90 天政策即将落地，零信技术已提前实施

SSL 证书 90 天有效期的国际标准即将落地，当然相应的商密标准也会相继落地，这是由谷歌在去年 3 月份发起的为了应对日益增强的算力而保障 HTTPS 加密安全的政策，这个计划有一个非常好听的名字：一起面向未来(Move Forward, Together)，核心思想是将 SSL 证书的最长有效期从现在的 398 天减少到 90 天。本文详细讲述这个 90 天政策的必要性、可行性和必然性，以及业界的应对之策，包括零信技术的实施方案。

一、 出台 90 天政策的必要性

谷歌于去年 3 月份在谷歌浏览器可信根认证计划网站提出了这个缩短 SSL 证书有效期为 90 天的计划，理由写得非常清楚：

(1)缩短 SSL 证书生命周期就是鼓励自动化部署实践，这些实践将推动 PKI 生态系统摆脱繁琐的、耗时且容易出错的部署流程。这样将允许更快地采用最新的安全功能和最佳实践，提高将 PKI 生态系统快速过渡到抗量子算法所需的敏捷性。

(2)缩短 SSL 证书生命周期还将减少 PKI 生态系统对“破烂不堪的”证书吊销检查解决方案的依赖，这个解决方案不仅无法解决故障，而且提供了不完整的保护。

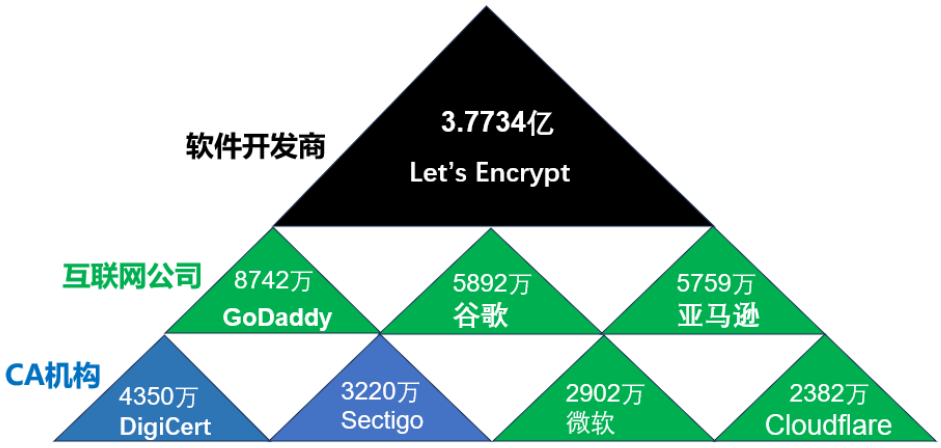
(3)较短生命周期的 SSL 证书将减少意外的证书透明日志系统被禁用的影响。

SSL 证书经历了从有效期为 5 年，降到 3 年，再降到 2 年，再降现在的到 1 年的不断缩短证书有效期的过程，这是全球业界考虑到随着全球算力的不断提升而随之而来的 SSL 证书被破解的风险的不断提升，唯一可行的方案只能是缩短密钥使用期限，在确保密钥不会被破解的时间内更换密钥，以保障 HTTPS 加密的安全，从而提升业务系统的持续安全能力。

二、 出台 90 天政策的可行性和必然性

如下图所示，截至到 6 月 22 日，全球有效的 7.44 亿张 SSL 证书中至少有 6.34 亿张是自动化部署的 90 天 SSL 证书，占比 85%，这些都是由软件厂商和互联网公司提供自动化证书管理服务来完成自动化域名验证、签发和部署的 90 天有效期的 DV SSL 证书。如果再加上传统 CA 机构(DigiCert 和 Sectigo)提供的自动化证书管理服务签发的 90 天 DV SSL 证书(按 60%比

例计)，则 90 天 SSL 证书占比已经高达 **91**%，这就是谷歌推动 90 天证书政策落地的底气，通过 91%网站已经实现 90 天政策来倒逼剩下的 9%的网站。



