aet europe

E-BOOK · CERTIFICATE LIFECYCLE MANAGEMENT

Are you absolutely certain you know which public certificate will expire next?

A calm, practical guide to understanding your CLM readiness, before shorter certificate lifecycles become daily work.

Public certificate lifecycles are moving from long renewal windows toward much shorter cycles. This guide helps you understand whether your organization is ready. Simply, clearly and without unnecessary complexity.

◆ trust accelerates growth ◆

Get in touch

Most CIOs answer "yes." Most IT teams answer "I'm not sure."

That difference is where certificate uncertainty begins.

For years, public certificates could be managed quietly in the background. A spreadsheet here. A mailbox reminder there. A colleague who knew where everything was. A supplier who handled part of the process.

And for a long time, that was enough.

But public certificate lifecycles are becoming shorter. Public TLS validity is moving toward **47 days**, making manual renewals increasingly difficult to sustain.

That does not mean organizations need to panic. It means they need **clarity**.

Because when renewal windows become shorter, the most important question is not:

Can we renew certificates?

The real question is:

Do we know exactly what needs attention next?

That is what this e-book helps you explore. And if you are not completely certain today, that is exactly why a **CLM Readiness Assessment** is a valuable first step.

Digital trust should feel simple, even when the technology behind it is not

Public certificates are easy to overlook. They do not ask for attention when everything works. They do not appear in daily management meetings. They rarely sit at the top of a CIO dashboard.

Yet they quietly support many of the digital services your organization depends on:

- Websites
- Customer portals
- APIs
- Identity services
- Cloud applications
- Partner connections
- Secure communication

When public certificates are well managed, nobody notices. **That is exactly how it should be.**

But when certificates are not visible, not owned or not renewed in time, they can create unwanted disruption. Not because your teams are careless. Not because your organization is behind. But because certificate management has quietly become more frequent, more distributed and more dependent on accurate information.

What is CLM? Certificate Lifecycle Management is managing the complete lifecycle of TLS/SSL certificates across an organization's infrastructure, from request and issuance to renewal and replacement.

The goal is not to make certificates more important. The goal is to make certificate management **simpler, more predictable and easier to trust**.

What changes when certificate lifecycles become much shorter?

When certificates were valid for longer periods, many organizations could manage renewals as occasional work. A reminder arrived. Someone renewed the certificate. The service continued.

That rhythm is changing.

As public certificate lifecycles shorten, organizations face more renewal moments, more checks, more handovers, and more opportunities for uncertainty. Public TLS validity is set to drop to **47 days by 2029**, a pace at which manual renewals become unsustainable.

398	200 → 100	47
DAYS TODAY	STEPPING DOWN	DAYS BY 2029

This does not necessarily require a complex response. It requires a **better overview**. Your organization should be able to answer, calmly and confidently:

- Which public certificate expires next?
- Who owns it?
- Which service depends on it?
- Which Certificate Authority issued it?
- What action is required?
- Who will make sure that action happens?

If these questions are difficult to answer, the problem may not be the certificate. **The problem may be the process around it.**

Can your organization answer these questions today?

Use the questions below as a first, honest readiness check. You do not need perfect answers.
You only need to know **where certainty ends and assumptions begin**.

1 Visibility

Can your team quickly provide a complete overview of all public certificates?

- [ ] Yes, centrally and confidently
- [ ] Partly, but not fully
- [ ] No, this requires manual checking

2 Ownership

Does every public certificate have a clear owner?

- [ ] Yes, ownership is documented and current
- [ ] Partly, but some ownership is unclear
- [ ] No, ownership depends on individual knowledge

3 Next expiry

Do you know which certificate will expire next?

- [ ] Yes, immediately
- [ ] Possibly, after checking several sources
- [ ] No, not with certainty

4 Systems and impact

Do you know which systems depend on every public certificate?

- [ ] Yes, this is documented
- [ ] Partly, for critical systems only
- [ ] No, this is not consistently visible

Where does certainty end and assumption begin?

5 Certificate Authorities

Do you know which CAs are used across your organization?

- ☐ Yes, centrally visible
- ☐ Partly, but not complete
- ☐ No, this is fragmented

6 Renewal process

Is renewal handled through a structured lifecycle process?

- ☐ Yes
- ☐ Partly
- ☐ Mostly through reminders, mailboxes or spreadsheets

7 Reporting

Can management quickly understand upcoming certificate risks?

- ☐ Yes
- ☐ Partly
- ☐ No, reporting takes manual effort

Selected "partly" or "no" more than once? That does not mean something is wrong. It means there is room to create more certainty, and that is exactly what a CLM Readiness Assessment is designed to clarify.

Most certificate uncertainty grows quietly

Certificate uncertainty usually does not appear all at once. It grows slowly.

A project starts. A certificate is requested. A system goes live. A supplier manages part of the service. A colleague changes role. Documentation becomes outdated. A renewal reminder goes to an old mailbox.

Everything still works. Until one day, someone asks:

Who owns this certificate?

And nobody is completely sure.

That moment is not a failure. It is a sign that the process has become too dependent on people remembering the right details at the right time. For organizations that want reliability, calm operations and predictable digital trust, that is not ideal.

The better approach is simple:

- Make certificates visible
- Make ownership clear
- Make next actions easy to see
- Make reporting available
- Make the process less dependent on memory

The ideal CLM experience works exactly this way: an operator sees deployments, statuses and assets from different CAs, and whether action is needed, user-friendly enough to act **without deep PKI knowledge**.

