Expired certificates aren't bad luck – they're a process failure

Monday morning, 08:30.

A critical application fails to start. Monitoring systems show alerts everywhere - yet at first glance the infrastructure looks fine. After about 40 minutes of intensive log analysis, the root cause is finally identified: a TLS certificate has expired.

The real problem in these situations isn't that certificates expire - it's that nobody on the team knows exactly who owns the certificate, where the private key is stored, or why it doesn't **appear** in any inventory.

Does this sound familiar? **Our experience shows this isn't a technical issue - it's a process issue.**

In a world with hybrid clouds, microservices, and thousands of machine identities, Certificate Lifecycle Management (CLM) is no longer a niche topic. It has become a critical operational function - not a technical detail to be remembered once a year..

TL;DR – What you'll find in this article

If you're short on time right now, feel free to save this article for later. It covers:

- a **five-building-block framework** for effective Certificate Lifecycle Management (CLM)
- common **warning signs** that indicate a high risk of outages
- a **90-day playbook**, from inventory to a stable, repeatable process
- a **responsibility matrix (RACI)** that clarifies roles and ownership
- a **checklist** to help you realistically assess your environment

Why you shoud address this now

Not long ago, certificate management was manageable: a handful of domains, one provider, renewals every two years. Today, IT reality is very different:

1. **Certificate volume explosion:** Containers, APIs, IoT, multi-cloud - each environment requires its own identities**.**
2. **Shorter validity periods:** Security standards force more frequent rotations, and manual processes no longer scale.
3. **Increasing compliance pressure:** In regulated environments, audits don't just check whether you use certificates - they evaluate how you manage renewals.

The question is not whether a certificate will expire - it will. The key question is: **Do you find out in time? And does your organization have a process that enables renewal without chaos?**

Typicel indicators of organizational chaos

Before we discuss solutions, check whether any of these scenarios are familiar:

- **Incomplete inventory:** "We don't know exactly how many certificates we have or where they are used."
- **Excel as the "central system":** Renewals are tracked in spreadsheets or emails that often reference former employees.
- **Unclear ownership:** The infrastructure team points to security, and security points to application teams.
- **Last-minute incidents:** The process only begins once users already see "Connection not secure" warnings and cannot access the application.

Remember: Automation without clearly defined responsibilities is a reliable recipe for chaos.

5 elements of effective CLM

To prevent certificate management from becoming a constant firefight, a stable framework is necessary. At Bacher Systems, we work with five core components:

1. **Inventory & Discovery:** You can only protect what you know exists. Continuous discovery of all certificates - both public and internal - is the first step.
2. **Ownership:** Every certificate needs a clearly defined owner. Shared responsibility almost always leads to outages.
3. **Policy & Governance:** Clear rules create reliability. Which CAs are permitted? What key lengths are acceptable? The goal is a minimum viable policy - concise, understandable, and enforceable.
4. **Renewal & Rotation:** Dashboards show certificate status and risk, moving from reactive firefighting to proactive operations.

Implementation plan: your 90-day playbook

Days 0-30: Inventory (Visibility)

- Perform a complete discovery scan and build a comprehensive inventory
- Classify criticality (what could stop the business?)
- Set up immediate alerts at 30/60/90 days before expiration

Days 31-60: Define rules and minimize risk (Governance)