全球前八大SSL证书提供商排名和证书签发量(2024.6.22统计)

这些数据证明了只要实现了自动化部署，证书有效期是可以缩短到 90 天的，是可行的。缩短证书有效期就是为了进一步鼓励证书自动化部署，可以说是强制要求必须自动化部署，因为 90 天有效期证书几乎无法实现手动申请和部署，一年需要部署 5 次或者 6 次，不仅太浪费人力而且太不可靠了(可能会忘记及时续期)。

也许大家都知道，要想修改 SSL 证书有效期为 90 天成为国际标准，需要 CA/浏览器论坛所有成员单位投票通过，而仅仅是谷歌浏览器提议是不够的。但是，大家都应该知道，谷歌浏览器拥有 70%以上的全球市场份额，即使这项政策投票未通过，如果谷歌一定要实施的话，则谷歌浏览器也可以独家宣布采用这个政策—不再信任超过 90 天有效期的 SSL 证书，则 CA 机构也就只能乖乖地执行这个政策了，SSL 证书有效期从两年降到 1 年也是因为苹果强势实施而变成了事实。所以，90 天政策一定会落地，只是一个何时落地的问题，业界和用户都必须做好思想准备，并提前行动起来。

三、 我国的 90 天证书应对之策

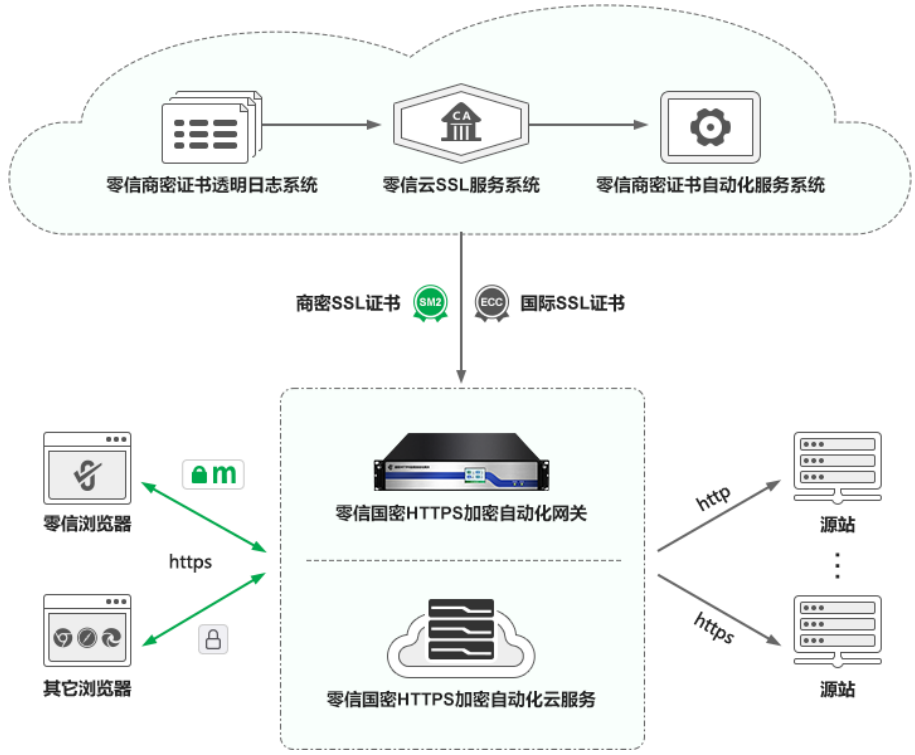
大家从上图可以看出，推动 90 天证书实施的是软件开发商和互联网公司，市场份额占比超过 85%。我国目前在这方面非常落后，自动化部署比例估计占比少于 10%，超过 9 成的 SSL 证书都是传统的手动申请和部署。也正是由于手动部署，也就很难实现普及应用 HTTPS 加密，使得我国网站的 SSL 证书普及率不到 20%，这严重制约我国互联网的整体安全水平，严重影响了互联网数据的安全和互联网应用的安全。

