Certificate Management (Silac — On-Prem)

Audience: Platform, Infrastructure, Security, and App teams
Scope: Public and internal SSL/TLS and client certificates issued by **Silacins-SubCA** and **DigiCert**; on-prem workloads (IIS, Nginx, load balancers, NSX, CI/CD, monitoring, etc.).

---

1) Objectives

- Maintain a **single source of truth** for all certificates.
- Ensure **no expired cert outages** via monitoring and early renewals.
- Clarify **ownership**: who requests, approves, installs, and monitors.
- Document **PKI** components and operational procedures (issuance, renewal, revocation, incident response).

---

2) Quick Links

- **Inventory workbook:** `\\share\security\Silac_Certificate_Management_Tracker.xlsx` (Sheets: *Certificate Inventory*, *PKI Overview*, *Responsibility Matrix*, *Renewal Calendar*)
- **Ticket type:** “Certificate – Request/Renewal/Install”
- **Escalation channel:** `#platform-oncall` / Ops phone tree

---

3) Roles & Responsibilities (RACI)

Function	Primary	Support	Notes

PKI infrastructure & policy (Root, SubCA, CRL/OCSP)	**Security**	Infrastructure	AD CS policy, CA backups, CRL publishing
Certificate request & issuance	**Platform**	Security	Requests via Silacins-SubCA or DigiCert
Installation/binding on servers & LBs	**Server/App Owners**	Platform	IIS bindings, Nginx, NSX LB, F5, etc.
Expiry monitoring & alerts	**DevSecOps/Platform**	App Owners	Nagios checks, weekly report
Client certs / mTLS	**Security**	App Owners	Enrollment, mapping, revocation
Incident response (expired/compromised)	**Platform**	Security + App Owners	Runbook below

---

4) Inventory Standards

Required fields

- Certificate Name
- Environment (Prod, Dev, Corp, Pre-Prod, Internal)
- Type (SSL/TLS, Client)
- Issuer (Silacins-SubCA or DigiCert CA name)
- Valid From / **Valid Until** / **Days to Expire** (auto)
- **Used On / Associated System** (e.g., IIS Portal, NSX LB, Grafana)
- Key Algorithm (RSA 2048/4096, ECC P-256)
- Certificate Path/Location (e.g., `C:\CertStore\*.pfx`, LB object name)
- Linked Domains (CN + SANs)
- Application/Service Owner

- Owning Team + **Technical Contact**
- Renewal Method (SubCA web enrollment, DigiCert portal)
- Monitoring Configured (Yes/No), Tool, Alert Channel
- Status and Notes/Actions

Updating the workbook (weekly)

1. Open **Certificate Inventory** tab.
2. For new or changed certs, populate required columns.
3. Ensure “**Used On / Associated System**” is set (use the dropdown and adjust if needed).
4. Confirm **Days to Expire** calculates and appears on **Renewal Calendar**.
5. Commit changes and notify `#platform-oncall` if anything <60 days.

---

5) Certificate Catalog (current highlights)

Keep this table in Confluence as a quick view; full details live in the Excel workbook.

Certificate	Environment	Used On / Associated System	Issuer
`portal.silacins.com`	Prod	Web Portal / IIS Frontend	DigiCert
`privacy.silacins.com`	Prod	Public Privacy Site	DigiCert
`sentry.silacins.com`	Prod	Sentry Monitoring	DigiCert
`secure.silacins.com`	Prod	Auth Gateway / Reverse Proxy	DigiCert
`api01.silacins.com`	Prod	API Gateway / LB	DigiCert
`media.silacins.com`	Prod	Media/File Delivery	DigiCert
`upload.silacins.com`	Prod	Upload Service	DigiCert

