

From Manual to Self-Healing: Automating Enterprise Certificate Management

AMBITION

An **industrial engineering enterprise** faced a growing, often invisible security risk: managing thousands of security certificates using outdated, manual Public Key Infrastructure (PKI) processes. Certificate tracking, renewal, and failure handling relied heavily on manual intervention, increasing the risk of unexpected expirations and system outages.

A single missed renewal could disrupt critical internal systems or introduce compliance violations. The ambition was clear: **replace manual PKI operations with an automated, resilient certificate management framework that ensured security, uptime, and audit readiness at scale.**

To achieve this, the organization needed to:

- **Automate certificate lifecycle management:** Remove reliance on manual tracking and intervention.
- **Prevent operational disruption:** Ensure critical certificates do not expire unexpectedly.
- **Strengthen compliance posture:** Enable transparent reporting and built-in failure handling.

ACTION

The organization partnered with **Wipro Engineering – Connected Services**, recognizing the need for an automated, resilient PKI capability. Working alongside the client's PKI Security and Identity teams, Wipro implemented a comprehensive modernization strategy:

- **Zero-Touch Architecture:** Introduced a subscription-based custom PKI client integrated with Microsoft CA and Dogtag.
- **Intelligent Automation:** Automated the full certificate lifecycle through event-driven workflows covering issuance, renewal, and monitoring.
- **Resilience Engineering:** Implemented fault-tolerant failover mechanisms, retry logic, and comprehensive unit testing to reduce the risk of missed renewals.
- **Compliance Tooling:** Delivered automated export and reporting features to support internal and external security audits.

AMBITIONS REALIZED

By replacing manual processes with an automated PKI solution, Wipro transformed how the organization manages enterprise trust — closing critical security gaps and converting a high-risk operational area into a stable, self-managed security capability.

The Business impact:

- **Automated lifecycle management**, removing day-to-day administrative burden from infrastructure teams and significantly reducing renewal times.
- **Elimination of expiration-related outages**, ensuring continuous operational uptime.
- **Future-ready scalability**, with a compliance-ready PKI foundation designed to integrate with modern and open-source Certificate Authorities.