a few seconds, with a signed audit trail.

TL;DR (canonical)

- **The threat:** social engineering at physical access points (claimed contractor at a server room, claimed delivery driver at a loading dock, claimed bank examiner at a branch, claimed clinical handoff at a hospital floor) is one of the most under-defended attack surfaces in enterprise security.
- **Traditional defenses are eroding:** physical badges are forgeable, RFID is cloneable, photo IDs are forgeable at high quality, and phone-tree confirmation is socially engineered.
- **What people verification adds:** a cryptographic verification gate at the physical interaction, completed in a few seconds (versus the 30 to 90 seconds typical of knowledge-based questions), with a signed audit event.
- **Where this matters most:** server rooms, utility closets, executive floors, branch high-value transactions, healthcare controlled areas, critical-infrastructure facilities, currency-courier handoffs, secure document custody.
- **The pattern is layered, not replacing:** physical badges, photo IDs, and existing access controls remain in place; People verification is the deterministic anchor for high-trust interactions on top.

Why physical-site verification is increasingly an attack target

Several converging trends:

1. **Cyber attackers have noticed physical paths.** Once internal network controls tighten, attackers turn to social engineering at facilities. Scattered Spider, ALPHV, and several APT groups have used physical-presence pretexts.
2. **Insider threat is durable.** The threat from a single compromised contractor or visitor with physical access has not diminished as cyber controls have improved. CISA's insider-threat resources continue to highlight the path.
3. **Critical infrastructure is in regulatory focus.** Energy, water, transportation, and healthcare facilities face explicit regulator expectations (TSA, NERC CIP, CISA, sector-specific) for physical access verification.
4. **Branch banking is a residual high-value path.** Currency, sensitive documents, customer assets, and access to internal systems all live at the branch.
5. **Healthcare facility access is a controlled-substance and PHI risk.** Drug rooms, clinical handoffs, and shared workstations are physical-access decisions with material risk.

The traditional defenses (badge inspection, photo ID, phone-call confirmation to dispatch) were designed when forgery was hard, social engineering was rare, and the attacker was less prepared. Today's adversaries have prepared OSINT, voice-cloning capability, deepfake video for distant verifications, and access to internal communications via prior compromise.

What's wrong with the traditional toolkit

Defense	Why it's eroding
Physical badge with photo	High-quality forgery is cheap; old badges are recoverable from trash
RFID badge	Cloneable with consumer-grade readers in seconds
Photo ID	Forgery quality has improved dramatically; verifier rarely scrutinizes
Sign-in book	Self-asserted; verification is procedural
Phone confirmation to dispatch	Voice-clone defeatable; dispatch number can be misdialed-by-design
Pre-registered visitor list	Useful but does not verify identity, only that someone with a name was expected
"I recognize them"	Contractor turnover is high; recognition decays
Photo-on-file vs camera	Defeated by AI face augmentation; not always operationally feasible

None of these is useless. The combination of all of them in a layered process can be reasonably strong. The point: none of them produces a cryptographic, deterministic, AI-resistant verification on its own.

How the people verification flow looks at a physical site

Concrete examples by site type:

Corporate facility, contractor at server room

- Contractor arrives at the security desk requesting access to the data center.
- Security staff initiates a people verification with the contractor's enrolled identity (the contractor was pre-enrolled as part of vendor onboarding).
- Contractor's mobile device prompts. Contractor approves with Face ID.
- Verification completes in a few seconds. Security sees the contractor's verified identity card: legal name, employer, work role, photo, work email (verified attributes flagged).
- Security cross-references the work order. Access proceeds with appropriate escort.
- Audit log records: timestamp, location (security desk ZID), contractor identity (SUID), attribute set, work-order reference, verification outcome.

Bank branch, customer requesting high-value transaction

- Customer presents at branch teller window for a $50K cash withdrawal.
- Teller initiates a people verification through the bank's customer authenticator. Customer's enrolled device authenticator prompts on their phone.
- Customer approves. Verification completes.
- Teller sees verified customer identity card with appropriate attributes (account-bound, not raw PII).
- Transaction proceeds. Audit captures the in-branch people verification event tied to the transaction record.

Healthcare facility, clinical handoff for controlled-substance access

- Clinician requests access to controlled-substance room outside their normal floor.
- Pharmacy or floor security initiates a people verification.
- Clinician's device authenticator signs the challenge.
- Verification confirms clinician's identity, role, and floor authorization.
- Access is granted. Audit captures who, when, where, attribute set, signed event.

Critical infrastructure facility, vendor visit

- Vendor technician arrives at a substation or water treatment facility.
- Site supervisor initiates a people verification through the vendor's enrolled work identity.
- Vendor's device authenticator signs.
- Verification confirms vendor identity, role, employer, work order.

- Site access proceeds with appropriate escort and time-bounded scope.

