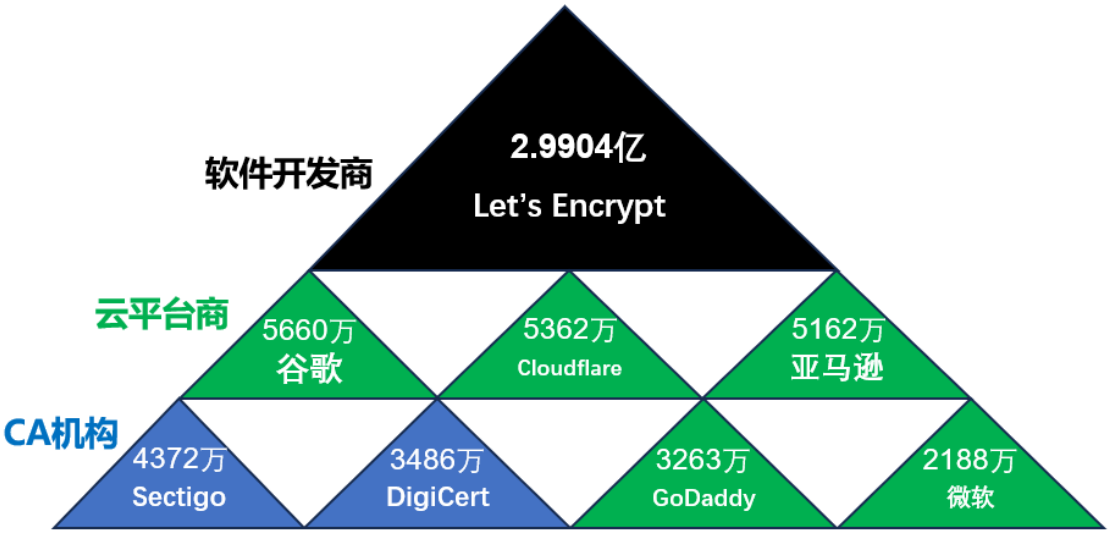
# 90 天 SSL 证书对策三：云平台篇

90 天 SSL 证书的倒计时开始了，我国做好准备了？该如何应对国际标准将把 SSL 证书有效期从目前的 1 年缩短到 90 天，笔者将针对四个不同的行业提出相应的对策，分四篇：政务篇、企业篇、云平台篇和 CA 篇，政务篇已于 10 月 19 日发表，企业篇已于 10 月 30 日发表。今天写云平台篇，就是云计算服务提供商，无论是在全球市场还是在中国市场，云服务提供商都是互联网服务提供商中最重要的提供商，所有互联网巨头也都是云平台服务提供商，所以为我国云平台服务提供商提供对策研究非常有意义，因为上一篇的企业篇的企业基本上是云平台服务提供商的用户，如果云平台服务提供商彻底解决了 90 天证书问题，也就等于大多数企业也就解决了这个问题。

## 一、 非 CA 机构如何逆袭成为主流 SSL 证书提供商的？

大家先看看下面的三角图，截止到 2023 年 11 月 4 日，谷歌证书透明日志数据库中的全球 SSL 证书签发数量排名图(前八名)，排名第一名的是一个浏览器厂商背景的 CA 机构，可以定义为是一个软件提供商，签发了 2.9904 亿张全球信任的有效 SSL 证书，排在第二位的是谷歌也是一个浏览器厂商背景的 CA 机构和云服务提供商，这里归类到云服务提供商中，也就是说其他 7 位中有 5 位是云平台服务提供商，只有两位是传统的 CA 机构，而排名第二位到第八位的 SSL 证书签发量总和比第一位还要少 412 万张。这就是自动化的魅力，因为 Let’s Encrypt 是自动化证书管理(ACME)的发起者和国际标准制定者，从 2015 年发起自动化证书管理到 2019 年成为全球第一大 SSL 证书提供商后一路高歌从未被超越过。请注意：签发数量统计数据是以证书签发中级根证书公司名称为统计依据，不是以顶级根证书来统计的。




全球前八大SSL证书提供商排名和证书签发量(2023.11.4统计)

其实 Let's Encrypt 也可以理解为是一个云密码服务提供商，Sectigo 和 DigiCert 也可以理解为一个云密码服务提供商，因为都是通过自动化云服务来为用户签发 SSL 证书，而谷歌既是云服务提供商，又是云密码服务提供商，通过自动化云服务为用户签发 SSL 证书。其他云服务提供商则不是为用户自动化提供 SSL 证书，而且直接为用户所选用的云服务自动化配置 SSL 证书而自动化实现 HTTPS 加密，这就又进了一步，让用户实现一站式云服务 HTTPS 加密安全。

