多CA高可用技术白皮书

——彻底解决SSL证书供应链不稳定的终极方案

一 背景：SSL证书供应链的脆弱性已反复得到证明

SSL证书是网站安全的基础，但其供应链却异常脆弱。近年来，多起CA机构被浏览器厂商不信任的事件，给全球数以百万计的网站带来了巨大的运维灾难。

1.1 真实案例：信任危机频繁发生

时间	事件	影响范围
2017年8月	赛门铁克（Symantec，全球第一大CA）SSL证书被浏览器不信任	全球**200多万**个网站受影响，也就是全球一半证书用户，几乎所有银行网站需连夜更换证书
2024年11月	Entrust（全球第二大CA）被谷歌不信任	全球**近60万**用户需重新申请部署证书
2025年7月	中华电信CA（台湾省）被谷歌不信任	台湾省政务网站、银行网站**3万多张**证书需紧急替换

“连全球第一大CA也难逃被浏览器不信任的厄运，所有SSL证书用户是否都应该做好应急应对准备工作呢？”

1.2 极端情况：地缘政治导致的断供

2022年俄乌冲突爆发后，几乎所有俄罗斯政府网站和银行网站的SSL证书被吊销，导致所有政府网站和银行网站无法正常访问，并且断供不再签发新证书。这表明，SSL证书供应链不仅面临技术层面的风险，还可能受到地缘政治等不可控因素的影响。

1.3 核心痛点：SSL证书自动化管理的局限性

当前，全球超过90%的SSL证书已通过ACME协议实现自动化管理。然而，**仅有自动化是不够的**。当出现证书供应中断时：

◆ **传统人工管理用户：**需重新申请、下载、部署成百上千张证书，工作量巨大，极易出错

◆ **单CA自动化用户：**虽能自动续期，但一旦该CA被浏览器不信任或者断供，“自动化”就失效，仍然需要重新选择新的CA，重新人工修改并启用新的ACME服务地址，逐个网站重新配置。

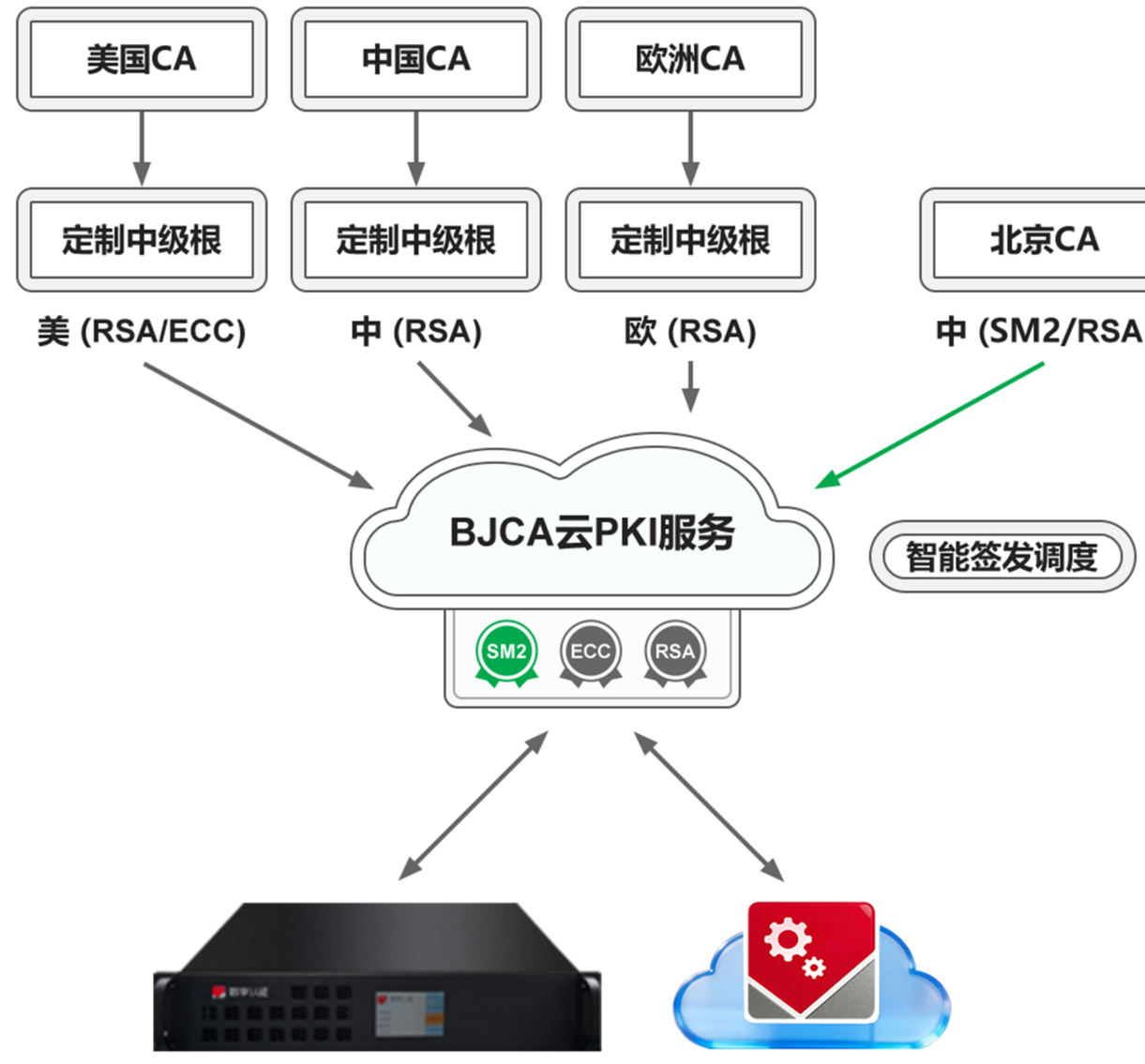
结论：单CA证书自动化管理，只能解决“如何快速更新证书”的问题，无法解决“CA断供后如何继续签发证书”的问题。

