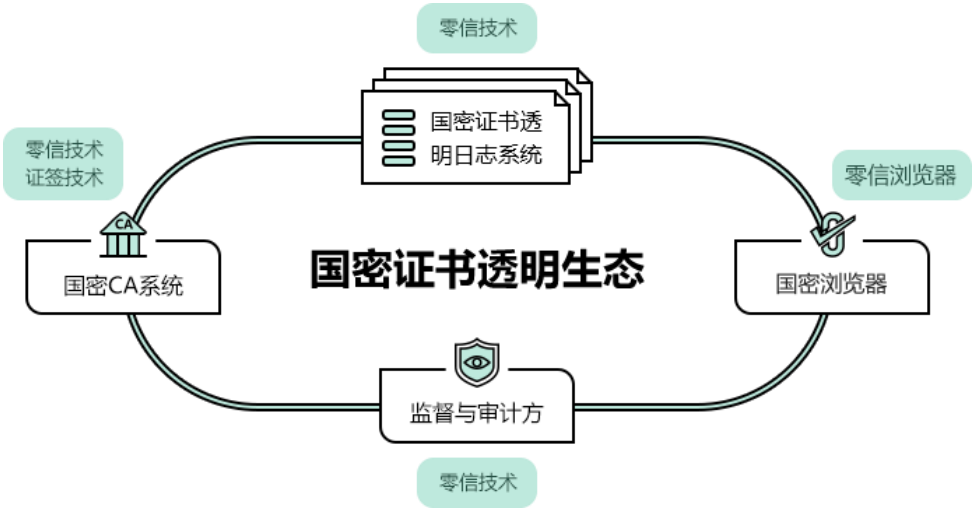
什么是国密 ACME？国密 HTTPS 终极解决方案

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 SSL 证书和自动化部署 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 82 亿张，其中自动化申请和部署的总量已达 70 亿张，占比达到 85%，可见自动化部署 SSL 证书是一个必然的趋势，因为用户需要简单易用地实现 https 加密。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！

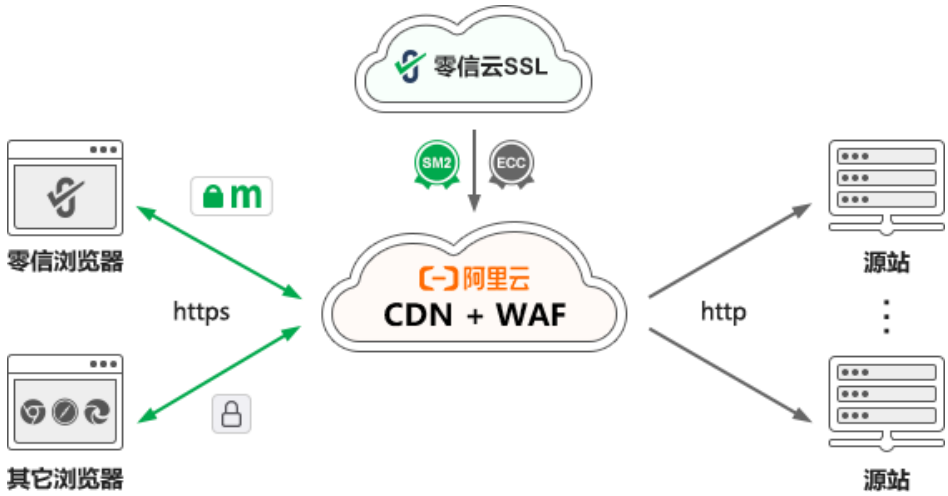
笔者第一次接触到这个标准的英文名称 ACME 时就不能理解为何要用 Environment 这个单词，用 System 不是更确切吗？但如果用了 System, 则英文缩写就是 ACMS，就不是一个通用单词，不方便记忆。而用了 Environment (环境)也说得过去，但好处是缩写变成了 acme (登峰造极，终极)的意思，突显了这个国际标准的技术地位和文学气息。这就让笔者想起了最近很火的发生在深圳的一件大事，结构生物学家颜宁博士从美国回国来深圳创立“深圳医学科学院”，其英文名称是 Shenzhen Medical Academy of Research and Translation，笔者当时就不理解为何后面加了一个 Translation (翻译)，以为是故意要凑成一个高大上的单词 SMART(高明、精明、智慧)硬扯了一个单词，但稍微对结构生物学做了一点点了解后就能理解为何用 Translation 这个生物学单词，很妙，很高明！

回到正题，ACME 国际标准虽好，但仅适用于自动化部署国际算法 SSL 证书(RSA 和 ECC)，不支持自动化部署国密 SSL 证书(SM2)，那我们就无法完全套用这个协议来实现国密 SSL 证书的自动化管理了。要实现自动化管理国密 SSL 证书来实现国密 https 加密，仅仅提供一个自动化证书管理**环境**(Environment)是不够的，需要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，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 同国际标准 ACME 的最关键的不同！

相信关注笔者博客的读者应该已知晓笔者在上个月初的乌镇 2022 世界互联网大会上全球独家创新发布了国密证书透明全生态产品，这些产品是零信技术联合证签技术经过将近两年时间打造出的国密 SSL 证书应用生态核心产品，实现了同国际 SSL 证书一样的国密 SSL 证书的全生命周期的国密算法支持，包括全球首个支持国密算法的国密证书透明日志系统、全球首个能签发支持国密证书透明的国密 SSL 证书的 CA 系统、全球首个支持国密证书透明的国密浏览器。



