MAINFRAME DIGITAL CERTIFICATE MANAGEMENT: SOLVING THE SYSTEM IDENTITY CRISIS

As digital certificate lifetimes drop to 47 days, automation becomes essential to maintain availability, security, and compliance. BMC AMI Digital Certificate Manager extends automated certificate lifecycle management to the mainframe, enabling standardization across the enterprise using your current CLM vendor.

Digital certificates are the connective tissue of the enterprise environment, enabling systems, workloads, applications, and APIs to verify each other and communicate securely. When a certificate fails due to expiration or error, the impact on service availability and security can be immediate and severe. And with regulators driving certificate lifetimes down to as little as 47 days by 2029, organizations face a sharp increase in both operational and compliance risk. That makes digital certificate management a top priority for BMC customers.

By enabling organizations to discover, track, and renew certificates across the infrastructure, digital certificate management prevents the outages and security gaps that can result from expired, misconfigured, or otherwise compromised certificates. This task has grown more difficult in recent years, and even greater challenges are on the horizon. But BMC has a solution.

Why digital certificate management is becoming an urgent

challenge

Traditionally, many organizations have managed mainframe certificates through manual processes centered on spreadsheets and tribal knowledge. In recent years, the growing number of system identities relying on these certificates has pushed these methods to the breaking point. Now, regulatory changes have made them completely unsustainable.

To reduce the exposure that can result from a compromised certificate, the CA/Browser Forum has announced aggressive reductions in TLS certificate lifetimes. Until this month, companies were allowed a relatively manageable 398-day renewal cycle. Now that window has been nearly cut in half to 200 days. Next March, it will shrink once again to 100 days, and by March 2029, TLS certificates will be good for only 47 days. Each of these reductions effectively multiplies the certificate management workload for mainframe security teams, and with it, the chance of manual errors, expirations, and system outages.

This isn't a future problem. The regulatory deadlines are fixed, the timelines are non-negotiable, and their impact is inevitable. That's why I'm excited to announce BMC AMI Digital Certificate Manager (DCM)—a new solution that fundamentally changes certificate management on the mainframe.

How to extend enterprise digital certificate management to the mainframe

Most enterprises already invest in Certificate Lifecycle Management (CLM) platforms for their distributed and cloud environments. These platforms haven't been able reach the mainframe, however, leaving z/OS as a manual island in an otherwise automated estate. Now BMC is filling that gap with the only solution enabling digital certificate management platforms to extend automation to the mainframe as part of a consistent enterprise strategy.

Proven in operational environments for over five years, DCM provides a unified integration layer to connect Venafi and Keyfactor digital certificate management tools to mainframe ESMs including RACF, ACF2, and Top Secret. With DCM, you can standardize on one BMC solution for your mainframe while supporting whichever certificate vendors your organization already uses, no rip-and-replace required.

End-to-end automated certificate operations

DCM extends your organization's CLM to automate the entire mainframe certificate lifecycle, from issuance and renewal to replacement and rollback. The impact is immediate and measurable:

- **Dramatic effort reduction:** Mainframe certificate implementations that previously took up to three hours of manual work are now fully automated.
- **Eliminated outage risk:** Expired or mismanaged certificates are a major cause of preventable mainframe outages. DCM's scheduled renewals and built-in rollback ensure continuous availability without late-night firefighting.
- **Reduced dependency on scarce skills:** Mainframe security expertise is increasingly hard to find. DCM removes the need for skilled personnel to manually execute certificate commands across RACF, ACF2, or Top Secret, freeing them for higher-value work.
- **Complete audit visibility:** Every action is logged with full detail, including which commands

were issued, which ESM responses were received, who authorized the change, and when.

Real-world impact at a major financial institution

One of the world's largest financial institutions evaluated DCM against its current, pre-automation state. With certificate volumes growing over 30 percent year over year, a small core team currently handles digital certificate management manually across many application owners and faces an increasing risk of outages, audit failures, and security gaps.

The firm projected the five-year value of deploying DCM as **$8.6 million**, driven by manual effort reduction and avoided headcount ($3.6M), eliminated application outages ($2.2M), compliance and audit risk reduction ($1.4M), operational efficiency gains ($0.8M), and future-proofing against accelerating certificate volumes ($0.6M). Beyond these measurable financial gains, the solution supports the institution's broader strategic priorities around operational resilience and responsible growth.

Strengthening Zero Trust across the enterprise

Machine identity is foundational to Zero Trust: Every workload, process, and system must be authenticated. Working alongside BMC AMI Security, DCM becomes part of a comprehensive Zero Trust strategy for the mainframe, enabling continuous threat detection, automated response, and end-to-end protection across your most critical environment. Security teams gain the observability, policy enforcement, and confidence they need to report to the chief information security officer (CISO) and the board that the mainframe is truly protected.

Looking ahead

The certificate landscape continues to move toward shorter lifetimes, more frequent renewals, higher volumes, and tighter regulatory scrutiny. All of these trends will drive an exponential growth in manual digital certificate management workloads. By acting now, organizations can stay ahead of increasingly urgent certificate deadlines while preparing their infrastructure for continuous, automated certificate renewals.

BMC AMI Digital Certificate Manager is generally available. We invite you to learn more about how DCM can modernize certificate management across your mainframe environment—preserving your existing tools, eliminating manual effort, and building the operational resilience your business demands.