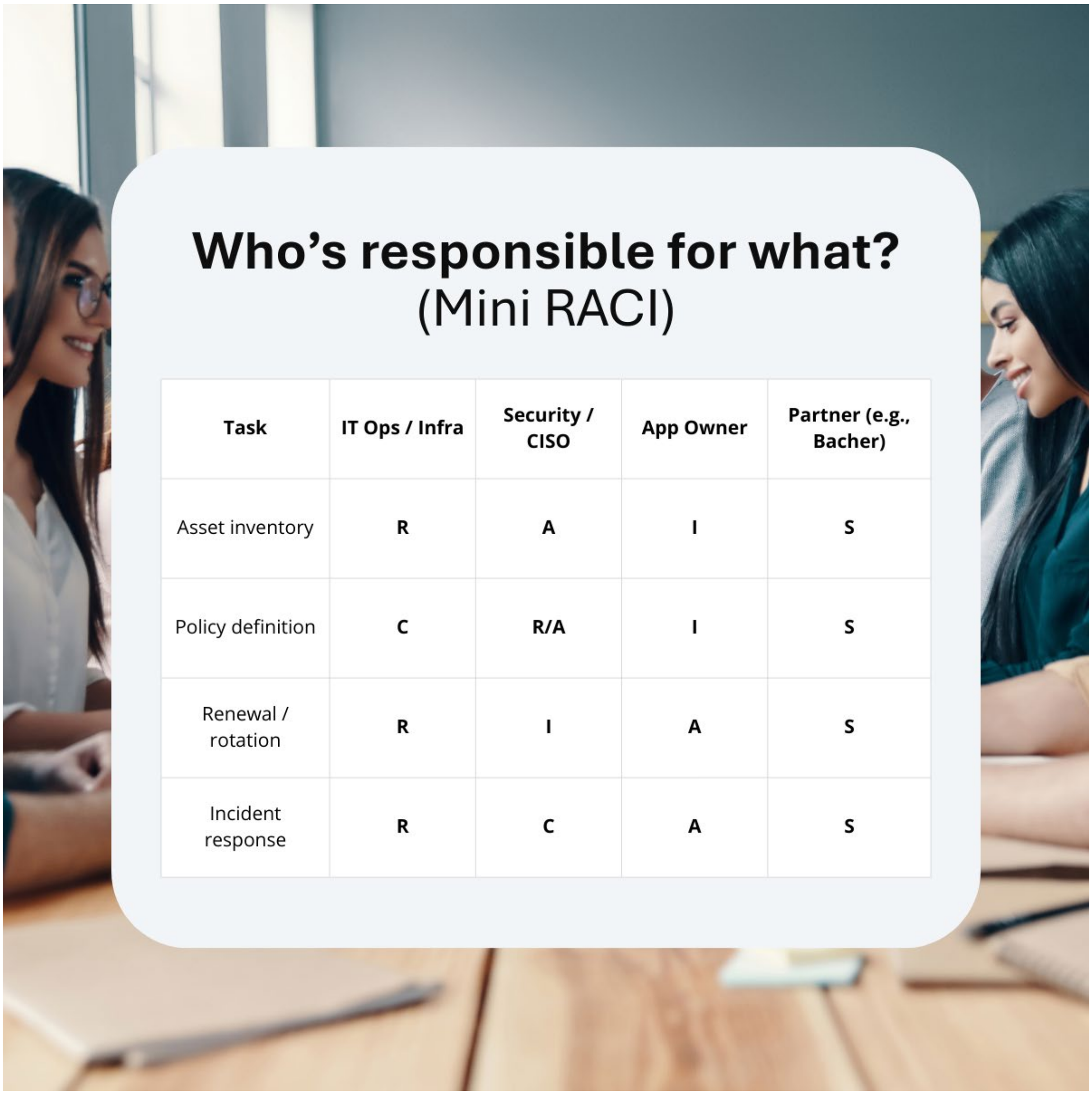
- Create a simple policy and technical standards
- Establish a process for certificate requests and renewals
- Identify owners for the 20 most critical services

Days 61-90: From project to process (Operations)

- Implement automation in the most stable and predictable areas
- Build KPI dashboards for management and security
- Develop runbooks — step-by-step procedures for renewal failures

Who is responsible for what? (Mini RACI)

The biggest challenge in CLM isn't the tools - it's the people. Establishing a clear RACI (Responsible, Accountable, Consulted, Informed) model helps eliminate ambiguity and ensures the right teams are accountable for CLM outcomes:



Who's responsible for what?
(Mini RACI)

Task	IT Ops / Infra	Security / CISO	App Owner	Partner (e.g., Bacher)
Asset inventory	R	A	I	S
Policy definition	C	R/A	I	S
Renewal / rotation	R	I	A	S
Incident response	R	C	A	S

Case study: From outages to operational resilience

In an organization we worked with, certificate renewal typically took five workdays and involved four people. Emails, tickets, and manual key copying made the process error-prone - and one forgotten certificate nearly brought down the entire payment system.

After implementing a complete CLM cycle, effort dropped to minutes and visibility reached 100%.