That is the kind of simplicity that gives teams confidence.

Your certificate landscape may be more spread out than you think

Many organizations do not manage public certificates from one single place. Certificates may come from different Certificate Authorities because of:

- Different departments
- Historical choices
- Suppliers
- Cloud applications
- Acquisitions
- Projects
- External service providers

In practice, organizations rarely standardize on a single CA, which means certificate management needs to work with the CAs you **actually use**.

This creates a practical challenge. Not a dramatic one. A practical one. Different CAs can mean:

- Different portals
- Different renewal messages
- Different contacts
- Different ownership
- Different reporting
- Different levels of visibility

The result is often a certificate landscape that still functions, **but is not easy to oversee**.

That is where doubt enters. And doubt is exactly what this e-book is meant to help remove.

CLM readiness is not about having more technology. It is about having less uncertainty.

A ready organization does not necessarily have the largest security team or the most complex tooling. **A ready organization has clarity.** It knows:

- What public certificates exist
- Where certificates are used
- Who owns them
- Which certificates need attention next
- Which CAs are involved
- Which services are most important
- What management should know

Good CLM readiness feels calm. It feels simple. It feels controlled.

It means IT teams do not need to search through old emails when a renewal deadline approaches. It means CIOs and CISOs can answer questions with confidence. It means the organization is not dependent on one person's memory.

And it means certificate management becomes a **manageable routine** instead of a last-minute concern.

That is the purpose of a CLM Readiness Assessment. Not to point out what is wrong, but to show what can be made clearer.

Five signs your organization may benefit from a CLM Readiness Assessment

SIGN 1

You need several sources to understand your certificate landscape

If your team needs different spreadsheets, portals, suppliers or inboxes to understand what certificates exist, visibility may be incomplete. An assessment identifies where the overview is strong and where it can be improved.

SIGN 2

Ownership is not always clear

If some certificates are linked to former employees, old projects or external suppliers, ownership can become unclear. An assessment reveals where responsibility should be made more explicit.

SIGN 3

You are not fully certain which certificate expires next

This is often the most powerful question. If the answer is not immediately clear, the organization may be relying on fragmented information.

SIGN 4

Reporting takes effort

If management reporting requires manual collection, checking and interpretation, the process may not yet be mature enough for shorter certificate lifecycles.

SIGN 5

Renewal still depends on reminders and individual follow-up

Reminders are useful. But reminders are not the same as lifecycle management. An assessment determines whether renewals are managed as individual events, or as a controlled process.

The real outcome is peace of mind

Certificate Lifecycle Management may sound technical. But the real value is very human.

- It gives people confidence that important digital services are being looked after
- It helps IT teams work more calmly
- It helps management make better decisions
- It reduces dependency on individual knowledge
- It prevents avoidable surprises

And it supports a simple belief:

Digital trust should not feel fragile. It should feel reliable. Manageable. Under control.

That is why this e-book does not ask whether your organization is "bad" at certificate management. It asks something much more useful:

How certain are you?

Because certainty is measurable. And once it is measured, **it can be improved**.

A practical first step, not a heavy project

A CLM Readiness Assessment should feel accessible. It is not meant to overwhelm your team, it is designed to create a clear first picture of your current certificate management maturity.

During the assessment, the focus is on six practical areas:

1
Visibility
What can you currently see?

2
Ownership
Who is responsible for what?

3
Renewal process
How are upcoming expirations managed?

4
Multi-CA complexity
Which Certificate Authorities are involved?

5
Reporting
Can risks and upcoming actions be explained clearly?

6
Shorter lifecycles
Will the current approach still work when renewal frequency increases?

The outcome is not a technical audit full of complexity. The outcome is a **clear overview** of where your organization stands today, and what can be improved next.

Your CLM Readiness Assessment gives you clarity

After the assessment, your organization receives a practical overview that supports both IT and management conversations.

You receive:

- A current-state overview
- A certificate lifecycle maturity indication
- Visibility gaps
- Ownership findings
- Renewal process observations
- Multi-CA considerations
- Practical improvement opportunities
- A recommended next-step roadmap

The value is simple. You know where you stand. You know where uncertainty exists. You know what to improve first. And you can move forward calmly, with better information.

The final question

Are you absolutely certain you know which public certificate will expire next?

If the answer is **yes**, that is good.
If the answer is **"probably"**, there may be room for improvement.
If the answer is **"we would need to check"**, this is the right moment to create more clarity.

As lifecycles become shorter, the organizations that feel most prepared will not be the ones with the most complicated processes. They will be the ones with the clearest overview, the clearest ownership, the clearest next actions, and the least dependency on assumptions.

Certificate management should not create stress. It should create confidence.

READY TO FIND OUT?

Find out whether your organization is ready for shorter public certificate lifecycles

Renewals are becoming more frequent. Certificate landscapes are becoming more distributed. Manual processes are becoming harder to rely on. But the answer does not need to be complicated.

Start with clarity. Start with a structured assessment. Start by finding out whether your organization is already in control, or whether hidden uncertainty exists.

Get in touch

A simple first step toward more certainty, less manual effort and better control over public certificates.

aet europe

Because digital trust should be simple, convenient and reliable, even when certificate lifecycles become shorter.

◆ trust accelerates growth ◆