以 Cloudflare 为例，这是一个提供 CDN 服务起家的云服务提供商，CDN 在起初是不支持 https 加密的，只支持 http 流量分发，但是在 https 加密日益普及的时代，CDN 必须支持 HTTPS 加密，传统的解决方案就是要求用户向 CA 申请 SSL 证书，拿到证书后手动上传到 CDN 服务中启用 CDN https 加密。但是，Cloudflare 重新定义了云时代的 CDN 服务方式，定制了自己品牌的 SSL 中级根证书，有了自动化自主签发全球信任的 SSL 证书的能力，并且提供 1.1.1.1 DNS 服务，还提供国际证书透明服务，只需用户把 NS 服务解析到 Cloudflare 的 DNS 服务器即可，自动化完成域名验证，自动化免费为 CDN 服务配置 SSL 证书，自动化实现 https CDN 服务。

这就是用户所需的云服务，因为用户都很懒的，用户需要省事的云服务，当然最好是完全免费的或省钱的，这两点非常重要，这也是为何 Let's Encrypt 能在 3 年内成为全球第一大 SSL 证书提供商的两大根本原因—自动化和免费。其他家就不详细分析了，都是因为要么自动化为用户提供 SSL 证书，要么是自动化为用户实现云服务所需的 HTTPS 加密，才赢得了全球市场，逆袭进入 CA 市场成为全球领先的 SSL 证书提供商。

## 二、 我国云服务提供商急需支持 SSL 证书自动化，自动化实现国密 HTTPS 加密

反观我国的云服务提供商，无论是传统的电信运营商还是互联网公司提供的云服务，仍然停留在传统的主机托管和虚拟主机、传统 CDN/云 WAF 服务的低层次云服务上。笔者公司使用了阿里云、腾讯云、华为云、京东云、天翼云等五大国内领先的云服务提供商的 CDN 服务，全都是需要用户自己向 CA 申请 SSL 证书，自己手动上传证书私钥和公钥到 CDN 中，再手动配置好证书才能启用 https CDN 服务，而一旦用户忘了续期 SSL 证书，就会导致 https CDN 服务失效。虽然有些服务商提供证书到期短信通知服务，但是往往会在提醒后如果有别的事情耽误了一下而后就彻底忘记了，所以，仅仅提醒是不够的，必须为用户实现自动化配置 SSL 证书，自动化实现云服务的 https 加密。这是我国云服务提供商必须向国际云服务提供商如 Cloudflare 好好学习的地方。

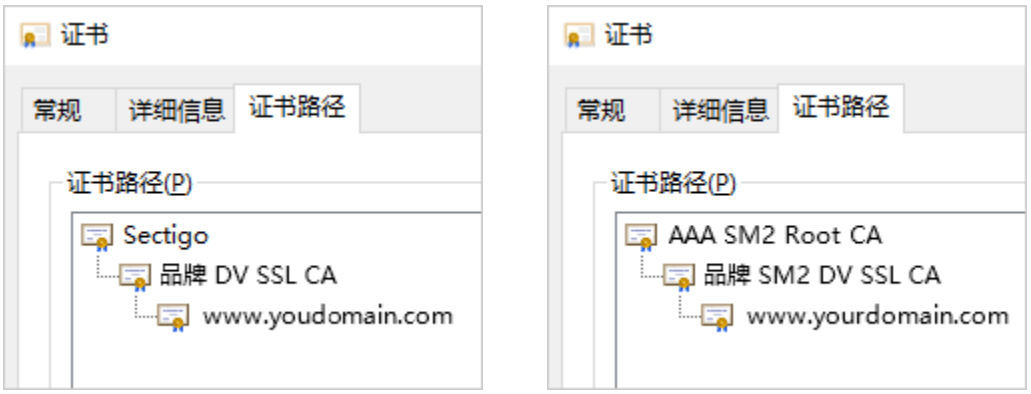
但是，我国又有不同于国外的应用需求，那就是必须实现国密 https 加密，这也是云平台可以大有作为的地方，因为传统的国密改造很难，而自动化实现国密 https 加密的云服务将成为用户的首选，也可以理解为把云服务叠加云密码服务，就能解决大多数企业用户的 https 加密自动化难题，解决 SSL 证书缩短为 90 天的危机。对于云平台来，这是一个逆袭的大好机遇，抓住了就逆袭成为领先的 SSL 证书提供商，领先的国密 https 加密服务提供商，而不应该仅仅像 CA 机构只是代理在线销售 SSL 证书。