Our approach at Bacher Systems: the Adoption Cycle

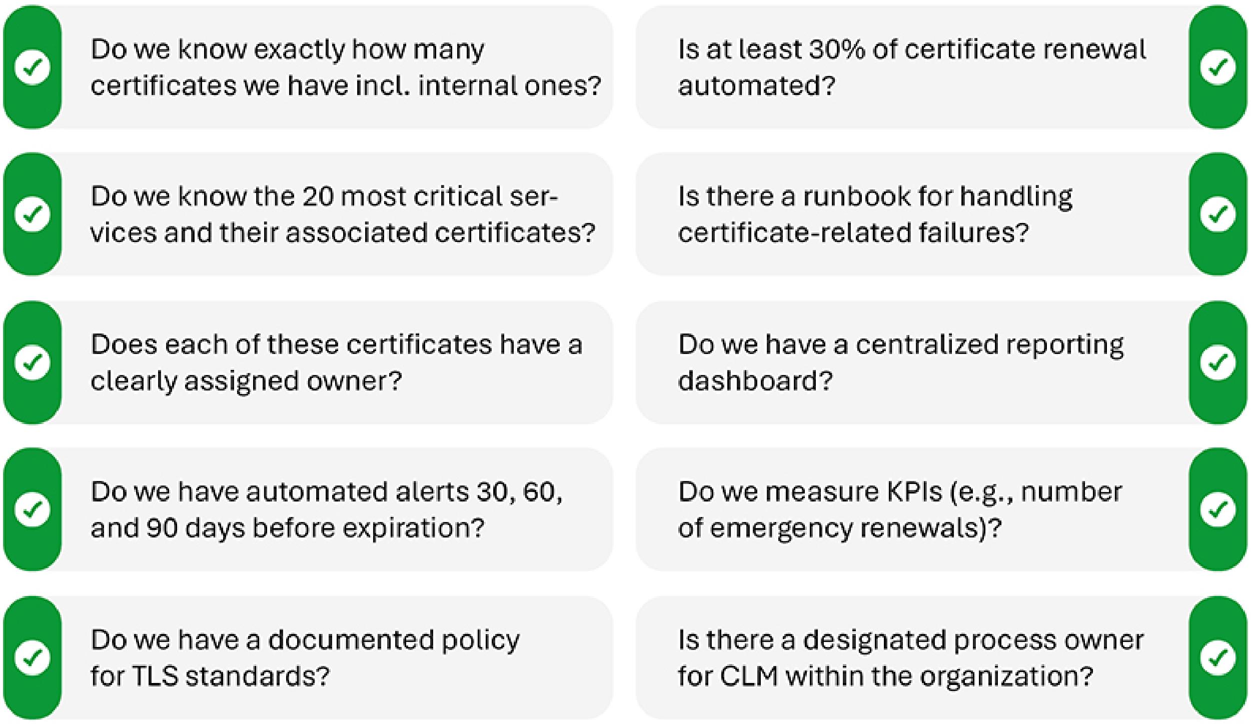
Certificate management is not a one-off tool deployment - it is continuous operational work. Our **Adoption Cycle model** includes:

- **Consulting:** Analyze current state and gaps.
- **Implementierung:** Select appropriate tools and design processes.
- **Operations:** Support day-to-day operations, updates, and patching.
- **Optimization:** Ongoing reduction of exceptions and increased automation.

We take responsibility for the outcome - not just the technology.

Checklist: Is your CLM under control?

Ask yourself and your team these ten questions:



- ✓ Do we know exactly how many certificates we have incl. internal ones?
- ✓ Do we know the 20 most critical services and their associated certificates?
- ✓ Does each of these certificates have a clearly assigned owner?
- ✓ Do we have automated alerts 30, 60, and 90 days before expiration?
- ✓ Do we have a documented policy for TLS standards?
- Is at least 30% of certificate renewal automated? ✓
- Is there a runbook for handling certificate-related failures? ✓
- Do we have a centralized reporting dashboard? ✓
- Do we measure KPIs (e.g., number of emergency renewals)? ✓
- Is there a designated process owner for CLM within the organization? ✓

If you answered “no” to many of these questions, now is the right time to bring structure to your process - before the next outage catches you off guard

What’s next?

What is currently your biggest challenge - lack of visibility, unclear ownership, or hurdles in automation?

Ready to get started? Feel free to contact us using the keyword **“CLM”**, and we will be happy to discuss how we can sustainably safeguard your process together.

Alexander Cornea

Business Owner Digital Identities

identity@bacher.at
+43 664 60126 - 376

We live accountability!

Bacher Systems EDV GmbH
Wienerbergstr. 11/B9 – 1100 Vienna
info@bacher.at | Tel: +43 1 60 126-0 | www.bacher.eu