随着 90 天政策落地步伐的不断临近，我国业界必须赶紧行动起来，为即将到来的 90 天政策做好充分的准备。云服务提供商和互联网公司应该向国际云服务提供商和国际互联网巨头学习，尽快提供 SSL 证书自动化部署服务，而传统 CA 机构也应该及时转型，为用户提供 SSL 证书自动化部署服务。

四部委 5 月 22 日发布的《互联网政务应用安全管理规定》(以下简称《规定》)要求所有互联网政务应用网站，也就是所有政府机关事业单位的官网都必须实现商密 HTTPS 加密，所有 CDN 服务都必须支持商密 HTTPS 加密，这个规定也适用于所有关键信息基础设施提供商的官网和业务系统。《规定》将于即将到来的 7 月 1 日施行，11 万多个机构事业单位官网要实现商密 HTTPS 加密，这是一个非常艰巨的任务，当然也是业界一个巨大的市场机会，唯一可行的方案是自动化，自动化部署商密 SSL 证书实现 HTTPS 加密安全连接。

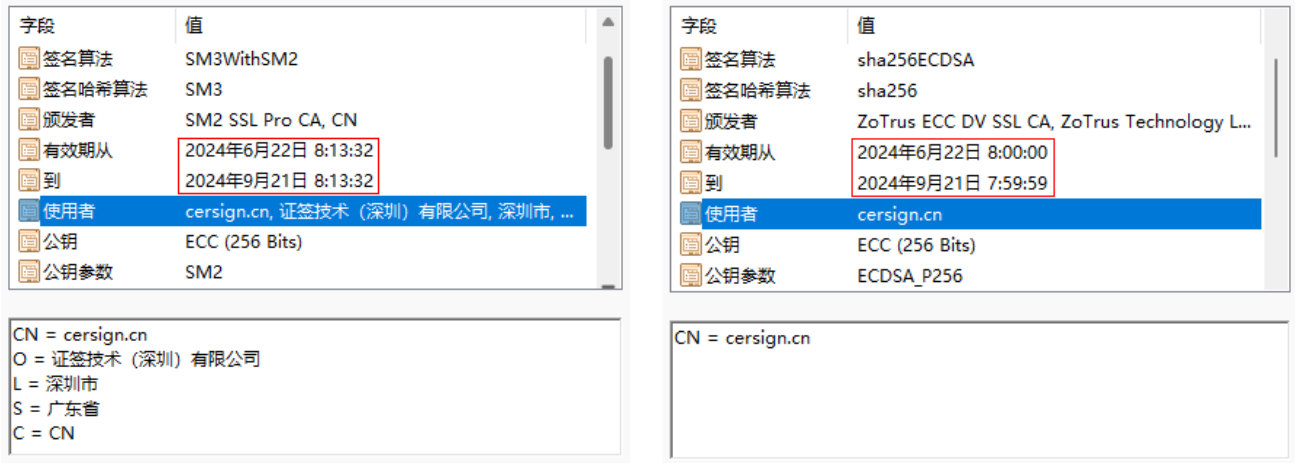
四、 零信技术为 90 天政策做好了充分的准备

零信技术早在 3 年前就认准了 SSL 证书自动化这个方向，发力双算法 SSL 证书的自动化管理，而不仅仅是国际算法 SSL 证书，而是商密 SSL 证书和国际 SSL 证书的双自动化部署解决方案，这是一个端云一体的、原 Web 服务器零改造的、自动化申请和部署双 SSL 证书、自动化实现自适应密码算法的 HTTPS 加密自动化解决方案。

