为什么必须实现证书自动化

——网站HTTPS加密管理的时代之变

一 传统模式的终结：一张通配证书管所有网站，已经行不通了

过去十年，许多单位采用**一张通配证书（*.domain.cn）覆盖所有二级域名**的方式管理网站HTTPS加密。这种方式看似简单高效，但在今天的安全环境和不断缩短证书有效期的合规要求下，已经难以为继。

1.1 私钥泄露风险极高：灾难级安全漏洞

通配证书的私钥需要经多人之手多渠道传递，并在所有需要该证书的服务器、CDN节点、WAF设备等多处部署存放。**任何一人或一个传递途径有问题，或一存放处被攻击，所有网站证书私钥全部泄露**。攻击者可利用泄露的私钥伪造任意子域名网站，实施中间人攻击、钓鱼诈骗等，后果不堪设想。

风险点	后果
一处泄露	所有子域名全部沦陷
难以追溯	私钥存放点过多，泄露后难以定位源头
更换成本高	私钥泄露后需更换所有相关证书，涉及数百个系统

1.2 证书有效期急剧缩短：从“年”到“月”的剧变

国际标准组织持续收紧证书有效期，2019年每月更换一次，将来可能每5天更换一次，一张通配证书，也无法减轻证书申请和证书安装负担。

时间	证书最长有效期
2020年之前	2年（825天）
2020年9月起	1年（398天）
2023年起	398天（已实施）
2026年3月15日	200天（已实施）
2027年3月15日	100天 (即将实施)
2029年3月15日	47天
未来趋势	7天

苹果、谷歌等浏览器厂商已明确推动缩短至90天，甚至更短。这意味着：

◆ 明年开始：每3个月需要更换一次证书

◆ 未来：可能每月更换一次

一张通配证书，也无法逃避这个趋势。

1.3 运维灾难：手工管理已不可能

假设您的单位有**200个网站**，每个网站需要独立证书（因为通配证书已不再安全）。按90天有效期计算：

项目	数量
每年证书申请次数	200 × 4 = **800次**
每次操作步骤	申请、验证、下载、安装、配置、测试
所需人力	**至少1-2名全职人员**
出错概率	极高，一次遗漏就导致业务中断

结论：手工管理证书的时代已经结束。无论您愿不愿意，证书有效期不断缩短的趋势不可逆转，只有自动化才能应对。

二 政策与技术双重驱动：自动化已成刚需

2.1 国内合规要求

法规/标准	要求	自动化价值
等保2.0	三级以上系统必须实现网站加密	自动化确保证书永不过期，持续合规
密评GM/T 0054	重要网站须支持国密SSL	自动化可一键完成国密改造
《密码法》	关键信息基础设施须使用商用密码	自动化确保国密证书持续更新

2.2 国际标准趋势

CA/浏览器论坛：持续推动缩短证书有效期，将来还有可能缩短到7天！这些趋势意味着：**无论您使用哪家CA的证书，有效期都在不可逆转地缩短。**

2.3 “先收集、后解密”的现实威胁

攻击者现在就可以窃取加密数据，存起来等待量子计算机成熟后再破解。这意味着：

◆ **今天的敏感数据，可能在3-5年后被批量泄露**

◆ 欧美政府、银行、高校、医院已基本完成后量子密码迁移

◆ **我国还是空白**

后量子密码不是未来概念，而是**现在就必须应对的现实威胁**。

三 自动化带来的三重价值

3.1 安全升级：消除证书管理的人为风险

传统方式的风险	自动化后的保障
人工操作易遗漏，导致证书过期	自动监控、自动续期，永不过期
私钥多处存放，泄露风险高	集中管理，私钥不出设备
通配证书一旦泄露，全部沦陷	每个网站独立证书，风险隔离

3.2 运维解放：让信息中心聚焦核心业务

传统方式	自动化后
每年数百次手动操作	一次部署，5年零运维
需要专人盯防证书到期	自动提醒、自动更新
深夜紧急处理证书过期事故	从此告别“半夜救火”

3.3 合规保障：从容应对检查与测评

检查项	自动化方案如何应对
等保2.0对网站加密的要求	证书自动更新，永不过期
密评对国密支持的要求	一键开启国密改造
信创验收对国产密码的要求	北京CA验证签发国密OV SSL证书

四 如何实现证书自动化？

实现证书自动化，需要一套完整的解决方案，而非单一工具。理想的自动化方案应具备：

能力	说明
多CA高可用	对接多家国际CA和国密CA，一家故障或断供自动切换，杜绝单点风险
国密+国际双证书	同时支持国际证书和国密证书，满足合规与兼容双重需求
后量子密码就绪	支持后量子密码算法，即刻防御“先收集后解密”攻击
内置WAF联动	证书自动同步至WAF，确保防护永不过期
软硬一体	旁路部署，无需改造网站架构，5年零运维

数字认证 SSL自动化网关正是这样一套完整方案。它帮助政府、银行、高校、医院等网站密集型机构，从容应对证书有效期缩短、国密改造、后量子迁移三大趋势，实现网站加密的**全自动、高可用、面向未来**。

五 行动建议

1. 立即评估：盘点您单位现有的网站数量、证书管理方式、国密改造进度

2. 明确趋势：认识证书有效期缩短的不可逆性，以及“先收集后解密”的现实威胁

3. 规划自动化：将证书自动化纳入年度信息化建设规划

4. 咨询专家：联系数字认证，获取SSL自动化网关的详细方案与试点支持

数字认证·为您的网站加密提供面向未来的自动化保障

北京数字认证股份有限公司　国有控股上市企业（300579）　·北京数据集团核心成员　·数字认证，SSL证书自动化领导者

联系我们：　官网 ssl.bjca.cn　　服务热线 4009-197-888　　邮箱 ssl@bjca.org.cn