TeleSeal Identity Proofing Checklist

Version: 1.0
Effective Date: 2025-07-27
Review Cycle: Annual
Owner: Chief Information Security Officer (CISO)

---

1. Purpose

This checklist establishes auditable procedures to ensure compliance with Arizona Remote Online Notarization (RON) identity proofing requirements. It aligns with industry standards (e.g., NIST SP 800-63-3 IAL2/AAL2) and provides a structured approach to protect notarial integrity.

2. Scope

This checklist applies to:

- All commissioned Arizona notaries performing remote online notarizations.
- All RON platforms and providers approved for use by TeleSeal.
- All principals and credible witnesses participating in RON sessions.

3. Definitions

- **Credential Analysis:** Automated verification of a government-issued photo ID.
- **Dynamic KBA:** Knowledge-based authentication using time-limited questions.
- **MFA:** Multi-factor authentication combining at least two independent factors.
- **Personal Knowledge:** Notary's direct, long-standing familiarity with the principal.
- **Credible Witness:** A third party who identifies the principal under state rules.
- **Provider/Platform:** Approved RON technology used for identity proofing and notarization.

4. Compliance Overview (Arizona RON)

- Identity proofing must occur **before** the notarial act.
- MFA is required, typically credential analysis + dynamic KBA, unless personal knowledge or credible witness applies.
- Identity proofing outcomes must be recorded in the electronic journal and associated with the audiovisual recording.
- Only approved providers meeting Arizona RON and industry standards may be used.

5. Roles & Responsibilities

Role	Responsibility
Notaries	Perform and document identity proofing per this checklist.
CISO	Owns this checklist, approves exceptions, monitors compliance.
Vendors	Provide compliant credential analysis, KBA, and MFA tools; maintain audit trails.

---

6. Checklist Procedures

6.1 Pre-Session Readiness

- Confirm notary's physical location is within licensed state.

- Confirm RON platform/vendor is on approved list.
- Enable time sync, logging, and session recording.
- Verify principal's device supports audio/video and ID capture.

6.2 Primary Method: Credential Analysis + Dynamic KBA

Credential Analysis

- Collect front and back images of valid government ID.
- Validate security features, MRZ/barcode, tamper detection.
- Perform liveness/face match between ID and live capture.
- Confirm consistency of data (name, DOB, expiration).
- Record provider, reference ID, timestamp, pass/fail result.

Dynamic KBA

- Generate time-limited questions from reliable sources.
- Enforce minimum pass criteria and time limits.
- Allow limited attempts; rotate failed questions.
- Record provider, timestamp, pass/fail, attempt counts.

Decision Gate

- Proceed only if both credential analysis **and** KBA pass.
- If either fails, follow Failure Handling.

6.3 Alternative Methods (if permitted)

Personal Knowledge

- Notary documents basis/duration of familiarity.

Credible Witness

- One personally known witness or two unknowns per state law.
- Proof each witness with credential analysis + KBA (unless personally known).
- Record oath, name, address, contact in journal and recording.

6.4 Fraud and Risk Controls

- Confirm ID name matches session/document name.
- Screen for coercion; terminate if suspected.
- Require physical IDs, not copies/screenshots.
- Capture principal's location for certificate wording.
- Re-verify if session interrupted or rejoined.

6.5 Failure Handling

- **Credential Analysis Fail:** Allow one re-capture; escalate or reschedule.
- **KBA Fail:** Limited retry; otherwise require credible witness or reschedule.
- **Lockout:** After repeated failures, document reason and outcome.
- **Do not proceed** if identity cannot be reliably established.

6.6 Journaling & Recording

- Journal entry includes date/time, act type, doc description, principal's name, method used, provider(s), pass/fail, attempts, credible witness info, fees.
- Associate journal entry with audiovisual recording and provider transaction IDs.
- Retain journal, recordings, and metadata per state law.
- Protect PII with encryption and restricted access.

6.7 Platform & Vendor Requirements

- Automated credential analysis with liveness/face match.
- Dynamic KBA per state/industry standards (time limits, attempts, refresh).
- Auditable logs, timestamps, reference IDs.
- Compliance with SOC 2/ISO 27001 and NIST SP 800-63-3 alignment.
- Contracts cover uptime, incident response, data retention, breach notification.

6.8 Quality Assurance

- Periodically sample RON sessions for compliance.
- Review vendor pass/fail rates and anomalies.
- Remediate gaps with training and updated procedures.

6.9 Training & Access

- Notaries complete required state RON training and registration.
- Limit platform access to authorized notaries; review quarterly.

6.10 Change Management

- Monitor statutes, rules, SOS guidance; update checklist as needed.
- Communicate updates to all notaries and vendors.

---

7. Exceptions

- Exceptions must be documented in the Exception Register.
- Must be approved by the CISO.
- Must include compensating controls (e.g., additional verification, audit review).