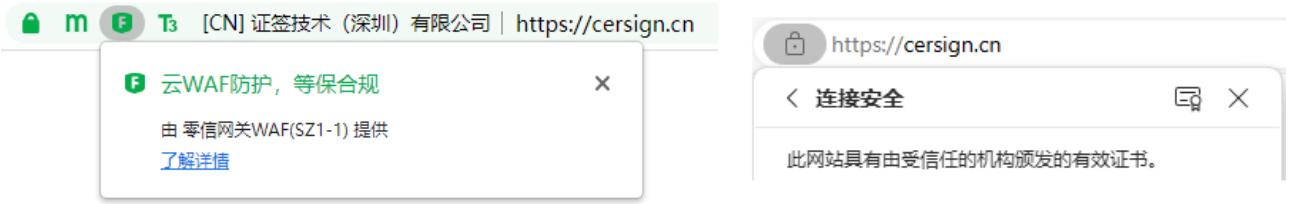


无论用户选择部署零信网关还是选用零信云服务，都可以快速(一天)实现双 SSL 证书自动

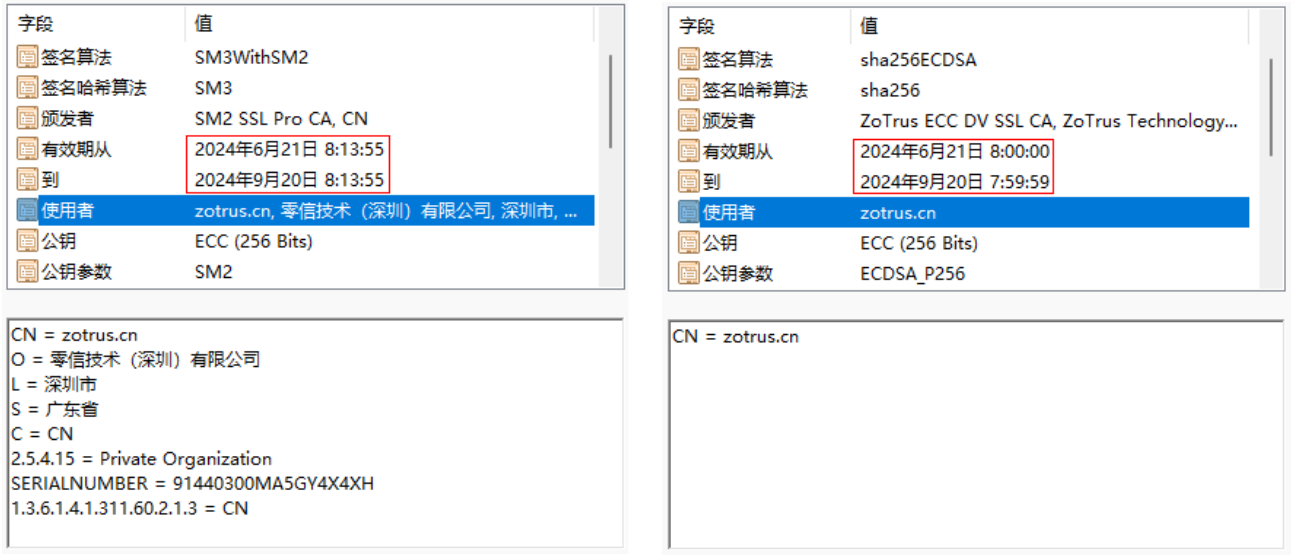
化管理，所有自动化配置的双 SSL 证书都是 90 天有效期证书，包括 DV/OV/EV SSL 证书，包括商密 SSL 证书和国际 SSL 证书。如下图所示，零信网关自动化默认为用户配置的双 SSL 证书是商密 OV SSL 证书和国际 DV SSL 证书。可以看出：这两张 SSL 证书的有效期都是 90 天，90 天商密 OV SSL 证书和 90 天国际 DV SSL 证书。