Currency or sensitive-document courier handoff

- Courier arrives at the receiving location for a chain-of-custody handoff.
- Receiver initiates a people verification with the courier's enrolled identity.
- Courier's device signs the challenge.
- Verification completes; the signed event is the chain-of-custody anchor for the handoff.
- Both sides have a cryptographic audit record of the handoff.

The pattern is consistent: the cryptographic verification gates the physical-access decision. The verification produces a signed audit event tied to the physical interaction.

The verifier's view: what shows up on screen

When the verifier (security staff, teller, clinician, dispatcher) consumes the artifact, they see the presenter's identity card with attribute provenance:

- **Photo / avatar** with verified ring (device-bound liveness check)
- **Legal name** with provenance mark (verified via HR/KYC, or self-asserted)
- **Employer / company** with provenance mark (verified via HR, or self-asserted)
- **Job title and department** (verified or self-asserted)
- **Work email** (verified via MX/domain proof)
- **Work phone** (verified via HR or OTP)
- **Custom attributes** (≤3 self-asserted fields; useful for purpose-of-visit context)

Each attribute carries a provenance mark. The verifier can make trust decisions on the basis of source quality (verified employer is stronger evidence than self-asserted employer). The cryptographic verification confirms the holder of the credential; the attributes confirm the contextual identity claims.

When people verification at physical sites is appropriate

The pattern fits where:

- **Access has material consequence** (data center, drug room, executive floor, currency, sensitive documents).
- **The visitor population is bounded enough to be enrolled** (named contractors, banked customers, badged employees, regulated couriers). For purely walk-in low-stakes traffic, the operational overhead is not worth it.

- **The procedural friction is acceptable** (security desk, teller window, supervisor approval) versus tap-and-go physical access. people verification is appropriate at decision points, not every door.
- **Audit and compliance value is real** (regulated industries, high-insurance-value contexts, legal chain-of-custody).

The pattern does not fit where:

- **Pure walk-in traffic** (retail customers paying with cash). Existing processes remain.
- **Low-friction perimeter** (cafeteria entry, lobby pass-through). Badge or biometric remains.
- **Speed-critical operational flows** where cryptographic friction would meaningfully degrade throughput.

Combining people verification with existing physical access systems

The architecture is layered, not replacement:

Layer	Existing	People Verification contribution
Perimeter (lobby, gate)	Badge, RFID, biometric, sign-in	Optional people verification for visitor-host confirmation
Internal access (floor, area)	Badge with role-based access	people verification at access decision for high-trust areas
Specific room access (data center, drug room)	Badge plus PIN, biometric, escort	people verification of identity and authorization
High-value transaction (branch, vault)	Existing teller process	people verification gate at the transaction
Chain-of-custody handoff	Manual signature	signed verification event as the chain-of-custody record

The pattern preserves existing physical access controls while adding cryptographic verification at decision points where forgery, cloning, or social engineering would have material consequence.

What about offline scenarios?

Some high-security physical sites are intentionally network-isolated (SCIFs, certain critical-infrastructure rooms, financial-services vaults). The standard people verification flow requires connectivity for the WebSocket channel and DID validation.

For offline scenarios, ScrambleID supports an offline Dynamic Identifier handshake pattern (covered by US Patent 12,388,656 B2) where a client agent and a server agent exchange a Dynamic Identifier within a time window, the verifier posts the DID to ScrambleID when reconnected, and the cryptographic verification is confirmed out-of-band. This pattern is more commonly applied to

machine-to-machine air-gapped scenarios; the application to in-person verification at network-isolated facilities is straightforward in principle.

For network-isolated branches and facilities, the practical pattern is to use intermittent connectivity (verifier's mobile device on cellular even when site network is offline) plus cached organizational policy. Pure-air-gap deployments require explicit architectural review.

Privacy and consent

People verification at physical sites preserves the same privacy properties as other People verification uses:

- **Presenter chooses what to share.** A contractor at a data center might share legal name, employer, and role. A customer at a bank branch might share name and account binding. A clinician at a controlled-substance room might share name, role, and authorization scope.
- **Verifier sees attribute provenance.** Verified vs self-asserted is explicit.
- **No biometric template storage server-side.** Device authenticators stay local; only cryptographic assertions reach the server.
- **Audit is tenant-scoped.** Verification events are stored under organizational policy.
- **Retention is configurable.** History windows are organizational settings.

For sensitive populations (healthcare clinicians, regulated industries, government contractors), explicit attribute selection means the verification can be performed with the minimum data necessary for the access decision.

Operational considerations

Vendor/contractor enrollment. Vendor security expectations should include a People enrollment requirement for representatives who will visit physical sites. Most enterprise vendor onboarding processes accommodate this with a one-time enrollment step.

Visitor pre-registration integration. Existing visitor management systems (Envoy, Proxyclick, iLobby, etc.) can integrate People verification with the host so the host's "approve admission" action becomes a cryptographic event rather than a click.

Branch teller training. Branch staff need training on when to invoke ScrambleID People (high-value transactions, account changes, customer-data-sensitive inquiries) versus when traditional verification suffices (low-stakes inquiries, deposits below threshold).

