Zero Trust in Manually Applying and Deploying SSL Certificate

December 29, 2025

In the digital age, SSL/TLS certificates are the cornerstone of network security and data encryption. HTTPS encryption safeguard communication between browsers/APPs, websites, APIs, and services, preventing man-in-the-middle attacks and data breaches. Yet, high-profile service outages caused by expired SSL certificates continue to expose the dangers of manual processes - especially when certificate application (requesting/issuing) and deployment (installation/configuration in Web server, load balance, SSL gateway) are handled by separate teams.

These incidents, often rooted in human oversight, miscommunication, or lack of coordination, make one thing clear: why should we still trust manual certificate workflows? This article highlights the critical importance of full automation, illustrates the risks through real-world disasters, and emphasizes the urgent need for automation in the context of post-quantum cryptography (PQC) migration. Calling for a full transition to a 'zero-trust human' certificate automation management model to prepare for the upcoming new regulation of a 200-day validity period.

1. Manual Application and Deployment ss a High-Risk Practice

The traditional manual workflow typically involves two distinct phases and often two different teams:

- **Application phase** (Certificate Issuance): Generating private key and CSR, submitting CSR to a CA, validating domain ownership, receiving the certificate, and,
- **Deployment phase** (Installation & Configuration): Uploading the certificate to servers, load balancers, CDN, SSL gateways, and configuring it correctly.

When these steps are handled by separate teams (e.g., security team handles issuance, infrastructure team handles deployment), the risks multiply:

- **Coordination failures**: Handover delays, miscommunication about validity periods, or incorrect domain names.
- **Human error**: Forgotten renewals, misconfigured servers, permission issues, or expired

certificates going unnoticed.

- **Scale challenges**: Large organizations manage thousands of certificates across multiple environments; manual processes are slow and prone to oversights.
- **Lack of monitoring**: Without automation, expiration is often only discovered after users complain.
- **Security risks**: Manual handling private keys or insecure configurations, especially in multi-team environments.

In contrast, automation certificate management (ACME protocol) enables seamless application, issuance, renewal, and deployment - eliminating handovers and human error. Even more critically, the rise of quantum computing makes PQC migration an immediate priority. Current RSA/ECC/SM2 algorithms may be broken within the next decade. Short-lived certificates (90 days or less) are the only feasible way to quickly adopt new PQC algorithms, and this demands full automation.

2. Real-World Disasters: Service Outages Caused by Manual Oversight

The following 5 high-profile website security incidents demonstrate the catastrophic consequences of relying on manual certificate application and deployment:

Date	Organization/Service	Incident Description	Impact Duration / Severity	Root Cause Analysis
Dec. 2018	Ericsson / O2 (UK mobile operator)	Expired certificate in Ericsson telecom software caused O2's mobile data system to fail.	~23–24 hours; affected 32 million users and operators in 11 countries	Manual renewal failure; O2 claimed millions in compensation from Ericsson.
August 2023	Adobe (account.adobe.com)	Adobe account login certificate expired 24 days prior, blocking access to Creative Cloud and other services.	~1–25 days; global subscriber impact	Lack of monitoring; expired certificate went unnoticed for weeks.
July 2011	Microsoft (Hotmail, Xbox Live, etc.)	Multiple Microsoft services had expired certificates, preventing global login and access.	Hours to 1 day; affected hundreds of millions of users	Manual renewal oversight; no effective monitoring.
Sept. 2021	Facebook (Instagram, WhatsApp)	Expired internal certificate (combined with other issues) triggered a global outage.	~6–7 hours; entire platform offline	Manual management of internal CA; certificate not renewed in time.
March 2023	OpenAI (ChatGPT)	Certificate issues disrupted	~1–2 hours;	Manual deployment

		login and API access to ChatGPT.	widespread global user impact	error, certificate not updated.

These are not isolated cases. From Microsoft's early incidents to recent outages at Adobe, Facebook, and OpenAI, manual certificate workflows - especially when split across teams - have repeatedly proven to be a ticking time bomb. Had these systems used automatic management, these disasters could have been entirely prevented.

The above incidents occurred during periods when SSL certificates were valid for 3 years, 2 years, and 1 year. As the validity period of SSL certificates is about to be reduced to 200 days, 100 days, and 47 days, if action is not taken promptly to achieve certificate automation, the author believes more similar security incidents will occur. It is crucial to immediately check all website system assets and implement automatic SSL certificate management for all systems.

3. PQC Migration: Automation is the Only Path Forward

Post-quantum cryptography is an urgent reality, there is now a security threat of 'harvest now, decrypt later'. Quantum computers could break current cryptography algorithms as early as the 2030s. NIST released PQC algorithm and is finalizing more PQC standards, and the global industry has already begun the PQC migration.

This transition demands:

- **Frequent rotation**: Certificates must be regularly updated to incorporate new PQC algorithms.
- **Short-lived certificates**: 90-day or even 47-day validity periods SSL certificates are coming. Only automation can handle such frequent renewals reliably.
- **Zero-trust model**: Certificate management must be fully automated via CI/CD pipelines and API-driven certificate integration, eliminating manual handovers between teams.

Currently, the widely implemented hybrid PQC algorithm for HTTPS encryption uses the traditional SSL certificate. If SSL certificate automation management is implemented, simply upgrading the web

server to support the hybrid PQC algorithm will automatically achieve PQC migration. Certificate automation is fundamental; without it, PQC migration will turn into a nightmare and is an impossible task to accomplish.

4. Call to Action: Automate Your Certificates Today

Stop gambling on human perfection and inter-team coordination. Take these steps now:

(1) **Assess your current state**: Scan all certificates for expiration risk using tools like SSL Labs or crt.sh.

(2) **Implement full automation**: Few websites use certificate automation tools or cloud services that support certificate automation to achieve full automation from application to deployment. Many websites achieve certificate automation by deploying HTTPS Automation Gateway.

(3) **Set up monitoring**: Even after implementing automatic certificate management, it is still necessary to strengthen monitoring initially to ensure that all certificates are properly managed automatically.

(4) **Start PQC migration**: The sooner the PQC migration is implemented, the sooner valuable data assets will be secured. Completing the PQC migration while implementing certificate automation is truly the best approach.

(5) **Adopt zero trust**: Zero trust manual handling, assume manual processes and team handovers will fail. Build fully automatic, redundant workflows.

Certificate automation is not a nice-to-have; it is a must-have, especially the imminent arrival of the 200-day certificate on 'March 15'. The major outages listed above are stark reminders that trusting manual application and deployment, especially across separate teams, is trusting luck, and often end up losing bets. Embracing automation not only prevents disruptions but also future proofs your systems for the quantum era.

Is your organization ready for certificate automation?

Richard Wang

December 29, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 106 articles in English (more than 228K words) and 246 articles in Chinese (more than 728K characters in total).