Integration of DigiCert® Trust Lifecycle Manager and CyberArk Central Credential Provider

Intelligent certificate automation with secure privileged credential management

The challenge: managing certificates without exposing privileged credentials

Organizations rely on privileged credentials to manage critical infrastructure across cloud environments, data centers, network devices, and enterprise applications. These credentials are commonly secured and governed through privileged access management (PAM) platforms like CyberArk Central Credential Provider (CCP).

At the same time, organizations must manage a rapidly growing number of digital certificates used to secure machine identities and encrypted communications. As TLS/SSL certificate lifetimes continue to shrink and organizations prepare for post-quantum cryptography (PQC), manual certificate management processes create operational risk and administrative burden.

When certificate lifecycle management and privileged credential management operate in separate systems, organizations often face:

- Delays caused by manual coordination between teams
- Duplicate credential management processes
- Increased risk of certificate expiration and service outages
- Compliance and audit challenges

Difficulty supporting automated certificate operations at scale Organizations need an automated, policy-driven approach that combines secure credential governance with enterprise certificate lifecycle automation.

The solution: automated certificate lifecycle management with dynamic credential retrieval

The CyberArk CCP integration enables DigiCert Trust Lifecycle Manager to securely retrieve privileged credentials at runtime while maintaining centralized control within CyberArk.

With this integration:

- Credentials remain securely stored and managed in CyberArk CCP
- Trust Lifecycle Manager retrieves secrets only when needed
- No passwords are stored within Trust Lifecycle Manager
- Credential rotations performed in CyberArk are automatically honored by certificate workflows
- Certificate lifecycle operations can be fully automated without exposing privileged credentials

Together, CyberArk CCP and DigiCert Trust Lifecycle Manager enable organizations to automate certificate discovery, issuance, renewal, reissuance, and deployment while maintaining strict governance over privileged accounts.

How it works

To securely establish communication with CyberArk CCP, organizations deploy at least one DigiCert sensor. For high availability, multiple sensors can be configured, allowing automatic failover if a sensor becomes unavailable.

Once the CyberArk connection is established:

- Trust Lifecycle Manager authenticates using a designated CyberArk AppID configured for certificate-based authentication
- CyberArk authorizes access to approved credentials stored within designated Safes

- Trust Lifecycle Manager retrieves credentials dynamically when executing certificate automation workflows
- Supported integrations—including infrastructure, cloud services, and application platforms—can use CyberArk-managed credentials without storing passwords locally
- When credentials are rotated in CyberArk, Trust Lifecycle Manager automatically uses the updated credentials without requiring reconfiguration

This architecture enables secure, automated certificate management while ensuring privileged credentials remain under CyberArk governance.

Business Value

- Together, Trust Lifecycle Manager and CyberArk CCP help organizations:
- Eliminate hard-coded and locally stored privileged credentials
- Support just-in-time access to secrets for certificate operations
- Prevent outages caused by expired or misconfigured certificates
- Automate certificate renewal and deployment for short-lived certificate environments
- Strengthen zero trust initiatives through dynamic credential retrieval
- Improve compliance through centralized credential governance and auditability
- Reduce operational overhead through certificate lifecycle automation
- Maintain visibility and control across machine identities
- Increase cryptographic agility in preparation for emerging standards and post-quantum transitions
- Improve collaboration between security, infrastructure, and operations teams

Build a more resilient machine identity strategy

As organizations expand across hybrid and multi-cloud environments, the number of machine identities and privileged credentials continues to grow. Managing these critical assets independently creates unnecessary complexity and operational risk.

By integrating CyberArk Central Credential Provider with DigiCert Trust Lifecycle Manager, organizations can automate certificate lifecycle management while maintaining centralized control over privileged credentials.

The result is stronger security, reduced operational burden, and a scalable foundation for modern machine identity management.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in identity security, trusted by organizations around the world to secure human and machine identities in the modern enterprise. CyberArk's AI-powered Identity Security Platform applies intelligent privilege controls to every identity with continuous threat prevention, detection and response across the identity lifecycle. With CyberArk, organizations can reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities, including workforce, IT, developers and machines, to securely access any resource, located anywhere, from everywhere. Learn more at cyberark.com.