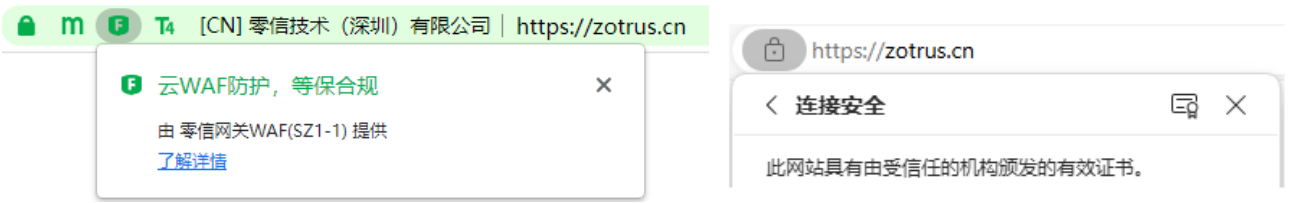
读者朋友可以使用零信浏览器查验，如下图所示，加密锁和 **m** 标识表示采用商密算法实现 HTTPS 加密，**F** 标识表示由零信网关 WAF 提供云 WAF 防护服务，T3 标识和浅绿色地址栏表示这张商密 SSL 证书是 OV SSL 证书。请同时使用其他浏览器查看国际 SSL 证书，是一张采用 ECC 算法的从 ZoTrus 自有品牌中级根证书签发的 90 天有效期 SSL 证书。



如下图所示，这是零信网关自动化为用户配置的另一种双 SSL 证书搭配：商密 EV SSL 证书和国际 DV SSL 证书。可以看出：这两张 SSL 证书的有效期也都是 90 天，90 天商密 EV SSL 证书和 90 天国际 DV SSL 证书。



读者朋友可以使用零信浏览器查验，如下图所示，加密锁和 **m** 标识表示采用商密算法实现 HTTPS 加密，**F** 标识表示由零信网关 WAF 提供云 WAF 防护服务，T4 标识和绿色地址栏标识这张商密 SSL 证书是 EV SSL 证书。请同时使用其他浏览器查看国际 SSL 证书，是一张采用 ECC 算法的从 ZoTrus 自有品牌中级根证书签发的 90 天有效期 SSL 证书。



细心的读者朋友可能会注意到：零信网关自动化配置的双 SSL 证书中的国际 SSL 证书是 DV SSL 证书，这是第二段落中全球八大 SSL 证书提供商普遍采用的 SSL 证书类型，因为 DV SSL 证书无需等待 CA 机构的人工身份鉴证就可以自动化签发和实时部署，并且 DV SSL 证书非常适合于政府机关事业单位无法提供身份证明材料和不允许身份数据出境的特别情况。

为何零信网关自动配置的商密 SSL 证书默认为 OV SSL 证书和可选 EV SSL 证书呢？因为 OV SSL 证书和 EV SSL 证书能证明网站可信身份，零信浏览器会在地址栏特别展示单位名称，以防止重要网站被假冒。同时，由于商密 SSL 证书可以实现国内自主签发，只要审核一次完成身份鉴证，后续就可以自动化签发和自动化配置到网关部署使用了。当然，在没有完成身份鉴证之前零信网关临时给用户网站自动配置 90 天有效期的双 DV SSL 证书(商密 DV SSL 证书+国际 DV SSL 证书)。

零信网关不仅为每一个网站自动化配置 90 天有效期的双 SSL 证书，而且是双网关负载均

衡热备配置的每台网关的每个网站都配置唯一的密钥和唯一的双 SSL 证书，所以都是单域证书，而不是传统人工申请和部署 SSL 证书常用的通配域名证书，所有网站共用一个密钥和一张通配证书非常不安全。

零信网关和由零信网关提供的云服务都已经提前准备好迎接即将到来的 90 天证书政策，已经实现自动化配置 90 天证书，不仅能让用户从容应对 90 天证书政策的落地，就算是哪一天变成了每天更换密钥都可以做到。只有这样，才能轻松过渡到抗量子算法，不断提升 HTTPS 加密服务的安全性和敏捷性，轻松帮助用户实现大规模的 SSL 证书部署，零改造完成商密 HTTPS 加密改造，满足用户商密合规、等保合规、密保合规、关保合规和全球信任等网络与通信安全及应用和数据安全的合规要求，快速实现所有互联网政务应用的商密 HTTPS 加密安全连接。

有诗为证：

九十天政策不可怕，关键还是自动化。

双算法自动九十天，零信网关都实现。

王高华

2024 年 6 月 24 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 170 篇(共 46 万 4 千多字)和英文 68 篇(8 万 4 千多单词)。。