SSL自动化网关技术白皮书

一 引言：网站加密的时代之变

随着国际标准持续收紧SSL证书有效期，以及我国《密码法》、等保2.0、密评GM/T 0054等法规对国密改造的强制要求，网站加密管理正面临前所未有的挑战：

挑战	具体表现
证书有效期缩短	2026年3月15日起，证书有效期最长200天；2027年将缩短至100天；2029年缩短至47天
人工管理不可持续	100个网站每年需人工处理500次证书申请、验证、部署操作，极易出错导致业务中断
国密改造强制	等保2.0三级、密评要求重要网站必须支持国密SSL证书，传统方案改造成本高、周期长
后量子威胁现实化	“先收集后解密”攻击已成现实威胁，欧美已大规模部署后量子加密，我国尚属空白
安全防护碎片化	SSL网关、WAF、证书管理系统各自独立，运维复杂，证书过期导致WAF失效风险高

数字认证 SSL自动化网关正是在这一背景下推出的**一体化网站安全解决方案**，将证书自动化、国密改造、后量子加密、A级WAF融为一体，帮助政府、银行、高校、医院等网站密集型机构，从容应对时代挑战。

二 产品概述

2.1 产品定位

数字认证 SSL自动化网关是一款**软硬一体化**的网站安全设备，部署于网站服务器前端，提供以下核心能力：

- **证书全生命周期自动化：**自动申请、自动续期、自动部署双算法证书（国际DV+国密OV）
- **国密改造一键完成：**无需改造Web服务器，自动为所有网站启用国密SSL
- **后量子密码就绪：**全球独家支持SM2MLKEM768 + X25519MLKEM768双混合PQC算法
- **内置A级WAF：**防护性能达A级（Cloudbric权威认证），与证书自动化深度集成

2.2 为什么必须同时实现全自动化？

型号	支持网站数	适用场景
基础版	20个	**小型单位、部门级网站群**
企业版	100个	**大中型单位、行业网站群**
旗舰版	255个	**省级政务云、大型银行、高校网站群**

2.3 产品架构

三 核心技术能力

3.1 证书自动化·多CA高可用

技术实现：

◆ 内置数字认证云PKI平台，预对接多家国际CA和国密CA

◆ 通过国密ACME协议自动申请、验证、续期、部署证书

◆ 实时监控各CA服务状态，主CA故障时**毫秒级自动切换至备用CA**

客户价值：

◆ 彻底杜绝单点故障，证书签发永不断供

◆ 5年零运维，解放运维工程师人力

◆ 证书有效期越短，自动化价值越大

3.2 国密改造·TLS 1.3 + 前向安全

技术实现：

◆ 原生支持国密SM2/SM3/SM4算法

◆ 率先实现**TLS 1.3国密算法套件**

◆ 支持**前向安全性（Forward Secrecy）**：每次会话使用临时密钥，即使服务器私钥泄露，历史加密数据也无法被解密

客户价值：

◆ 一键完成国密改造，无需改造现有Web服务器

◆ 满足等保2.0、密评GM/T 0054要求

◆ 为政府、银行等长期敏感数据提供**长期安全保护**（私钥泄露不泄密）

3.3 后量子密码·双混合PQC算法

技术实现：

◆ 全球独家支持双混合PQC算法：**SM2MLKEM768**（中国方案）+ **X25519MLKEM768**（国际方案）

◆ 自动与客户端协商最优算法，优先顺序：SM2MLKEM768、X25519MLKEM768、SM2、ECC、RSA

◆ 与**零信浏览器**配套，优先采用SM2MLKEM768，实现端到端后量子密码HTTPS加密生态

客户价值：

◆ 彻底防御“先收集后解密”攻击——攻击者现在窃取的数据，未来量子计算机也无法破解

◆ 一步到位，避免未来二次投资

◆ 与国际主流生态对齐，同时满足国密合规

3.4 内置WAF·一体化架构

技术实现：

◆ 网关先完成HTTPS解密，将明文HTTP流量交给WAF模块清洗

◆ **WAF无需持有证书**，永不面临证书过期问题

◆ 通过Cloudbric WAFER权威在线测试：**真阳率98.06%，假阳率0%，检测能力和识别能力均为A级**

客户价值：

◆ 无需单独采购WAF，降低总拥有成本

◆ 彻底消除“WAF证书过期导致业务中断”的风险

◆ 覆盖SQL注入、XSS、命令注入等OWASP Top 10主要攻击类型

四 合规对应表（等保2.0 / 密评）

4.1 等保2.0对应表

等保2.0要求	对应能力	网关实现
三级 8.1.4.5 通信保密性	应采用密码技术保证通信过程中数据的保密性	自动部署双算法SSL证书，保障HTTPS加密
三级 8.1.4.6 通信完整性	应采用密码技术保证通信过程中数据的完整性	TLS协议天然支持完整性校验
三级 8.1.8.3 密码管理	应使用符合国家密码管理规定的密码产品	支持国密SM2/SM3/SM4算法，使用数字认证国密根签发证书
三级 8.1.4.8 可信验证	可基于可信根对通信设备进行可信验证	部署双证书都是由浏览器可信根签发，网关设备自身通过可信启动验证
四级 8.1.4.5 通信保密性	应采用硬件密码模块实现密码运算	网关内置通过商密产品认证的密码卡保护私钥和密码运算

