Silac Certificate Management Documentation

For Platform, Security, and Infrastructure Teams

1. Objectives

- Maintain a single source of truth for all on-prem SSL/TLS and client certificates.
- Ensure no expired certificate outages via monitoring and proactive renewals.
- Clarify ownership between Platform, Infrastructure, and Security teams.
- Document PKI, issuance, renewal, and incident response procedures.

2. Roles and Responsibilities (RACI)

Function	Primary	Support	Notes
PKI Infrastructure & Policy	Security	Infrastructure	Manage Root/Sub CAs, CRL, and policy.
Certificate Request & Issuance	Platform	Security	Handle requests through SubCA or DigiCert.
Installation / Binding	Server / App Teams	Platform	Bind certificates on IIS, Nginx, NSX LB.
Expiry Monitoring & Alerts	DevSecOps	App Owners	Nagios and weekly report review.
Client Certificate Management	Security	App Owners	mTLS enrollment, mapping, and revocation.
Incident Response	Platform	Security + App Teams	Follow documented runbook.

3. Standard Operating Procedures (SOPs)

A. New Certificate (Server or Load Balancer)
1. Submit request with hostname(s), SANs, environment, and contact info.
2. Generate CSR (via MMC, OpenSSL, or certreq).
3. Submit CSR to Silacins-SubCA (internal) or DigiCert (external).
4. Receive certificate and store securely.
5. Install/bind to server or LB and validate.
6. Update inventory and enable monitoring.

B. Renewal (60–30 days before expiry)
- Renew using same CSR or new keypair per policy.
- Validate bindings and replace old certs.
- Update inventory and renewal calendar.

C. Revocation / Compromise
- Replace certificate immediately.
- Revoke in CA (SubCA or DigiCert).
- Purge old certs from systems.
- Document incident response.

D. Emergency (Expired Cert)
- Generate emergency certificate from SubCA.
- Replace and restore service immediately.
- Complete RCA and full replacement within 72 hours.

4. Monitoring and Reporting

Monitoring ensures proactive alerting for upcoming expirations.

Nagios Example: `check_http -H portal.silacins.com -p 443 -S -C 30,7`
PowerShell:
``` Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.NotAfter -lt (Get-Date).AddDays(60) } ```
Linux Bash Check:
``` for c in /etc/ssl/certs/*.pem; do end=$(openssl x509 -enddate -noout -in "$c" | cut -d= -f2) echo "$(basename "$c"),$end" done ```

Weekly reports are generated automatically by PowerShell script and emailed to the Platform and Security teams.

5. PKI Overview

Component	Description	Owner
Root CA	Silacins Root CA (offline)	Security
Subordinate CA	Silacins-SubCA (AD CS)	Security
External CA	DigiCert public CA	Security
CRL / OCSP	On-prem CRL/OCSP servers	Security
PKI Server	pki01.silacins.local	Infrastructure
Key Protection	HSM or secured store	Platform

6. Reporting and Automation

The automated PowerShell job `Send-CertExpiryReport.ps1` runs weekly to identify certificates expiring within 60 days and emails results to Platform and Security teams.

Steps:
1. Reads data from *Silac_Certificate_Management_Tracker.xlsx*
2. Generates HTML table of expiring certificates
3. Emails report via SMTP to preconfigured contacts
4. Logs sent reports to `\\share\\Security\\Reports`

Task Scheduler: runs every Monday at 8:00 AM under service account with Excel and SMTP access.

7. Governance and Review

- Evidence: Excel inventory, renewal tickets, monitoring logs.
- Reviews: Quarterly inventory review; annual PKI audit.
- Compliance: SOC-2 / NIST-aligned key lifecycle management.
- Change Control: All rotations follow standard CAB process unless emergency.

Prepared for Silac Platform, Infrastructure, and Security Teams.