Healthcare workflow latency. Clinical environments are extremely latency-sensitive. A verification that takes a few seconds fits within typical workflow tolerance but should be tested in the specific clinical context (code-blue scenarios, ED handoffs, etc.).

Critical-infrastructure regulatory framing. TSA, NERC CIP, FERC, and sector-specific frameworks may have specific verification expectations for site access. Access gated by people verification supports these frameworks but does not by itself satisfy regulator-specific physical-security requirements (which include camera coverage, escort policies, log retention, etc.).

Standards posture

People verification at physical sites maps to:

- **NIST SP 800-63B authenticator posture** at the cryptographic verification.
- **NIST SP 800-207 Zero Trust** continuous verification at every interaction.
- **CISA insider threat mitigation** principles for physical-access decisions.
- **Industry-specific frameworks** (TSA, NERC CIP, HIPAA Security Rule physical safeguards, PCI DSS physical access controls).

For regulated-industry depth, see the relevant industry guide:

- Authentication for Financial Services
- Authentication for Healthcare
- Authentication for Government and Public Sector

Key Takeaway

Physical-site identity verification (contractors, vendors, visitors, in-person counterparties) has historically depended on physical badges, photo IDs, and phone-tree confirmation, all of which are increasingly defeatable through forgery, RFID cloning, AI-driven document fabrication, and voice-cloning of dispatch contacts. Person-to-person cryptographic verification adds a deterministic identity gate at the physical decision point, completing in a few seconds (versus the 30 to 90 seconds typical of knowledge-based questions) with a signed audit event tied to the physical interaction. The pattern is layered (existing badges, photo IDs, and access controls remain) and applies where access has material consequence: data centers, drug rooms, executive floors, branch high-value transactions, healthcare controlled areas, critical-infrastructure facilities, and chain-of-custody handoffs. The verification produces a verifier-visible identity card with attribute provenance (verified employer/role vs self-asserted) and a tenant-scoped immutable audit record.

FAQ

What's wrong with physical badges?

Physical badges can be forged at high quality with consumer-grade printing, cloned via inexpensive RFID readers, and stolen or borrowed without immediate detection. They are useful as a low-friction

social signal in low-threat contexts but are not adequate verification for high-trust physical-site interactions (utility-room access, server rooms, executive floors, branch high-value transactions, healthcare access to controlled areas).

How does people verification work at a physical site?

Security staff (or branch teller, clinical staff, dispatch operator) initiates a people verification request from their ScrambleID app. The visitor or counterparty's enrolled device authenticator signs a server-issued single-use challenge with a 60-second TTL using the QR/QID channel (most common in-person), the Type Code channel (for distance scenarios), or the SMS deep link channel. Both parties see the verified identity card with attribute provenance (verified employer, verified role, verified work email). The interaction proceeds only on success.

What if the contractor's company doesn't use ScrambleID?

ScrambleID-bound verification only works for parties enrolled with ScrambleID. For non-enrolled contractors, the fallback is the existing process (physical badge check, photo ID, phone tree to vendor's dispatcher). The recommended pattern is to make enrollment a condition of physical-site access in the contract itself; this is typically negotiated as part of the broader vendor security expectations and does not require the contractor's own employees to use ScrambleID for anything beyond client-facing interactions.

Does this work for delivery drivers and walk-in vendors?

Yes, particularly for high-trust deliveries (HVAC repairs, server maintenance, security camera installation, currency couriers) where the access granted is consequential. For low-stakes delivery (package drops, food delivery), the operational overhead of People enrollment is typically not worth it; the existing process remains. The pattern: people verification is appropriate where the visitor has access to assets material to the organization.

What about visitor lobbies in office buildings?

Office-lobby visitor verification typically combines pre-registration (the visitor's host pre-registers them, the visitor receives a check-in QR), in-person ID inspection (existing process), and optionally a people verification with the host (the visitor's host receives a verification request when the visitor arrives, and confirms the visit cryptographically rather than just clicking a "yes admit" button). The people verification with host adds host-side cryptographic accountability without slowing the visitor's lobby flow.

How fast is verification at a busy lobby?

The verification itself completes in a few seconds after the verifier triggers consume, versus the 30 to 90 seconds typical of knowledge-based questions. The bottleneck at a busy lobby is typically the visitor opening their app and approving the prompt; this takes a few additional seconds. The total in-

lobby time is comparable to existing visitor processes (badge issuance, sign-in form) and produces a much stronger audit trail.

References (public)

- CISA Insider Threat Mitigation Resources: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation
- FBI / CISA Joint Advisory on Scattered Spider (AA23-320A): https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
- 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

---

Related reading

- What Is People Verification?
- People Verification vs Photo ID, Video, Notary, and KBA
- Stopping Help-Desk Impersonation with People Verification
- People Verification for Finance: Wire Transfers and Vendor Banking Changes
- Deepfake-Resistant Identity Verification
- Authentication for Financial Services
- Authentication for Healthcare