TeleSeal Certificate Management Policy

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

1. Purpose

To establish consistent controls for the lifecycle of X.509 certificates used by TeleSeal—notary PDF-signing certificates and server TLS certificates—ensuring their secure issuance, storage, use, renewal, and revocation in support of Arizona RON requirements (A.R.S. § 2-12-1307).

2. Scope

This policy covers all digital certificates within TeleSeal:
- **Notary-provided X.509 certificates** used for document sealing
- **Platform TLS/HTTPS certificates** (e.g. `teleseal.app`, `telesealhq.com`)
- **Code-signing or API client certificates**, if any

It applies to all personnel and systems involved in certificate handling: Notaries, Developers, IT/DevOps, Security Team.

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy owner; approves exceptions; oversees audits
Security Team	Define certificate standards; monitor compliance; conduct reviews
IT/DevOps	Issue, install, renew, and revoke server certificates; enforce HSM/KMS usage
Notaries (Users)	Provide valid X.509 certificates; safeguard private keys locally
Compliance Team	Verify certificate attributes against Arizona RON statute

4. Policy Statements

4.1 Certificate Standards

- **Key Algorithms:** RSA 2048+ or ECDSA P-256+
- **Signature Hash:** SHA-256 or stronger
- **Validity Period:**
  - **Notary certificates:** <= 3 years (per state commission term)
  - **TLS certificates:** <= 1 year (auto-renew via ACME)

4.2 Notary Certificate Onboarding

1. **Submission:** Notary uploads public certificate (`.pem` or `.crt`) via secure onboarding portal.
2. **Validation:**

   - Confirm certificate subject DN includes Notary's legal name, commission number, and state of commission.

   - Verify certificate chain to a trusted root or intermediate CA.

3. **Installation:**
   - Public certificate metadata imported into Teleseal.app PKI registry.

   - Private key **never** leaves the Notary's device/HSM.

4.3 Certificate Storage & Access

- **Public Certificates & Metadata:**
  - Stored encrypted in AWS RDS (AES-256 + KMS).

  - Access limited to signing microservice and Compliance Team via RBAC & MFA.

- **Private Keys:**
  - Held **exclusively** by Notaries in a secure store (hardware token, OS keychain, or HSM).

  - TeleSeal does **not** store or transmit private keys.

4.4 Certificate Use in PDF Sealing

- Signing operations performed in-browser or in dedicated microservice called by client, invoking the Notary's private key locally.

- The platform attaches the certificate's public portion and seal metadata into the PDF per A.R.S. § 2-12-1307 certificate block requirements.

4.5 Renewal & Expiry

- **Notary Certificates:**
  - Notaries must submit renewed certificates at least **30 days** before expiry or commission renewal.

  - Expired certificates are removed from the PKI registry and any in-flight signing requests will be blocked.

- **TLS Certificates:**
  - Automated via ACME (Let's Encrypt or internal CA); monitored by IT/DevOps with alerting on < 15 days to expiry.

4.6 Revocation & Compromise

- **Revocation Triggers:**
  - Notary commission suspension or termination

  - Certificate key compromise or device loss

- **Revocation Process:**
  1. Notary or Compliance submits revocation request.

  2. Security Team marks certificate revoked in PKI registry.

    3. For TLS: Remove certificate from load balancers and issue replacement.
    4. Notify affected parties (e.g., clients with pending transactions).

- **CRL/OCSP:**
    - Maintain and publish an internal CRL or OCSP responder for Notary certificates.

4.7 Audit & Monitoring

- **Logging:** All certificate issuance, renewal, and revocation events logged to SIEM with 1-year retention.
- **Periodic Review:**
    - Quarterly audit of PKI registry for expired or soon-to-expire certificates.
    - Annual compliance check against Arizona RON certificate requirements.

4.8 Incident Response

- In the event of a certificate breach (e.g., private key compromise):
    1. Activate Incident Response Plan.
    2. Revoke affected certificates immediately.
    3. Issue new certificates and enforce re-authentication for Notaries.
    4. Conduct root-cause analysis and update controls.

5. Exceptions

- Any exception (e.g., extended validity for legacy code-signing certs) must be:
    1. Documented with risk assessment
    2. Approved by the CISO
    3. Reviewed within 90 days

6. Enforcement & Sanctions

- Non-compliance may result in loss of signing privileges, disciplinary action, or commission suspension.
- Security Team performs enforcement audits semi-annually.

7. Review & Updates

- Reviewed annually or upon:
    - Changes in Arizona RON statute (§ 2-12-1307)
    - PKI security incidents
    - New industry best practices or cryptographic standards

End of TeleSeal Certificate Management Policy