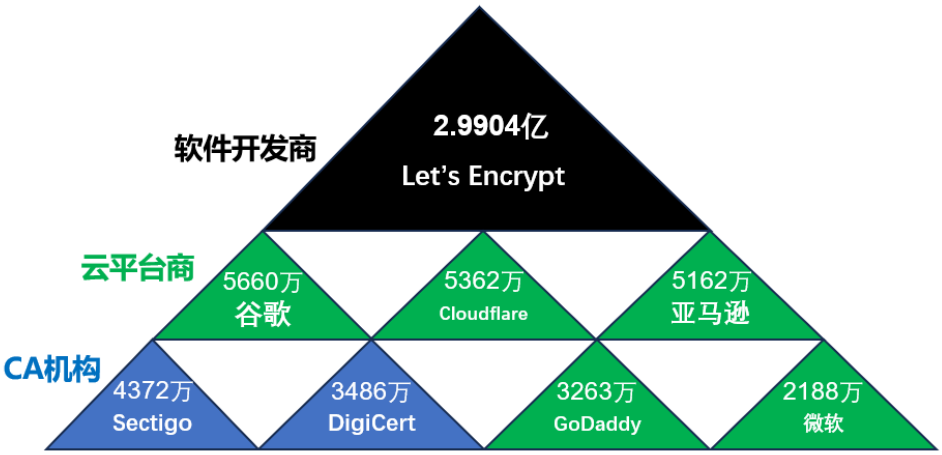
90 天 SSL 证书对策四：CA 篇

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？笔者针对四个不同的行业提出了相应的对策，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，云平台篇已于 11 月 6 日发布。今天写最后一篇-CA 篇，为何笔者把 CA 篇放在最后写呢？当然是因为笔者从事 CA 业务将近 20 年，其中前 16 年从事的是纯国际 CA 业务，而随后的 4 年是 CA 证书应用业务，对 CA 最有感情，所以把最好的最精彩的内容留在后面写，并且是倾情巨献，写完这一篇就全部完成了《90 天 SSL 证书对策》系列文章，以期能为 SSL 证书相关业界都有所启发和帮助。

一、 非 CA 机构是如何逆袭成为主流 SSL 证书提供商的？CA 机构应该怎么办？

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开发商，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 年提出自动化证书管理到 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)

这个统计图是用在上一篇-云平台篇的，为何又出现在 CA 篇？这就是要让 CA 机构了解如果 CA 机构不能及时做出战略转变，就会被云平台颠覆，就真的彻底风光不再。CA 机构的第一次风光是《电子签名法》的施行，使得 CA 机构签发的 USB Key 证书非常火爆，一个企业都需要买好几个。但是，随着政府简政放权和减轻企业负担的落实，随着移动互联网应用的流行，使得身份认证不再仅仅依赖于 USB Key 证书，让 CA 的日子就不再风光无限，仅剩下招标业务还在使用 USB Key 证书，但这个小众市场不足以养活 CA 机构。怎么办？

所幸的是，《密码法》的施行又一次把处于低谷的 CA 机构推向了更大的舞台，CA 机构应该及时抓住这次世纪大机遇。当然，这次大机遇不是《电子签名法》机遇中的安全认证业务，而是《密码法》第二条定义的对信息进行加密保护的业务，这个市场更大。特别在去年 2 月 14 日俄乌冲突发生了美国 CA 吊销和断供几乎所有俄罗斯政府和银行网站的 SSL 证书这个与 CA 有关的安全大事后，这给了 CA 机构一个绝地重生的大好机会。写本文的目的就是希望能帮助 CA 机构看清这一点，看到这个大机遇而抓住机遇，而不是在国密改造大潮中仍然只盯住已经萎缩的 USB Key 证书市场。《密码法》第二条的安全认证应用只能保证用户的身份可信，但是更重要的是要保障用户的业务系统的数据流通安全，需要用密码来实现对信息的加密保护。

中国 CA 已经错过了国际 SSL 证书市场，不是我们不努力，努力了但是由于这个市场的主导权(密码算法)掌握在人家手中，我们无法在别人主导的市场上能有所作为。所以，《密码法》和俄乌冲突的 RSA 算法 SSL 证书被吊销和断供事件给了国密 SSL 证书一个巨大的市场机会！一个让中国 CA 能夺回中国 SSL 证书市场的大好机会，这次再错过就真的不再有机会了。

应该怎么干才能抓住这次世纪机遇呢？看到国际 SSL 证书的市场份额排名大家应该清楚怎么干了，要想取胜，则学习这些胜者是怎么干的！那就是自动化证书管理！就是国密证书自动化管理！因为用户想省事，不想申请和安装 SSL 证书，不想改造 Web 服务器以支持国密算

