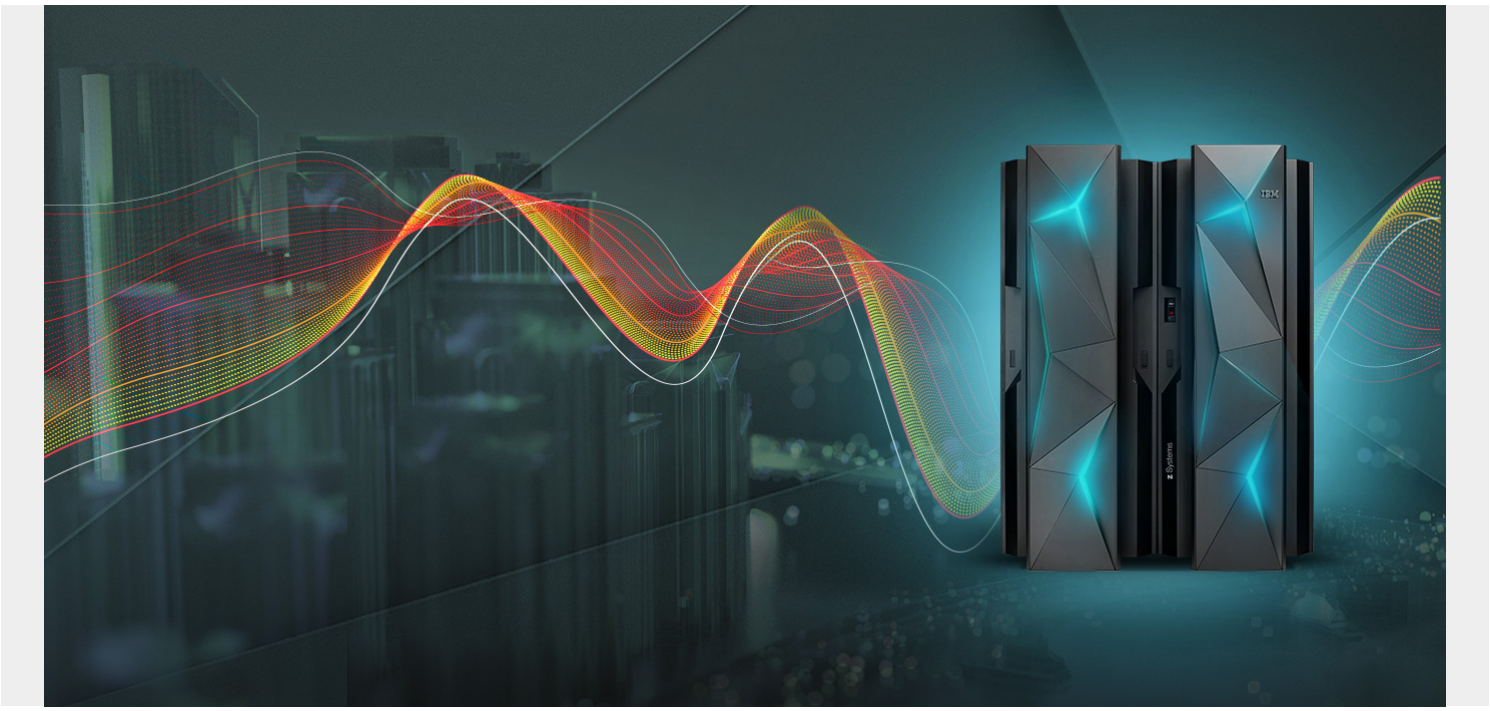
AUTOMATED CERTIFICATE MANAGEMENT ON THE MAINFRAME



Today, enterprise means everything—including the mainframe. Once upon a time, however, the cry of, "We're struggling to integrate our IBM® Z mainframe with enterprise solution X or Y," was commonplace. Indeed, “enterprise solution” could be taken to mean "enterprise solution *apart from the mainframe.*"

Times change. A new breed of BMC integrations is enabling the mainframe to benefit from those nifty enterprise solutions that it was previously difficult—or impossible—to utilize.

The secret of these integrations is to hide the complexity of the mainframe platform from the enterprise software. It can now “speak mainframe”—in other words, issue requests to the mainframe, including IBM RACF® and Top Secret®, as if it were any other server or IT platform, and without needing to understand logical partitions (LPARs), system complexes (sysplexes), multiple mainframe security databases, and so on. This approach can help solve a multitude of issues.

For example, some time ago, a BMC Mainframe Services security consultant was working onsite with a client, where someone was struggling to implement machine identity management on the mainframe. Despite playing a central role in so many organizations, machine identity management protection solutions didn’t yet extend to the platform. However, BMC was already talking to Venafi, the machine identity specialists, and our consultant suggested this person talk to their enterprise Venafi colleagues.

The reason this matters is *certificate management*. Most of us have tried to access a website and received a warning that advises caution because the site’s trust certificate has expired. In a major enterprise, there can be tens of thousands of servers and endpoints in play. As you can imagine, implementing and managing all those certificates and ensuring they have not expired, is a serious

undertaking. And if certificates aren't managed properly, you get outages because applications simply stop. Meanwhile, homegrown solutions and manual fixes may not actually ensure application availability, and could even raise potential security risks.

Enter Venafi: its Trust Protection Platform (TPP) manages the creation of certificates to enable the trust of those all-important connections. BMC's integration with Venafi brings automated certificate management and access control to the mainframe, helping you move closer to enterprise-wide Zero Trust security, support application availability, and avoid error-prone manual processes.

So how did we get to this place?

A couple of years ago, a large Venafi client in financial services wanted to extend its use of Venafi to—you guessed it—automate certificates on the mainframe, where it still had manual checks and balances in place. Three weeks before the certificate's expiration, the customer would renew it and put it in the vaults. Then, two weeks before expiration and once the application team was ready, they would swap it over at 2 AM with the help of the certificates team. The client was doing this twice a week, if not more frequently. Each time, a member of the certificates team was on call overnight and paid overtime. And all of this was risky, prone to errors and mistakes that could potentially damage the business. There had to be a better way.

Venafi did some research into, "*How do you get a Windows machine to talk to the mainframe?" and "What interfaces are there on the mainframes?"* There were no easy answers: the TPP simply wasn't designed to accommodate a mainframe requirement out-of-the-box. Then BMC Mainframe Services experts got involved.

Fast forward to 2022 and we have Venafi for IBM® z/OS®, powered by BMC. You can generate all the certificates you need, load the signed certificates, and execute enterprise security manager (ESM) commands to implement them as and when needed. Automation, control, peace of mind. This capability can also work in tandem with BMC AMI Security as part of a wider mainframe security strategy, automatically detecting and responding to threats and providing continuous protection against malicious actions and data theft. Again, all this contributes to a Zero Trust stance.

The message for mainframe shops that need machine identity management is clear: don't settle for a sub optimal "solution" that risks expired certificates and might expose the business. If you already have Venafi, integrate it. It's a faster, lower-cost, proven outcome that removes risk and avoids maintenance headaches. "But every Venafi implementation is different," you say. Indeed. Talk to your Venafi architect, connect with BMC experts, and together we can define how this valuable integration will adapt and work for you and your mainframe.

To learn more, download our Solution Brief: "BMC AMI Enterprise Connector for Venafi."