`kibana.silacins.com`	Corp	Kibana UI	Silacins-Sub CA
`NSX-LB00.silacins.com`	Prod	VMware NSX Load Balancer	Silacins-Sub CA
`prometheus.silacins.com`	Corp	Prometheus	Silacins-Sub CA
`grafana.silacins.com`	Corp	Grafana	Silacins-Sub CA
`alertmanager.silacins.com`	Corp	Alertmanager	Silacins-Sub CA
`apps-corp.silacins.com`	Corp	Corporate Apps Portal	Silacins-Sub CA
`windapi.silacins.com`	Prod	Windows API App	Silacins-Sub CA
`tableau.silacins.com`	Corp	Tableau	Silacins-Sub CA
`teamcity-artifacts.silacins.com`	Dev	TeamCity Artifacts	Silacins-Sub CA
`extstream.silacins.com`	Prod	External Streaming Gateway	Silacins-Sub CA
`apps-prod.silacins.com`	Prod	Production App Platform	Silacins-Sub CA
`flower.silacins.com`	Prod	Celery/Flower	Silacins-Sub CA
`syslog.silacins.com`	Corp	Syslog/Logging	Silacins-Sub CA
`apps-pre-prod.silacins.com`	Pre-Prod	Pre-Prod Apps	Silacins-Sub CA
`concourse.silacins.com`	Dev	Concourse CI	Silacins-Sub CA
`design-library.silacins.com`	Corp	UI Component Library	Silacins-Sub CA
`intake.silacins.com`	Corp	Intake Portal	Silacins-Sub CA

`agent-rewards.silacins.com`	Corp	Agent Rewards Portal	Silacins-Sub CA
`apps-dev.silacins.com`	Dev	Dev App Platform	Silacins-Sub CA
`sonarqube.silacins.com`	Dev	SonarQube	Silacins-Sub CA
`teamcity.silacins.com`	Dev	TeamCity CI	Silacins-Sub CA
`cicd-dashboard.silacins.com`	Dev	CI/CD Dashboard	Silacins-Sub CA
`apps-ste.silacins.com`	STE	Staging/Test Apps	Silacins-Sub CA
`nsx-lb00.silacins.com`	Corp	NSX LB Secondary	Silacins-Sub CA
`admin.silacins.com`	Corp	Admin Console	Silacins-Sub CA

Add/remove rows as your list grows; keep the Excel as the canonical record.

---

6) Standard Operating Procedures (SOPs)

A. New Certificate (server or LB)

1. **Create ticket** (type “Certificate – Request”). Include hostname(s), environment, owner, contact, key type/size, SANs, usage (IIS/Nginx/LB), and path target.
2. **CSR generation**
   - **Windows/IIS:** use MMC Certificates or `New-SelfSignedCertificate` + `certreq` CSR.
   - **Linux/Nginx:** `openssl req -new -newkey rsa:2048 -nodes -keyout host.key -out host.csr`
3. **Issuance**
   - **Internal:** submit CSR to **Silacins-SubCA** (AD CS web enrollment).

  - **External:** submit CSR in **DigiCert** portal.

4. **Receive cert** (and chain), **store securely** (`.pfx` if needed), and record in **Inventory**.
5. **Install & bind** (IIS site, Nginx, NSX LB virtual server, etc.).
6. **Verify**:
   - Browser padlock, chain validity, protocol suite.
   - CLI: `openssl s_client -connect host:443 -servername host -showcerts`.
7. **Document**: update Excel (path, owner, monitoring) + attach to the ticket.
8. **Monitor**: ensure Nagios check is enabled (see Monitoring below).

B. Renewal (60–30 days before expiry)

1. Inventory shows **<90 days** → auto-create renewal ticket.
2. Re-use existing CSR + key if policy allows, or **generate new keypair** (preferred for public certs).
3. Issue via **Silacins-SubCA** or **DigiCert**; maintain same SAN set unless change is requested.
4. Stage on **secondary node** or off-hours.
5. Rotate/bind → validate → remove old bindings.
6. Update **Inventory** (Valid Until, Renewal Date, Path, Status).
7. Close with screenshot/CLI proof.

C. Revocation / Compromise

1. Pull traffic (maintenance or LB drain) and **replace immediately** with a new cert/key.
2. **Revoke** in Silacins-SubCA or DigiCert; publish CRL/OCSP.
3. Audit where the old cert was installed and purge artifacts.
4. File an incident report (root cause, blast radius, corrective actions).

D. Emergency: Expired Certificate

1. Triage: identify impacted FQDN(s), app owners, and LB/node scope.
2. Issue a **short-term emergency cert** (same SANs) from SubCA or DigiCert.
3. Bind, verify, restore service.
4. Replace with long-term cert/rooted process within 72 hours.
5. Update inventory + post-incident RCA.