## 三、 云平台全面实现国密 HTTPS 加密自动化行动方案

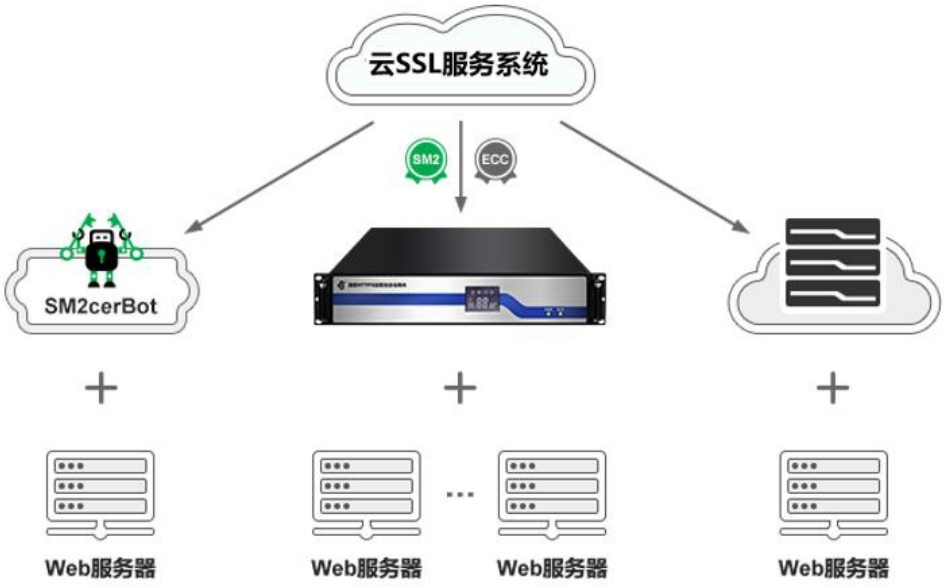
要实现国密 HTTPS 加密，当然首先必须有可靠的双算法 SSL 证书生产能力，这个生产能力就是自主自动签发支持证书透明的双算法 SSL 证书，为什么要强调支持证书透明呢？因为如果平台自动配置的 SSL 证书不支持证书透明，用户怎么能相信平台是否在用户不知晓的情况下为用户域名配置了 SSL 证书？是否会借用户的网站托管在云平台而实施其他不敢公开的非授权网络活动？所以，不仅是自动配置的国际 SSL 证书必须支持国际证书透明，而且自动配置的国密 SSL 证书也必须支持国密证书透明。

而如何具备双算法 SSL 证书的可靠生产能力？当然必须是像国际云服务提供商一样定制国际 SSL 证书中级根证书自主签发 90 天有效期 SSL 证书，还同时需要定制国密 SSL 中级根证书为用户提供双算法 SSL 证书，而不是去申请 CA 牌照成为 CA 机构或只是代理销售 SSL 证书，因为 SSL 证书只是实现 https 加密的中间产品，用户需要的是 https 加密，这是云平台应该提供的。零信技术可为云平台提供双算法 SSL 中级根证书定制服务和提供双算法证书透明

的自动化证书签发服务。




云平台在具备了双算法 SSL 证书的可靠生产能力后就可以实现具备 https 加密自动化能力，为所有云服务自动化配置双算法 SSL 证书，为云主机、CDN 服务、WAF 服务等提供自动化配置双算法 SSL 证书，并默认支持国密算法以支持国密算法 https 加密。推荐参考零信技术国密 HTTPS 加密自动化管理解决方案，在各种云服务器上部署国密 ACME 客户端软件、部署国密 HTTPS 加密自动化网关等方式为用户提供国密 HTTPS 加密自动化云服务。




而一旦实现了双 SSL 证书的自动快速部署能力为用户提供自动化国密 HTTPS 加密服务，则云平台就可以为用户提供无需国密改造的国密 https 加密改造解决方案，快速切入国密改造大市场，为用户提供国密 HTTPS 加密通道，让企业数据从产生就通过国密加密通道安全地流通，这不仅是国密合规的要求，更重要的是保证了企业数据不会在“路”上被打劫，不会被非法窃取和非法篡改，保障了企业数据的“在途”安全，有力保障我国网空安全和大数据安全。

## 四、 国密 HTTPS 加密自动化，云平台大有作为

云平台服务提供商切入国密 HTTPS 加密自动化市场，不仅是云平台自身的所有云服务系统所需的 SSL 证书实现了自动化，而且销售国密 HTTPS 加密自动化服务是一个新的利润增长点，增强云服务核心竞争力，而且真正能为企业解决 90 天证书问题而提供强大的支持，为普及国密 https 加密做出一个云平台应有的贡献。

李白有一首诗写道“楚山秦山皆白云，白云处处长随君”，这两句诗在现在一切都上云的时代可以翻译为：全国各地都在建设云平台，随时随地可为用户提供云服务。那么，云平台该如何应对即将到来的 90 天 SSL 证书规则呢？笔者也赋诗一首：

**祖国大地云涌起，端云传输需加密。**

**似水自来云服务，自动配置双证书。**

**自动化增云竞力，自动化减企负担。**

**国密普及云引领，国密加密保国安。**

王高华

2023 年 11 月 6 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。