第 10 讲 什么是 ACME？什么是国密 ACME？

首先，祝大家节日快乐！上一期我们讲了 SSL 证书是如何可靠地生产出来的，整个 Web PKI 生态是如何通过浏览器的可信根认证计划和证书透明计划来保障 SSL 证书的安全可靠供给的。产品生产出来当然是为了应用，SSL 证书主要用于 https 加密，其整个使用过程是这样：

(1) 用户向 CA 申请 SSL 证书，注册账户、下单付款等

(2) 在 Web 服务器或者在 CA 系统在线生成证书签名请求文件(CSR)，并把 CSR 粘贴到在线申请页面中

(3) 选择以下三种方式验证域名控制权：

a) 文件验证方式：把 CA 提供的验证文件上传到 Web 服务器的指定目录中(/.well-known/pki-validation/)中

b) DNS 验证方式：把 CA 提供的验证码配置到待验证的域名 CNAME 记录中

c) 邮箱验证方式：选择 5 个专用域名管理员邮箱收取 CA 系统发送的验证码，收到后把验证码粘贴到验证页面上提交验证

(4) 完成以上之一的验证后，等待 CA 系统自动签发(DV SSL)或人工签发(IV/OV/EV)SSL 证书

(5) 证书签发后下载并按照各种 Web 服务器的要求配置好证书链后安装部署 SSL 证书

(6) 如果部署国密 SSL 证书，还得安装国密算法支持模块，才能启用国密 SSL 证书

只有经过了以上 5 个或 6 个步骤后才能启用 https 加密或国密 https 加密服务。经测试，工程师完成以上步骤至少需要 1-3 个小时，这是指 DV SSL 证书，如果是其他类型的证书则需要的时间更长。但这只是一个网站域名，如果是 10 个网站？100 个网站？1 千甚至 1 万个网站？相信读者在了解了申请和部署 SSL 证书的过程也就不能理解目前 SSL 证书市场的两个怪现象：

(1) 为何用户喜欢部署通配多域证书？因为多个域名和各种子域名的网站只需申请一次证书就能用这一张证书搞定，解决证书申请过程难的问题。但是，这是非常不安全的证书部署方式，因为一旦一台服务器被黑而需要吊销这张 SSL 证书，会导致所有服务器的证书都需要重新部署！这种方式同时也大大增加了 SSL 证书私钥泄露而带来的安全风险。

(2) 为何那么多的政府网站都没有部署 SSL 证书，因为一个省的政务云平台要管理几千甚至几万个网站，人工部署 SSL 证书根本是不可能做到的事情！不是不想部署 SSL 证书，

而且这个过程太难了。绝对不是经费的问题，是部署难的问题！

所以，要想普及使用 SSL 证书实现 https 加密，人工申请和部署 SSL 证书是做不到的，特别是现在大量的物联网设备也需要部署 SSL 证书。怎么办？ACME 就闪亮登场了！

英文单词“acme”是“顶峰、顶点、最高点”的意思。而在计算机网络界则是一个非常有名的国际标准协议的名称，“**ACME**”是 Automated Certificate Management Environment (**自动化证书管理环境**)的缩写。这是一个 RFC 8555 国际标准，用于自动化申请、部署和续期 SSL 证书，包括 ACME 客户端和 ACME 服务端。目前，全球已经在谷歌证书透明日志系统备案的 SSL 证书总量高达 92 亿张，其中自动化申请和部署的总量已达 81 亿张，占比达到 88%，可见自动化部署 SSL 证书已经在全球范围成为了常态方式，不仅是用户需要简单易用地实现 https 加密，而且大量的物联网设备 https 加密用的 SSL 证书只能是自动化申请和部署。这大概也是证书自动化管理协议作者为何把这个协议命名为“acme”的原因，因为他们相信这是 SSL 证书管理的**终极**解决方案，彻底摆脱人工手动申请和部署 SSL 证书的繁琐，彻底消除因忘了续期 SSL 证书而造成业务系统瘫痪的巨大安全隐患！

那么，ACME 是如何做到的？简单地讲，ACME 就是把以上的 5 个步骤全部实现了自动化当然是用一个程序来实现，那就是 ACME 客户端软件，由这个软件来实现 SSL 证书的在线申请、生成 CSR 文件、提交 CSR 文件到 CA 系统、在 Web 服务器上准备好验证文件后通知 CA 系统来验证(文件验证方式)、CA 系统完成验证后签发证书给 ACME 客户端，ACME 客户端拿到证书后把 SSL 证书和私钥文件放置到 Web 服务器要求的位置即可。整个过程都是由 ACME 客户端同 CA 系统的 ACME 服务端直接对话自动化完成，这个自动化流程遵循 ACME 国际标准 RFC8555，需要 CA 系统改造支持 ACME 协议，提供 ACME API 服务。

