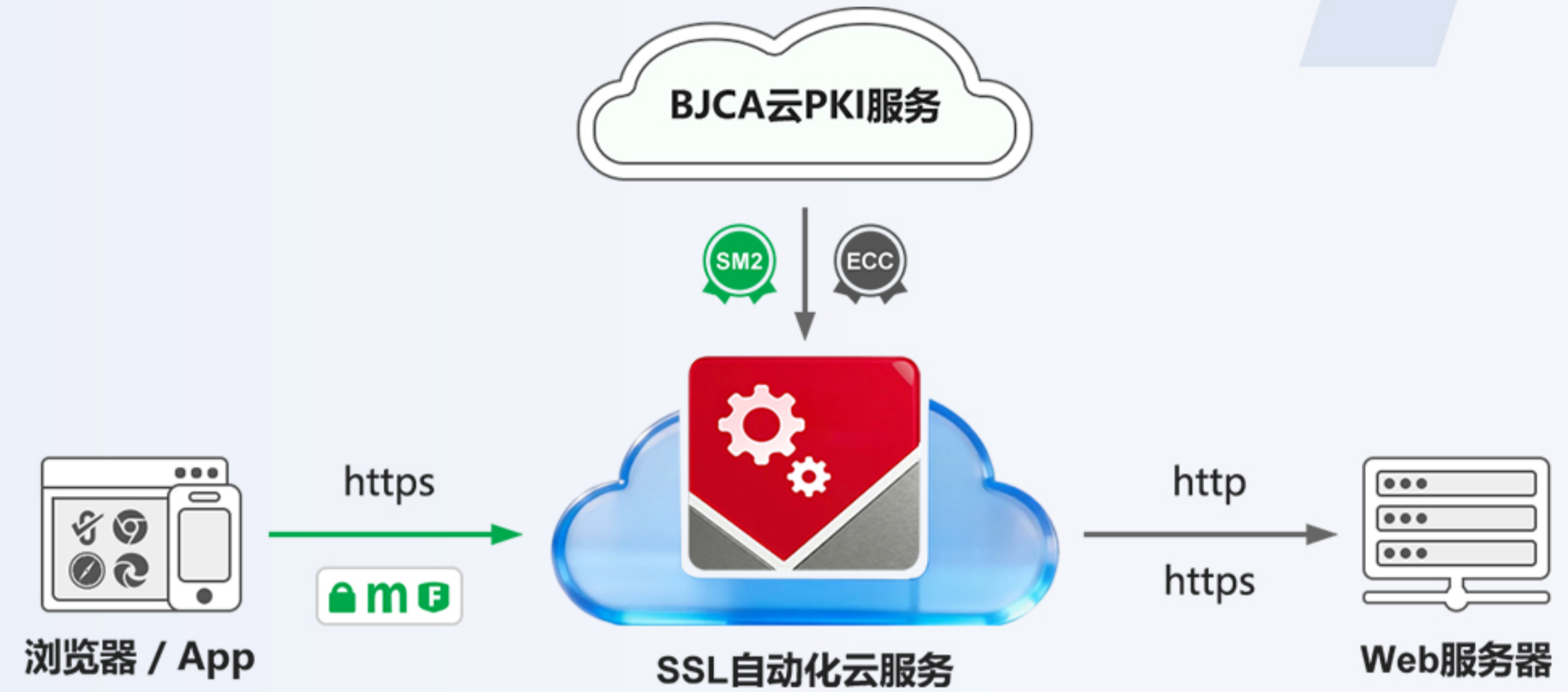


# 数字认证SSL自动化云服务

## ——为CDN而生的双算法SSL证书自动化管理

您的CDN服务，SSL证书还在手工上传吗？  
证书有效期即将缩短至100天、47天，手工管理已不再可能！  
数字认证SSL自动化云服务，让您无需更换CDN，  
无需改造架构，一键实现双证书自动化。



## 两种可选方案对比，快速选择最适合您的路径

对比维度	方案A：CDN API自动化	方案B：CDN原生集成
适用对象	正在使用CDN的客户 (阿里云、腾讯云、华为云等)	CDN服务提供商
技术路径	通过调用CDN API实现证书自动化管理	与数字认证深度合作，将密码能力原生集成至CDN平台
部署复杂度	低，仅需授权API密钥	需技术合作，集成后对用户一键开通
国密算法支持	依赖CDN节点是否支持	CDN节点原生、高性能支持国密SM2与TLS 1.3国密协议
后量子密码(PQC)	依赖CDN节点升级	架构级就绪，支持SM2MLKEM768和X25519MLKEM768
管理界面	数字认证统一管理平台	集成于CDN服务商用户控制台
核心价值	快速、低成本支持证书自动化	打造差异化安全CDN，提升核心竞争力

## 核心能力一览（方案A与方案B共享）

- 全自动双证书：** 自动申请、验证、部署、续期国密OV + 国际DV双证书，5年零运维
- 多CA签发自动切换：** 已对接多家国际CA和国密CA，双证书签发永不断供
- 统一管控：** 多CDN服务商、多域名集中管理

## 典型客户

政务云

金融机构

大型企业

CDN服务商

电商平台

# 数字认证SSL自动化云服务

## 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。

数字认证为您提供：

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	私钥由专用设备生成后通过API直接导入CDN节点服务器，不经人手，杜绝人为泄露风险
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

方案A：授权API密钥，30分钟内完成配置，双证书自动签发

方案B：作为CDN控制台原生功能，一键开通，无缝体验

从证书自动化到国密合规，从后量子就绪到统一管理，数字认证的SSL自动化云服务解决全部证书安全需求

## 产品规格简表

项目	规格
双证书类型	国密OV + 国际DV
证书有效期	默认90天，自动续期
加密算法	SM2, RSA, ECC, MLKEM768 (方案B)
混合PQC (方案B)	SM2MLKEM768 (IANA 4590) , X25519MLKEM768 (IANA 4588)
管理控制台	数字认证统一管理平台 (方案A) / CDN控制台原生集成 (方案B)
合规性	满足国密合规、等保合规、密评要求、后量子密码就绪 (方案B)