

# 数字认证SSL自动化网关

我们不卖SSL证书，我们提供证书自动化解决方案与持续服务。

您真正需要的不是一张张证书，而是网站HTTPS加密的持续保障、国密合规的顺利通过，以及数据在量子时代的长期安全。

## 数字认证SSL自动化网关

一台设备，一次部署，一站式解决证书自动化管理、国密改造、后量子迁移与WAF防护四大难题。



## 三大核心难题，一揽子解决

客户痛点	自动化网关解决方案
SSL证书有效期缩短至47天，手工管理崩溃，业务中断风险高	<b>全生命周期自动化：</b> 自动申请、验证、部署、续期，预设90天轮换，5年零运维
国密改造涉及服务器、浏览器全栈改造，技术复杂、周期长	<b>原系统零改造：</b> 前置部署，自动配置国密OV+国际ECC双证书，智能自适应加密
量子攻击威胁当前加密数据，“先收集后解密”已成现实	<b>后量子密码就绪：</b> 独家支持SM2MLKEM768（国密混合PQC）和X25519MLKEM768（国际混合PQC），数据长期安全

## 四大核心能力

全自动证书管理	国密合规一步到位	后量子密码迁移	一体化WAF防护
单台纳管255个网站，自动申请、验证、部署、续期，杜绝证书过期风险	自动配置双证书(国密OV+国际DV)，智能自适应算法，兼容所有浏览器	传统密码和后量子密码混合架构，为未来十年数据安全提供保障和储备	内置企业级WAF，真阳率98.06%，假阳率0%，无需单独采购

## 增强价值

<b>高性能：</b>	9Gbps HTTPS吞吐，百万级并发，默认双机热备配置
<b>高安全：</b>	硬件级私钥生成，永不离开设备；国产化平台，商用密码产品认证
<b>低总拥有成本：</b>	融合证书自动化管理、国密SSL网关、后量子密码、WAF、负载均衡于一体

## 典型客户

政务云

金融机构

医疗机构

高等院校

大型企业

# 数字认证SSL自动化网关

## 可信赖的证书自动化服务优势

在证书自动化时代，技术方案可以复制，持续、可靠的服务能力才是关键。

北京CA为您提供：

能力维度	数字认证的保障能力
资质硬核	CA牌照、国密产品资质、等保三级、信创适配认证，二十年关基服务经验
多CA供应链保障	已对接多家国际CA和国密CA，毫秒级故障切换，保证双证书永不断供
私钥绝对安全	网关硬件内生成并存储，不经人手，永不泄露
持续运维能力	7×24小时原厂技术支持，5年服务周期内免费升级算法、自动续期证书
应急响应承诺	一旦CA断供或浏览器不信任事件，立即切换证书签发通道，业务零影响

## 部署即合规，运维即安全

旁路部署，不改变现有网络架构

1小时内完成上线部署，HTTPS加密即刻生效

从证书自动化到国密合规，从后量子密码就绪到WAF防护，一台网关解决全部网站安全需求

## 产品规格简表

项目	规格
支持域名数	100 / 255 (可选)
证书类型	国密OV + 国际DV (双证书)
加密算法	SM2/SM3/SM4, RSA/ECC, MLKEM768
混合PQC	SM2MLKEM768 (IANA 4590) , X25519MLKEM768 (IANA 4588)
WAF性能	真阳率98.06%，假阳率0%，A级
部署方式	旁路透明代理，默认双机负载均衡，支持多机集群
硬件平台	国产化CPU+国产OS，商用密码产品认证