二 多CA高可用技术：从“单点依赖”到“多路保障”

2.1 技术定义

多CA高可用是指在证书自动化系统中，预对接多家权威CA机构（国际CA和国密CA），通过智能监控与自动切换机制，确保在任一CA发生故障、被不信任或断供时，证书签发通道**毫秒级自动切换至备用CA**，用户网站证书续期与签**发完全无感知、不中断**。

2.2 技术架构



2.3 核心技术能力

能力	说明
多CA预对接	已预集成多家国际CA和国密CA
实时健康监控	持续检测各CA的证书签发接口可用性、响应时间、成功率
毫秒级自动切换	默认主CA故障时，智能调度引擎自动切换至备用CA，切换时间<1秒，用户无感知
证书续期无缝衔接	切换后，仍在有效期内的证书继续使用，新签/续期证书自动由新CA签发
多算法支持	同时支持国际RSA/ECC算法和国密SM2算法，满足双合规要求

三 多CA高可用的核心价值

3.1 杜绝单点故障，确保证书签发永不断档

场景	单CA	多CA
主CA被浏览器不信任	所有证书无法续期，需人工更换供应商，耗时数周	自动切换至备用CA，证书续期正常进行，业务零影响
主CA系统升级故障	证书签发中断，业务受阻	毫秒级切换，用户无感知
主CA因地缘政治断供	证书无法获取，网站面临安全风险	自动切换至不受影响的CA，保障业务连续性

3.2 大幅降低运维负担与应急成本

◆ **传统模式：**CA供应中断后，需重新选型、采购、申请、部署，至少需要**2-3人全职工作2周**
◆ **单CA自动化：**需向新CA申请ACME服务，并逐台服务器修改ACME服务地址，仍需**大量人工操作**
◆ **多CA高可用：零人工介入**，系统自动完成切换

3.3 符合监管与行业最佳实践

◆ **等保2.0：**三级以上系统要求“高可用性”，多CA高可用是技术实现路径之一
◆ **密评要求：**国密证书需有稳定签发渠道，多CA保障国密证书供应链安全
◆ **金融行业：**网银系统对业务连续性要求极高，多CA高可用是必备能力
◆ **政务服务：**政务服务系统对业务连续性要求极高，多CA高可用是必备能力

四 实现多CA高可用的技术条件

4.1 自动化是基础

多CA高可用必须建立在**证书自动化管理**之上。如果证书仍靠人工申请部署，CA切换后仍需大量人工操作，无法发挥自动切换的价值。

4.2 遵循《自动化证书管理协议》国密标准

数字认证云PKI自动化服务系统遵循国密标准，无论证书自动化实现方式是客户端方式、还是云服务方式、还是自动化网关方式，都能实现可靠的双算法SSL证书自动化申请和签发。

4.3 健康检测与切换策略略

◆ **被动检测：**根据证书签发请求的返回结果判断CA可用性
◆ **主动检测：**定期发送探针请求，预判CA服务状态
◆ **切换策略：**支持主备模式、优先级模式

4.4 证书一致性管理

多CA签发的证书需在证书格式、有效期、算法强度等方面保持一致性，确保切换后用户侧无需适配。

五 数字认证 SSL自动化网关的多CA高可用实现

数字认证 SSL自动化网关内置了完整的**多CA高可用能力**：

特性	说明
预对接CA数量	已预对接多家国际CA和国密CA
切换机制	毫秒级自动切换，主CA故障时无缝切换到备用CA
支持算法	同时支持国际RSA/ECC和国密SM2，双算法均实现多CA保障
用户感知	完全无感知，无需任何人工干预
运维保障	5年内持续保障证书签发通道可用，免除用户后顾之忧

六 行动建议：如何评估与选择多CA高可用方案

6.1 评估现有供应商

- 您的证书供应商是否仅依赖单一CA?
- 您的证书管理是否实现了自动化?

6.2 选择标准

评估项	理想标准
多CA预对接	至少预对接3家以上国际CA和2家以上国密CA
自动切换	故障切换时间<10分钟，理想情况<1秒
自动化能力	支持国密/国际ACME协议，实现证书全生命周期自动化
国产算法支持	同时支持国密SM2算法，实现双算法多CA保障

七 总结

SSL证书的供应链安全，已经从“技术细节”上升为“业务连续性”的关键命题。频繁发生的CA不信任事件和极端情况下的断供风险，迫使每一个依赖HTTPS加密的组织必须重新审视其证书管理策略。

仅有自动化是不够的。 唯有多CA高可用 + 自动化管理的组合，才能从根本上解决SSL证书供应链不稳定的难题，确保网站HTTPS加密服务在任何情况下都能不间断运行。

数字认证 SSL自动化网关，正是基于这一理念打造的一体化解决方案，帮助政府、银行、高校、医院等网站密集型机构，构建面向未来的、高可用的网站HTTPS加密基础设施。

数字认证·多CA高可用，确保证书签发永不断供!

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