4.2 密评GM/T 0054对应表

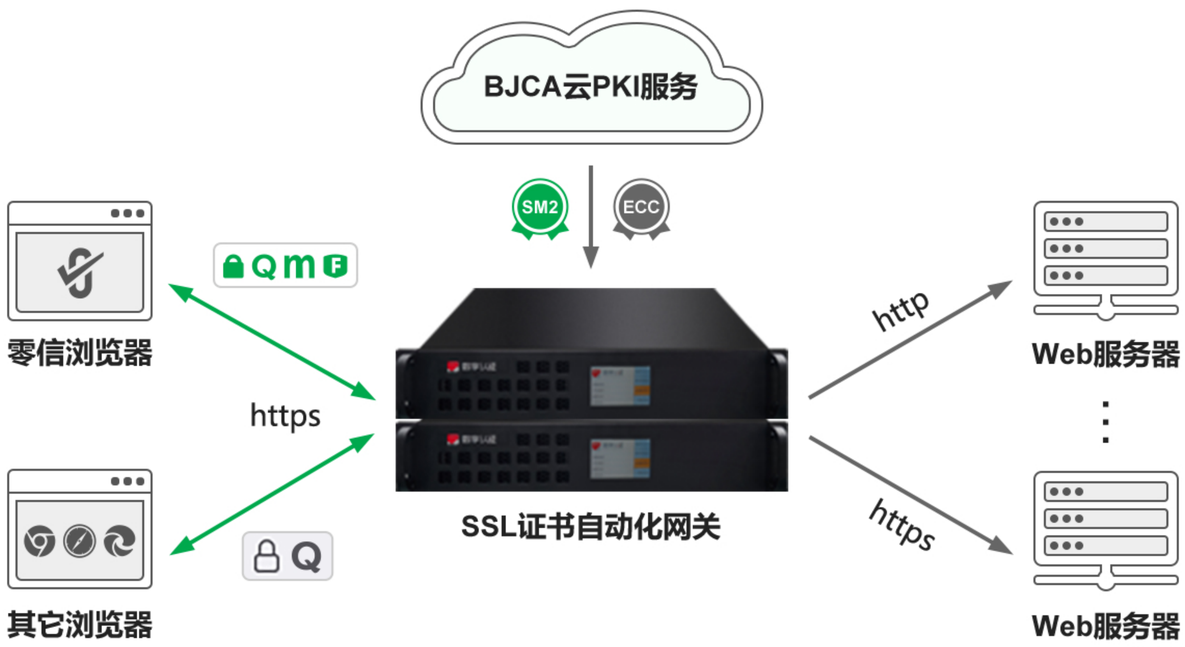
密评要求	对应能力	网关实现
GM/T 0054-2018 6.2.1 通信安全	SSL VPN网关应支持国密SSL协议	原生支持国密SSL协议（GMT 0024-2014，TLCP）
GM/T 0054-2018 6.2.2 算法支持	应支持SM2、SM3、SM4算法	支持SM2签名/加密、SM3哈希、SM4对称加密
GM/T 0054-2018 6.2.3 证书管理	应支持国密数字证书	自动对接数字认证的国密根CA，自动签发国密OV SSL证书
GM/T 0054-2018 6.2.4 密钥管理	应具备密钥全生命周期管理能力	网关内置证书自动化系统，管理证书私钥全生命周期
密评高分要求	实现TLS 1.3国密协议	**率先支持TLS 1.3国密算法，获得更高测评分数**
密评高分要求	支持前向安全性	**支持前向安全，私钥泄露不泄密历史数据，符合金融级安全要求**

4.3 信创合规对应表

信创要求	对应能力	网关实现
国产芯片适配	支持国产CPU	采用鲲鹏CPU，可选海光CPU
国产操作系统适配	支持国产OS	采用欧拉操作系统，可选麒麟OS、统信UOS等国产操作系统
国密算法支持	使用国密算法	原生支持SM2/SM3/SM4算法
国密证书支持	支持国密CA签发证书	自动对接数字认证的国密根CA，自动签发国密SSL证书

五 部署架构

5.1 典型部署拓扑



5.2 部署特点

特点	说明
前置部署	不改变现有网络架构，无需改造网站服务器
并联部署	同现有传统SSL网关并联部署，逐步分流流量，直至完全替换不支持证书自动化的传统网关
透明代理	用户无感知，网站服务器无需配置变更
高可用集群	支持双机热备，保障业务连续性
灵活接入	支持串联、旁路、云上部署等多种模式

六 性能指标

指标	基础版	企业版	旗舰版
支持网站数	20个	100个	100个
SSL握手性能	5,000 TPS	15,000 TPS	15,000 TPS
最大并发连接数	25万	150万	150万
WAF吞吐量	1 Gbps	9 Gbps	9 Gbps
证书自动化	支持	支持	支持
多CA高可用	支持	支持	支持
TLS 1.3国密	支持	支持	支持
后量子PQC	支持	支持	支持

七 总结

数字认证 SSL自动化网关是应对当前网站加密挑战的**一体化解决方案**，具备以下核心价值：

客户痛点	网关解决方案
证书管理负担重	**全自动**，5年零运维
国密改造难	**一键完成**，无需改造原Web服务器
量子威胁	**全球独家**双混合PQC算法支持，即刻防御
后量子密码迁移	待国产后量子密码算法发布后免费无缝平滑升级支持
WAF证书过期	**一体化架构**，WAF无需持有证书
多设备采购成本高	**一台替代三台**（SSL网关+WAF+证书自动化系统）
合规检查压力	**全面满足**等保2.0、密评GM/T 0054、信创要求

选择数字认证 SSL自动化网关，一次部署，五年无忧，迎接网站加密的自动化时代。

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