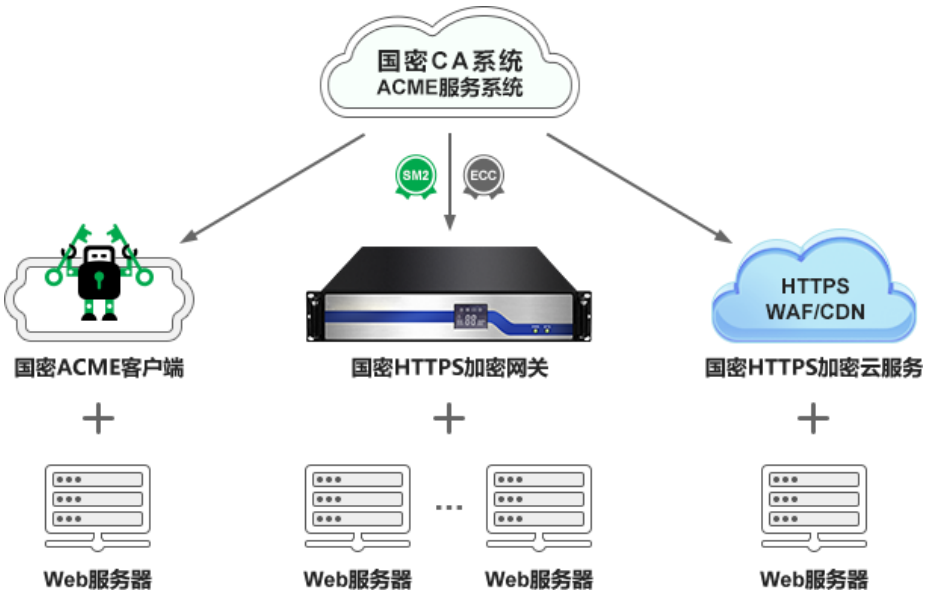
这就是 ACME，一个只用了 3 年时间就成功把欧美网站的 SSL 证书部署率从 40%提升到 80%的大功臣！当然，这个技术也已经开始在我国快速普及中，现在包括清华大学的很多高校官网都已经启用了 ACME 服务来实现自动化证书申请和部署。但是，这个非常好的技术无法用于国密 SSL 证书的自动化部署，这一条普及 SSL 证书的阳关大道只能通向 RSA 算法的 https 加密！

要通向普及国密 SSL 证书实现国密算法的 https 加密的阳关大道，就需要国密 ACME！国密 ACME 系统由零信技术全球率先鼎力打造闪亮登场。这不仅仅是一个自动化证书管理 **环境**(Environment)，而是一个支持国密算法的自动化证书管理 **生态**(Ecosystem)，因为现有的 Web 服务器不支持国密算法，浏览器不支持国密算法，CDN/WAF 不支持国密算法，保障 SSL 证书自身安全的证书透明日志系统不支持国密算法和国密 SSL 证书，要实现国密 https 加密的自动化，需要现有的基于 RSA 密码体系的整个生态系统都支持国密算法。所以，国密 ACME

的 **E** 是 **Ecosystem**(生态系统)的第一个字母，而不是 Environment(环境)的第一个字母。这就是国密 ACME 同国际 ACME 的最关键的不同！

还有两个不同之处：一是国密 ACME 实现的是自动化申请和部署国密 SSL 证书和国际 SSL 证书，双算法双 SSL 证书，而不是单国际算法 SSL 证书，因为目前的 https 加密应用环境还需要双 SSL 证书来实现自适应加密算法的 https 加密，使得用户无论是否使用国密浏览器都可以无缝地实现 https 加密。二是国密 ACME 不是仅仅提供一个 ACME 客户端就能搞定，而是需要同时提供国密算法支持模块。而且还需要提供更多的选择让一些无法安装客户端软件和国密支持模块的 Web 服务器也能实现国密 https 加密。

目前国密 ACME 解决方案主要有三种可选的方案：一是在 Web 服务器上安装国密 ACME 客户端软件；二是在 Web 服务器前面部署国密 HTTPS 加密自动化网关，原 Web 服务器无需安装 ACME 客户端软件，零改造实现国密 https 加密；三是启用国密 HTTPS 加密云服务，原 Web 服务器也无需安装 ACME 客户端软件，只需做 3 次域名解析，完成 CDN/WAF 设置即可零改造实现国密 https 加密。这三个解决方案当然需要国密 CA 系统提供国密 ACME 服务，为客户端软件、网关和云服务提供自动化证书申请和签发服务。



谷歌在 3 月 3 日提出了缩短 SSL 证书有效期为 90 天的计划，明确指出了这是为了进一步推动 ACME 技术的普及应用，促进和提高整个 Web PKI 生态系统的敏捷性、安全性、稳定性和简单性，为下一步轻松过渡到抗量子算法做准备。由此可见，ACME 有多重要，因为用户根本不可能每 90 天就要手动为网站申请和部署 SSL 证书，特别是有多个网站需要部署 SSL 证书的单位！当然，也由此可见推广和普及应用国密 ACME 非常紧迫，这是唯一一个能实现普及应用国密 SSL 证书的技术手段！

关于需要验证身份的 IV/OV/EV SSL 证书的自动化申请和部署，目前的 RFC8555 标准是建

议用户采用绑定 CA 系统账户的方式来实现的。而最新计划更新 ACME 国际标准的 ARI 扩展项(ACME 证书续期信息)不仅可以实现更加灵活地实现证书续期和证书吊销，更是可以用于自动化申请和部署 IV/OV/EV SSL 证书，用户在自动化获取 DV SSL 证书后，CA 系统可以在完成了用户的身份认证后通知 ACME 客户端来重新申请 OV SSL 证书或 EV SSL 证书，使得 OV/EV SSL 证书一样可以分两步实现自动化！

下一讲内容预告 | 第 11 讲 什么是 CDN？什么是 WAF？

本讲将讲解 CDN 和 WAF 在提升 Web 服务性能上的重要作用，当然离不开 SSL 证书，离不开 https 加密，这两个已经普及应用的网络服务将在“90 天证书革命”中发挥新的不可替代的作用。

王高华

2023 年 5 月 4 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。