法，他们只想一键完成国密改造，一键实现国密 https 加密，这就是 CA 机构努力的方向和实现的目标。CA 机构必须具备双算法 SSL 证书的可靠生产能力和快速应用部署能力才能赢得这个巨大市场。

二、 CA 机构如何抓住国密 HTTPS 加密的大市场？

首先，必须正确地认识到 CA 机构是要抓住国密 HTTPS 加密大市场，而不是要抓住国密 SSL 证书的市场，是需要自动化提供国密 SSL 证书和国际 SSL 证书来自动化实现国密 HTTPS 加密。因为用户需要的就是 HTTPS 加密，而不是 SSL 证书这个中间产品，而且传统的 SSL 证书申请和部署方式由于证书有效期将缩短为 90 天而变得不可操作了。

也许 CA 机构会思考这个问题：国际 SSL 证书市场就已经被国际云平台商逆袭了，国内云平台商也个个都是实力非凡，我们如何在高手如林的市场环境中取胜呢？在问答这个问题之前还是请大家先看一看深圳政务云平台的 SSL 证书招标的产品资质要求，明确要求国密 SSL 证书必须由具有工信部和国密局 CA 许可证的 CA 机构的国密根证书签发，这就是 CA 机构的独特优势，这是云平台商没有的优势，CA 机构必须把握好这个巨大优势。


三、产品资质要求

1．国密 SSL 证书由具有工信部和国密局 CA 许可证的 CA 机构的国密根证书签发；

2．国际 SSL 证书由谷歌、微软 Edge、苹果等信任的 RSA 根证书签发。

但是，请注意，这里只是要求国密 SSL 证书必须由 CA 机构的国密根证书签发，并没有要求投标方必须是 CA 机构，这是为了体现公平公正但又能保证合规。所以，CA 机构千万不要认为有了这一条要求就是你的订单了，你还需要满足其他要求才能赢得订单。

那么，CA 机构应该具备哪两个能力才能赢得国密 HTTPS 加密大市场呢？

第一，必须具备双算法 SSL 证书的可靠生产能力。

实现国密 HTTPS 加密需要国密 SSL 证书，所以 CA 机构首先必须有能力签发双算法 SSL 证书，包括国密 SSL 证书和国际 SSL 证书，因为用户需要部署双算法 SSL 证书，实现自适应算法 HTTPS 加密。其中，国密 SSL 证书必须是从自己的国密根证书签发，这就要求 CA 机构升级改造自己的 CA 系统，建设自己的国密根证书和相应的 DV/IV/OV/EV SSL 中级根证书，能签发支持国密证书透明的国密 SSL 证书，因为传统的 CA 系统只能签发 USB Key 证书。

第二，必须具备双算法 SSL 证书的快速部署能力。

有了双算法 SSL 证书的可靠生产能力后，必须具备 SSL 证书自动化管理能力，只有具备这个能力才能真正拿下国密 SSL 证书市场，才能拥有领先的市场份额，否则空具生产能力而守着金山没饭吃。第一个能力是基础，第二个能力才能核心。大家从上面的国际云平台商的逆袭可以看出，这些云平台即使没有自己的顶级根证书，也可以通过定制中级根证书来为用户提供全球信任的 SSL 证书。国内云平台也可以采用这个技术路线来实现逆袭，CA 机构就只能退居二线为其提供证书产品而已。但是，如果 CA 机构也能提供自动化部署服务，则是可以发挥其优势引领国密 HTTPS 加密大市场的。

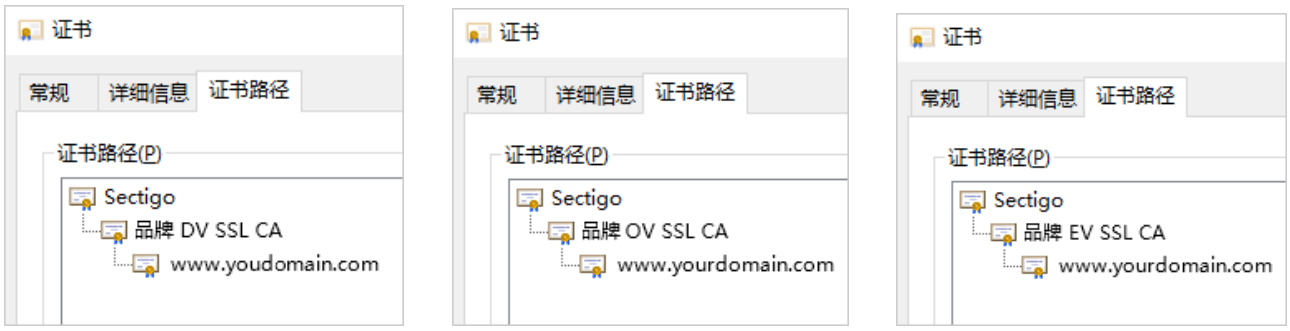
现在，如果 CA 机构不具备这两个重要能力怎么办？零信技术能助力 CA 机构具备双能力！