---

7) Monitoring & Reporting

Targets

- Alerts at **90/60/30/7 days** before expiry.
- Weekly **Renewal Calendar** review (from Excel).

Nagios examples

- TLS expiry (remote):
  `check_http -H portal.silacins.com -p 443 -S -C 30,7`
  (Warn at 30 days, critical at 7)
- HTTPs chain/host:
  `check_ssl_cert -H grafana.silacins.com -c 30 -w 60`

Windows local store (scheduled task) – PowerShell snippet

```
Get-ChildItem Cert:\LocalMachine\My |
  Where-Object { $_.NotAfter -lt (Get-Date).AddDays(60) } |
  Select-Object Subject, NotAfter, Thumbprint |
  Export-Csv "C:\Temp\certs_expiring_60d.csv" -NoTypeInformation
```

Linux PEM path check

```
for c in /etc/ssl/certs/*.pem; do
  end=$(openssl x509 -enddate -noout -in "$c" | cut -d= -f2)
  echo "$(basename "$c"),$end"
done
```

Reporting

- Excel's **Renewal Calendar** tab + chart shared to Confluence weekly.
- App owners tagged on anything <60 days.

---

8) 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 endpoints	Security
PKI Server(s)	`pki01.silacins.local` (AD CS)	Infrastructure
Key Protection	HSM/Key vault for private keys	Platform
Backup/DR	Nightly backup, quarterly restore test	Platform

---

9) Naming, Key & Policy Standards

- **Naming:** `host.domain.tld-YYYY-MM` (matches your current convention)
- **Validity:**
  - Public (DigiCert): 12–13 months max
  - Internal (SubCA): 12–24 months per policy
- **Keys:** RSA 2048 minimum; prefer RSA 3072/4096 or ECC P-256 where supported
- **SANs:** Only required hostnames; avoid wildcards unless justified and approved
- **Storage:** Keys and PFX protected; no keys in repos or tickets

- **Change Management:** Cert rotations follow normal change window unless emergency

---

10) Request Templates

New/Change Request (paste into ticket)

- Hostname(s)/SANs:
- Environment:
- Use (IIS/Nginx/NSX LB/Other):
- Key Algorithm: RSA 2048 / RSA 4096 / ECC P-256
- Owner & Contact:
- Required by date:
- Notes/Dependencies:

Post-Install Validation Checklist

- Chain trusted (browser/`openssl s_client`)
- Correct CN/SANs
- Old cert removed from binding
- Inventory updated
- Monitoring enabled

---

11) Governance & Audit

- **Evidence:** tickets, Excel inventory, Nagios alert history, renewal emails
- **Reviews:** quarterly inventory review; annual PKI policy review

- **Compliance:** aligns with SOC-2/NIST control families for key management and change control

---

12) Change Log

Keep a simple table in Confluence with date, change, and owner (e.g., “Added Grafana cert renewal SOP – 2025-10-24 – Platform”).

🧾 Weekly Certificate Expiration Report

Last updated: {{date}}

Certificate	Environment	Owner	Valid Until	Days to Expire	Status
`portal.silacins.com`	Prod	Platform	2025-04-12	158	🟢 Active
`secureapi.silacins.com`	Prod	Platform	2025-02-15	102	🟠 90-day Window
`intranet.silacins.local`	Internal	Infrastructure	2026-06-01	565	🟢 Long-term
`grafana.silacins.com`	Corp	DevSecOps	2025-11-25	20	🔴 Expiring Soon

`kibana.silacins.com`	Corp	DevSecOps	2025-11-25	20	🔴 Expiring Soon
`apps-prod.silacins.com`	Prod	Platform	2027-06-07	605	🟢 Active

Summary:

- 🟢 15 certificates active (>90 days)
- 🟠 2 certificates within 90 days
- 🔴 3 certificates expiring within 30 days
- No expired certs detected

Next Actions:

- Renew `grafana.silacins.com` and `kibana.silacins.com` before Nov 25, 2025.
- Confirm new DigiCert replacements in ADCS store and update Excel inventory.

💡 **Tip:**
You can use Excel's `Renewal Calendar` tab → *File* → *Export* → *CSV* → paste values into this Markdown table each Monday morning.