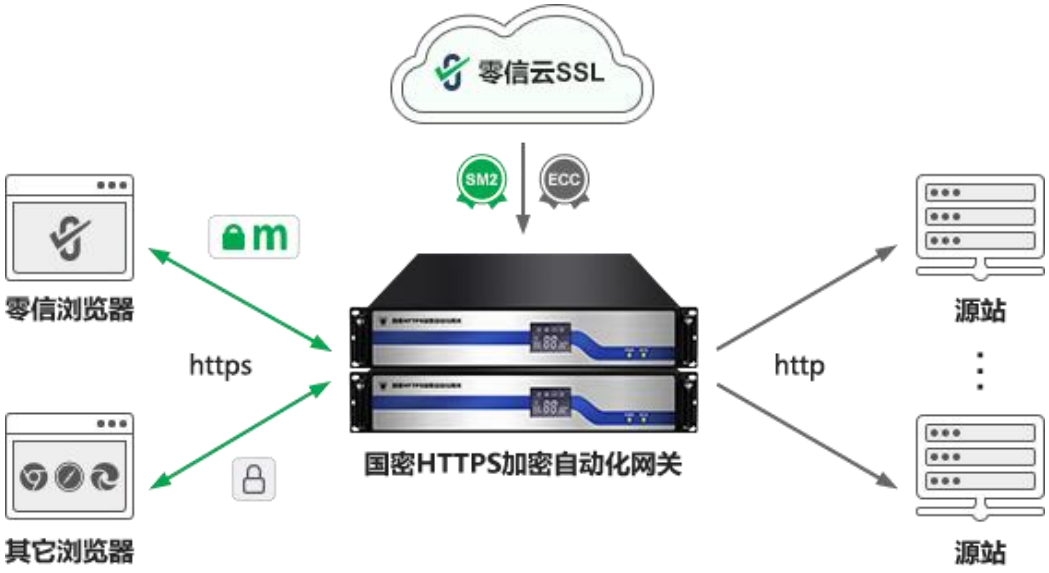
而同时在乌镇发布的一个创新云服务是零信网站安全云服务，这是一个典型的自动化证书管理实现 https 加密的解决方案，一个零改造实现国密 https 加密的解决方案，用户无需手动人工向 CA 申请 SSL 证书，无需在 Web 服务器上安装 SSL 证书，只需做 3 次域名解析就能零改造实现国密 https 加密，自适应加密算法，支持国际算法实现 https 加密，并且同时实现云 WAF 防护、CDN 分发和网站可信认证，这是一个四维的网站安全全方位保障解决方案。



而本次国密 ACME 解决方案的发布，是在国密证书透明生态的基础上继续创新打造了一个国密证书自动化管理生态，这个生态系统中有国密证书透明生态中的产品：国密 CA 系统(零

信云 SSL 系统)、国密 CA 系统签发的双算法双 SSL 证书、国密证书透明日志系统和支持国密证书透明和国密算法的浏览器，新增加的产品有国密 ACME 客户端、国密 ACME 服务系统和国密 HTTPS 网关。这六大国密证书自动化管理生态产品自成体系，形成了一个可以实现全自动国密 https 加密的应用生态，让网站系统能全自动实现 https 加密，满足不同用户的国密合规和全球信任的网站安全应用需求。

本次上线的国密证书自动化管理生态除了参考国际 ACME 标准一样有国密 ACME 服务端和完全免费的国密 ACME 客户端软件-SM2cerBot 外，我们还创新地发布了国密 HTTPS 加密自动化网关，这是为了解决政务系统和大型企业管理系统无法在正在运行的 Web 服务器上安装 ACME 客户端的难题而设计，一个集 https 加密响应、https 卸载转发、国密算法模块、SSL 证书自动化、负载均衡等多项功能于一体的高性能网站安全硬件网关设备，同零信网站安全云服务一样，无需改造原 Web 服务器就可以实现国密 https 加密，但又满足了这类用户希望本地化部署系统而不依赖于云服务的自主可控管理需求。



相信看完本文的读者一定能体会到我们的解决方案的独到创新之处，为了让广大用户能根据自己的业务需要选择适合自己的国密证书自动化管理解决方案，特在最后总结如下四点：

第一，要实现国密 https 加密，无法简单照搬国际 ACME 标准，必须有创新改造，必须有一个国密证书自动化管理**生态**，而不是简单的一个**环境**。

第二，用户可以在 Web 服务器上安装完全免费的国密 ACME 客户端软件-SM2cerBot，自动化配置完全免费的 90 天有效期或收费的 1 年期的国密 SSL 证书和国际 SSL 证书，自动化安装国密算法模块，自动化实现国密 https 加密和自适应加密算法的国际算法 https 加密。不仅实现了同其他国际 ACME 客户端软件一样的自动化部署 SSL 证书的功能，而且实现了自动化国密改造，实现了双算法双 SSL 证书的自动化管理。

第三，对于无法在 Web 服务器上安装国密 ACME 客户端软件的用户，则可以选择在现有 Web 服务器之前部署即插即用的已经内置了国密 ACME 客户端的国密 HTTPS 网关，一样可以实现零改造原服务器的国密 https 加密，确保了政务系统和大型企业管理系统能无缝从 http 到 https 和国密 https 的平滑稳定升级。

第四，对于既不想也不能在现有服务器上安装 ACME 客户端软件，又不想购买和本地部署硬件网关设备的用户，则更简单的方案就是选用零信网站安全云服务，只需做三次域名解析，零信云 SSL 系统会自动化配置双 SSL 证书到阿里云 CDN+WAF 系统中，把原网站变成 CDN+WAF 的源站即可，更加低成本和更加轻松地完成国密 https 加密改造，轻松地同时实现 https 加密、云 WAF 防护、CDN 分发和网站可信认证四位一体的网站安全全方位保障。

王高华

2023 年 1 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。