三、 零信技术助力 CA 机构快速具备拿下国密 HTTPS 加密市场的双能力

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 CA 机构签发的 SSL 证书不支持证书透明，用户怎么能相信 CA 机构是否会在用户不知晓的情况下为用户域名签发了 SSL 证书呢？所以，CA 机构必须能自证清白，必须透明公示每一张签发的国密 SSL 证书和国际 SSL 证书，这样才能让用户放心使用 CA 签发的 SSL 证书。这也是为何谷歌推出证书透明要求时全球 CA 都很快一致积极响应的原因，所以，从 2013 年开始每一张全球信任的国际 SSL 证书都已经支持国际证书透明，为了让用户信任国密 SSL 证书，所有 CA 签发的国密 SSL 证书也理应如此。

1. 双算法 SSL 证书的可靠生产能力

如何具备双算法 SSL 证书的可靠生产能力？对于还没有自己的全球信任的国际顶级根证书的 CA 机构，最快捷的方案就是从全球信任的国际 CA 机构定制国际 SSL 中级根证书，快速具备国际 SSL 证书的相对自主的自有品牌国际 SSL 证书签发能力，这就是零信技术提供的国际 SSL 中级根证书定制服务，助力 CA 机构能快速具备自主品牌国际 SSL 证书的自主签发能力。



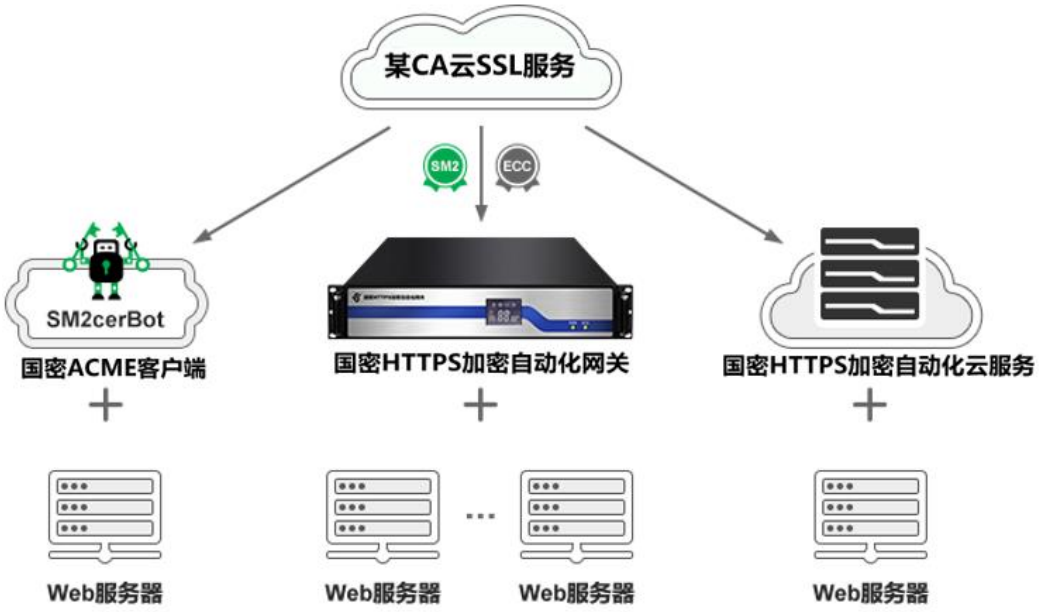
当然，还必须同时具备国密 SSL 证书的自主签发能力，这个能力必须是：(1) 自己拥有国密 SSL 顶级根证书；(2) 能自主签发支持国密证书透明的国密 SSL 证书。这就要求现有 CA 系统支持，零信技术可以为 CA 机构免费提供升级指导。如果短期内无法升级 CA 系统支持这两点，零信技术可以提供全托管服务，只需 CA 系统签发 3 个国密 SSL 中级根证书即可，直接在零信云 SSL 服务系统为用户提供双算法 SSL 证书的自主签发能力。这个全托管方式让 CA 机构能快速自主签发自己品牌的全球信任的国际 SSL 证书和自己品牌的从自己的国密顶级根证书签发的国密 SSL 证书，最终用户看到的都是 CA 机构自己品牌的支持双证书透明的双算法 SSL 证书。

