对人工申请和部署 SSL 证书零信任

2025 年 12 月 29 日

在数字化时代，SSL 证书是保障网络安全和数据加密的核心组件，HTTPS 加密确保了浏览器/APP、网站、API 和服务之间的安全通信，防止中间人攻击和数据泄露。然而，近年来因证书过期导致的重大服务中断事件频发，这些事故大多源于人工申请和部署过程中的疏忽—尤其是当 证书申请（生成 CSR、向 CA 提交申请、领取证书）和 证书部署（服务器证书安装、配置负载均衡器或网关设备）由两个不同团队负责时，风险成倍放大。

这些频发事故生动地告诉我们：为什么还要对人工操作抱有信任？本文将通过真实的大规模故障案例，说明人工申请与部署证书的巨大风险，强调证书自动化的必要性，并结合后量子密码（PQC）迁移的迫切需求，呼吁全面转向“零信任人工”的证书自动化管理模式，以迎接即将到来的 200 天有效期新规。

一、 人工申请和部署 SSL 证书是高风险操作

传统人工流程通常分为两个环节，且往往由不同团队负责：

- 申请阶段（证书颁发）：生成私钥和 CSR、提交 CSR 给 CA、验证域名控制权、领取证书。
- 部署阶段（安装与配置）：将证书上传到服务器、CDN、负载均衡器、网关设备，并完成证书安装与配置。

当这两个环节由不同团队（例如安全团队负责申请、运维/基础设施团队负责部署）时，风险显著增加：

- 协作断裂：交接延迟、有效期信息传递错误、域名填写不一致等。
- 人为失误：忘记续期日期、配置错误、权限问题，导致证书过期后服务直接崩溃。
- 规模难题：大型企业管理成千上万张 SSL 证书，手动操作效率低下，容易遗漏。
- 监控缺失：没有自动化告警，证书过期往往是在用户投诉后才被发现。
- 安全隐患：手动流程存在私钥泄露风险，不安全配置风险，尤其在多团队协作时。

相比之下，自动化证书管理可以实现从证书申请到证书部署的全流程无缝自动化，彻底消除团队交接、人为失误和私钥泄露等问题。更重要的是，随着量子计算的兴起，后量子密码迁移已成为当务之急。传统 RSA/ECC/SM2 算法可能在 2030 年前后被破解，短生命周期证书（90 天或更短）是快速轮换 PQC 新算法的唯一可行方式，而这只能依靠全自动化实现。

二、 真实案例：人工疏忽引发的服务中断“大灾难”

以下 5 个经典安全事件都因人工管理证书失误（尤其是申请与部署环节的脱节）导致全球用户受影响、导致数亿美元损失。大家不要以为这些事件都发生在国外，国内事件更多并且更严重，只是没有公开披露而已。

日期	组织/服务	事故描述	影响时长/严重性	根因分析
2018 年 12 月	Ericsson / O2 (英国电信运营商)	Ericsson 电信设备中的软件证书过期，导致 O2 的移动数据管理系统崩溃。	约 23-24 小时，全网中断，影响 3200 万用户及全球多家电信运营商	人工未及时续期，软件失效引发连锁崩溃；O2 向 Ericsson 索赔上亿美元。
2023 年 8 月	Adobe (account.adobe.com)	Adobe 账户登录门户证书过期 24 天，用户无法登录 Creative Cloud 等服务。	1-25 天，全球订阅用户受影响，中国用户影响最长	人工监控缺失，过期后才被大规模发现，发现一个更新一个，并没有全部检查更新。
2011 年 7 月	Microsoft （Hotmail、Xbox Live 等）	多个微软服务证书过期，导致全球用户无法登录和使用。	数小时至 1 天，影响数亿用户	人工续期遗漏，无有效监控机制。
2021 年 9 月	Facebook （包括 Instagram、WhatsApp）	内部证书过期（结合其他问题）引发全球性服务中断。	约 6-7 小时，全平台瘫痪	人工管理内部 CA，过期未及时处理。
2023 年 3 月	OpenAI（ChatGPT）	ChatGPT 登录和 API 访问因证书问题受阻，用户无法正常使用 AI 服务。	约 1-2 小时，高峰期全球用户受影响	人工部署失误，证书未及时更新。

这些事件并非孤例。从微软的早期中断，到 Adobe、Facebook、OpenAI 的近期事故，人工申请与部署流程（尤其是多团队协作）的“定时炸弹”一次次爆炸。如果这些系统采用自动化证书管理，这些灾难本可以完全避免。

以上事故发生在证书有效期为 3 年、2 年、1 年的时段，而随着 SSL 证书有效期即将缩短为 200 天、100 天、47 天，如果不赶紧采取行动实现证书自动化的话，笔者相信还会发生更多的类似安全事故，必须马上清查所有网站系统资产，为所有系统实现 SSL 证书自动化管理。

三、PQC 迁移：自动化是唯一出路

后量子密码不是遥远的未来，而是迫在眉睫的现实，现在已经存在“先收集后解密”安全威胁。量子计算机可能在 2030 年前后破解当前密码体系，美国 NIST 已经发布 PQC 算法并还在推进新 PQC 算法，我国 ICCS 也已启动后量子密码算法征集工作，全球业界已经启动 PQC 迁移。这意味着：

- 频繁轮换：证书需定期更新以集成新算法，手动操作将不可能。
- 短生命周期证书：90 天甚至 47 天有效期已成为行业趋势，只有自动化才能可靠处理高频续期。
- 零信任框架：证书管理应完全自动化，通过 CI/CD 管道和 API 驱动的证书集成交付，消除人工团队交接。

目前全球广泛实施的混合 PQC 算法 HTTPS 加密使用的传统算法 SSL 证书，只要实现了 SSL 证书自动化管理，则只需升级 Web 服务器支持混合 PQC 算法，就自动化实现后量子密码迁移，证书自动化是基础，没有证书自动化，PQC 迁移将变成一场噩梦，是不可能完成的工作。

四、行动呼吁：从今天开始自动化你的 SSL 证书

笔者呼吁：作为运维、开发或安全团队，别再赌运气和团队协作。应该立即采取以下行动：

(1) **评估现状**：用 SSL Labs、crt.sh 等在线工具扫描所有域名的证书过期风险。

(2) **实现全流程自动化**：单个网站采用证书自动化工具-ACME 客户端或支持证书自动化的云服务，实现从证书申请到部署的全自动。大量网站采用部署 HTTPS 加密自动化网关方式实现证书自动化管理。

(3) **建立监控**：即使是实现了证书自动化管理，还需要前期加强监控，以确保所有证书正常实现证书自动化。

(4) **启动 PQC 迁移**：早一天实现 PQC 迁移，宝贵数据资产就早一天安全。在实施证书自动化改造的同时完成 PQC 迁移改造，这才是上上策。

(5) **零信任原则**：不信任人工处理，假设人工和团队交接总会出错，构建冗余自动化流程。

证书自动化不是“锦上添花”，而是“雪中送炭”，特别是迫在眉睫的“3 月 15 日”的 200 天证书到来。那些“大事故”教训告诉我们：信任人工申请和部署，尤其是跨团队协作，就是在赌运气，并且往往都会赌输。果断转向自动化，不仅能避免业务中断，还能保障宝贵数据在量子时代的持续安全。

你的系统“证”的准备好实现证书自动化了吗？

王高华

2025 年 12 月 29 日于深圳