ProofID + CYBERARK®

From certificates to AI agents: Building resilience in the machine identity age

There are two main actors on your network: humans and machines. Right now, the humans are vastly outnumbered.

We have entered the machine identity age, an era defined by the explosion of workloads, devices, bots and AI agents that drive innovation. But while we've spent decades perfecting how we authenticate people, the machines have been quietly multiplying. Now, a major shift in industry standards is forcing security teams to pay attention.

This whitepaper summarises key insights from recent discussions between CyberArk and ProofID regarding the imminent changes to certificate lifecycles and the rise of agentic AI. The takeaway is simple: manual management is dead. To build resilience, organisations must pivot to a strategy of rigorous discovery, governance and automation.

The 47-day mandate: a problem you can't solve manually

For years, managing public TLS certificates was a once-a-year exercise. This is about to change. Microsoft, Google, and Apple are pushing to reduce the lifespan of public certificates to just 47 days. This isn't a suggestion; it's a mandate, with significant reductions starting as early as March 2026.

This change means a team that rotates certificates annually will now need to do it roughly eight times a year - a 12x increase in workload. If you have 10,000 certificates, and the four-hour manual process to manage each one suddenly multiplies by twelve, spreadsheets and reminders won't cut it. Relying on humans to handle this volume isn't just inefficient; it's impossible.

When a human forgets a password, they can call the helpdesk. When a machine identity expires, business stops. Roughly 40-50% of P1 and P2 outages can be traced back to expired or mismanaged certificates, translating to lost revenue, stalled patient care, or halted transactions.

The three pillars of resilience

To survive the shift to 47-day lifecycles and secure the growing army of AI agents, you need a strategy that scales.

Continuous discovery (see it)

You can't secure what you can't see. Most organisations have a massive "shadow IT" problem, with certificates spun up by developers in cloud environments that central IT knows nothing about. Implement scanning tools that look beyond the enterprise network and into cloud environments to build definitive, centralised register of every machine identity.

Governance (control it)

Finding the identities is step one. Governing them is step two. Not every certificate is necessary. Identify which certificates are using weak encryption or belong to decommissioned systems. A central registry also builds crypto-agility, allowing you to identify where your keys are so you can swap them for quantum-safe alternatives when the time comes.

Automation (fix it)

This is the only way to beat the 47-day crunch. Zero-touch rotation reduces the four-hour manual provisioning process to a near-instantaneous background task. Automated validation also ensures that when a certificate rotates, it actually works by preventing the "rollback" outages that happen when a script breaks or a human makes a typo.

The next frontier: AI agents and bots

Certificates are the urgent "beachhead" of machine identity, but not the end of the story. We are seeing a rapid rise in agentic AI-bots that don't just chat but act. These digital agents perform high-value tasks like processing insurance claims or making bank transfers. Just like human employees, they need to be authenticated and authorised. If we don't apply the same rigor to these AI agents, we risk granting autonomous systems "admin rights and zero chill", allowing them to make unauthorised transactions or expose sensitive data.

Conclusion: Don't panic, just prepare

The machine identity landscape is exploding, but it doesn't have to be a disaster. The tools to manage this exist. The CISO's job today is to recognise that the "spreadsheet method" is a liability and to operationalise a machine identity strategy before the 47-day clock runs out.

Actionable next steps

1. **Run a discovery scan now:** Stop guessing. Engage a partner to run a scan of your environment. You need to know if you have 2,000 certificates or 20,000.

2. **Triage and govern:** Identify the high-risk, weak, or orphaned certificates and clean house.

3. **Automate the lifecycle:** Start with the most critical, high-volume certificates. Implement automation to handle issuance, renewal, and revocation.

4. **Treat machines like humans:** Apply standard IAM principles (Authentication, Authorisation, Lifecycle Management) to every bot, workload, and AI Agent.

The countdown to 47 day certificates has already started, with the first reduction in March 2026. You'll want to act before the alarms go off - which, trust us, is loud, messy, and usually comes with a side of panic emails.

Free certificate scan powered by ProofID & CyberArk

ProofID + CYBERARK®