2. 双算法 SSL 证书的快速部署能力

CA 机构在具备了双算法 SSL 证书的可靠生产能力就为具备双算法 SSL 证书的快速部署能力打下了实现基础。双算法 SSL 证书的快速部署能力建设是取胜的关键，就是必须提供双算法 SSL 证书自动化管理能力，帮助用户零改造实现国密 HTTPS 加密。

零信国密 HTTPS 加密自动化管理解决方案有三个：一是在用户 Web 服务器上安装国密

ACME 客户端软件-SM2cerBot，这个方案仅适用于单个网站的 SSL 证书自动化部署。对于有大量网站需要实现国密 HTTPS 加密的客户，他们希望是原 web 服务器零改造的解决方案，这就是部署零信国密 HTTPS 加密自动化网关的方案，由网关自动对接 CA 的云 SSL 服务系统，自动化为用户网站配置双算法 SSL 证书，其中国密 SSL 证书从自己的国密根签发，国际 SSL 证书从定制的自己品牌中级根证书签发，双算法 SSL 证书支持双算法证书透明。对于不想或无法部署硬件网关的用户，则可以把国密 HTTPS 加密自动化网关部署在云上提供国密 HTTPS 加密自动化云服务，一样可以帮助用户实现原 Web 服务器零改造的国密 HTTPS 加密，自适应加密算法，支持国密算法的零信浏览器优先采用国密算法实现国密 https 加密，不支持国密算法的其他浏览器则采用国际算法实现 https 加密，满足用户 https 加密自动化国密合规和全球信任的应用需求。这三个解决方案不仅为用户自动配置的双算法 SSL 证书由 CA 自己品牌根证书签发，而且还可以 OEM 为 CA 机构的自己品牌产品，满足 CA 机构拓展自己品牌的国密 HTTPS 加密自动化解决方案的战略需要。



3. 端云一体，无缝实现国密 HTTPS 加密自动化

要实现国密 HTTPS 加密，除了具备双算法 SSL 证书的可靠生产能力和自动化部署能力外，用户端还需要有国密浏览器的支持。零信浏览器是目前我国唯一一个支持国密算法和国密证书透明的、完全免费的国密浏览器，并且也是全球唯一一个集成 PDF 阅读器支持实现验证 PDF 数字签名、展示数字签名者可信身份信息及数字签名详情的通用浏览器。零信浏览器从 2022 年 6 月 1 日发布全球公测版，只用了一年半时间就已经成为了我国第一大用户使用量的国密浏

览器，这就是免费的魅力，因为国产密码应用就像国际密码应用一样需要完全免费的浏览器支持，这是用户的普遍心理预期和共识。

零信浏览器目前已经预置信任了 14 家 CA 机构的国密根证书和国家国密根证书，欢迎还未申请预置信任国密根证书的 CA 机构抓紧联系我们申请国密根证书预置信任。也希望已经预置信任的 CA 机构抓紧对接零信国密证书透明日志系统实现国密 SSL 证书支持国密证书透明。

零信浏览器是一个国密改造不可或缺的用户端软件，完全免费，有利于各家 CA 机构推广国密 HTTPS 加密自动化服务，零信国密 HTTPS 加密自动化网关是一个部署在服务端的硬件网关，零信国密 HTTPS 加密自动化云服务也是一个用于服务端的云服务，在加上零信云密码基础设施为这两个端提供自动化密码应用所需的云密码服务，端云一体才能无缝实现国密 HTTPS 加密自动化。有了云密码服务的支持，用户端和服务端都支持国密算法，就可以自动化实现从用户端到服务端的信息传输国密加密，实现全程采用国密算法来保障我国大数据流通加密安全，从而有力保障我国网空安全。

四、 CA 机构在国密 HTTPS 加密自动化市场大有作为

《密码法》的施行，给了 CA 机构再次腾飞的大好机会，CA 机构应该抓住发展机遇，踔厉奋发，加快建设双算法 SSL 证书的可靠生产能力和快速部署能力，只有具备了双能力才能赢得国密 HTTPS 加密大市场。国密 HTTPS 加密自动化服务是一个新的利润增长点，增强 CA 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 CA 机构应有的贡献。

有诗为证：

密码法助力腾飞，密码应用大机遇。

踔厉奋发早行动，能力建设放首位。

双证书自动签发，自适应加密传输。

自动化引领市场，自动加密赢未来。

王高华

2023 年 11 月 8 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。