内网 SSL 证书自动化的核心是自给自足

2025 年 12 月 1 日

笔者在多篇博文详细介绍了公网 SSL 证书自动化管理和自动切换多 CA 签发通道，这是公网 SSL 证书自动化管理的核心。本文讲一讲内网 SSL 证书自动化管理，其核心要点是自给自足。

一、 内网流量急需 HTTPS 加密，急需内网 SSL 证书和证书自动化

由于内网 IP 地址和主机名无法验证，所以，国际标准和国密标准都是禁止公共信任的 CA 签发内网 SSL 证书。但是，内网处理的都是不能连接公网的机密信息，这些机密信息更需要 HTTPS 加密保护。所以，内网管理员们只好自建内部 CA 系统，自己签发浏览器不信任的 SSL 证书。

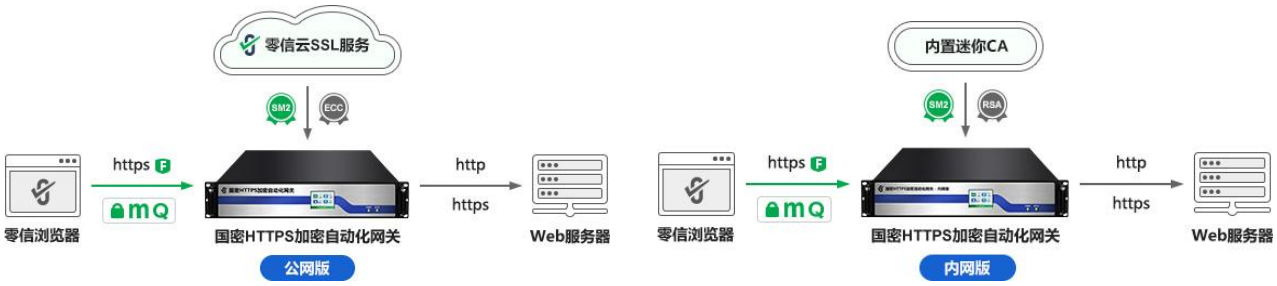
随着内部管理系统越来越多，同时随着公网 SSL 证书有效期的不断缩短，内网 SSL 证书也需要实现自动化管理，内网也需要实现国密 HTTPS 加密，内网 HTTPS 加密也需要支持后量子密码算法。但是，公网所采用的 SSL 证书自动化管理解决方案无法用于内网 SSL 证书自动化管理，因为公网 SSL 证书自动化管理需要通过互联网连接到证书签发 CA 的证书自动化管理服务系统。怎么办？

二、 内网 SSL 证书自动化管理的核心是自给自足

正是由于内网无法连接互联网，所以，要想实现 SSL 证书自动化，那只有自建 CA 系统升级支持证书自动化，同时内部 Web 服务器也要支持证书自动化。也就是说，为了实现内网 SSL 证书自动化，用户需要复制建设一套同公网 SSL 证书自动化一样的系统，这个投入太大和大大增加了内部系统管理工作，不是一个好的解决方案。

由于内网无法连接公网获得公网 SSL 证书自动化管理的所有资源，那就只有实现自给自足一条路可走了。但是，投资建设整套证书自动化管理系统费用太高，并且管理复杂，零信技术正是充分认识到用户的难处，在完成了公网 SSL 证书自动化管理解决方案后继续研发完成了内网 SSL 证书自动化管理解决方案，那就是把公网的用户端(零信浏览器)—云端(零信云 SSL 服务系统)—服务端(零信国密 HTTPS 加密自动化网关)为一体的公网 SSL 证书自动化管理解决

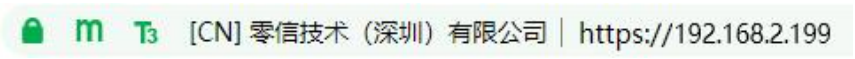
方案(如下左图所示)衍生出内网的用户端(零信浏览器)—服务端(零信国密 HTTPS 加密自动化网关内网版+内置迷你 CA 系统)为一体的内网 SSL 证书自动化管理解决方案(如下右图所示)。



这就是零信技术在实现了公网 SSL 证书自动化管理的基础上打造的内网 SSL 证书自动化管理解决方案，不需要连接外部 CA 系统，也不需要投资建设复杂的内部 CA 系统，直接在内网网关上集成迷你 CA 系统，实现双算法内网 SSL 证书的自给自足，这才是最优解决方案。

零信技术的创新解决方案不仅实现了内网 SSL 证书的自给自足，而且还解决了用户投资建设自用 CA 系统的根证书浏览器不信任难题，零信浏览器不仅是完全免费的支持商用密码算法和后量子密码的通用浏览器，而且还预置信任了用于零信内网网关自给自足签发双算法 SSL 证书的内网 SSL 证书根证书，彻底解决了内网 SSL 证书的浏览器信任难题。零信技术为每台内网网关定制了两个用户品牌名称(如：Abcdef)的零信浏览器信任的中级根证书(SM2/RSA)，分别用于自动化签发 SM2 和 RSA 算法内网 SSL 证书，证书主域默认绑定已验证的用户域名，可以自动签发已验证的主域名的子域名 SSL 证书、内网 IP 地址证书和内部域名 SSL 证书。每台内网网关最多支持 510 个内网网站，自动配置的双算法 SSL 证书(国密 OV SSL 证书+国际 OV SSL 证书)完全免费，双算法 SSL 证书的证书链如下图所示。

零信浏览器在地址栏显示内网网站的单位名称，让用户确信访问的是本单位内网网站，如下左图所示。当然，用户也可以使用其他浏览器(如谷歌浏览器)使用 RSA 算法实现内网 HTTPS 加密，其他浏览器信任零信内网网关签发的 RSA 算法内网 SSL 证书，如下右图所示。



零信国密 HTTPS 加密自动化网关(内网版)除了自动配置是内网 SSL 证书外，其他功能同

公网版网关，一样同时支持国密算法、国际算法和后量子密码算法，满足用户内网系统的国密合规、兼容国际算法和后量子密码迁移应用需求，是保障内网流量安全的最佳解决方案。

三、 配置自签 SSL 中级根证书，满足特殊应用需求

为了满足有些用户的内网使用的是公网 IP 地址的特殊应用需求，零信内网网关还为用户设立了另外两个用户品牌的零信浏览器不信任的自签根(**Intranet SM2 Root** 和 **Intranet RSA Root**)签发的中级根证书(SM2/RSA)，用于自动化签发绑定无法验证的公网 IP 地址和公网域名的内网 SSL 证书。

根据零信浏览器内网 SSL 根证书信任规则，零信浏览器仅预置信任签发合规的内网 IP 地址和内部域名的内网 SSL 证书的内网根证书。所以，要想为公网 IP 地址或公网域名签发内网 SSL 证书只能从零信浏览器不信任的根证书签发了。这就等于零信内网网关免费为用户提供了一个浏览器不信任的自建 CA 系统用于任意签发所需的内网 SSL 证书，这是零信内网网关免费赠送给用户的一个实用的迷你自建 CA，解决了用户内网使用公网 IP 地址的难题，使得这些用户一样可以实现内网 SSL 证书自动化管理。

由于零信浏览器不信任这两个自签根签发的内网 SSL 证书，需要用户手动安装信任 RSA 根证书，这样常用的浏览器就能信任部署了自签根签发的 RSA 算法内网 SSL 证书。如果需要支持国密算法，则需要手动导入 SM2 根证书到零信浏览器的证书管理器-本地证书-自定义中，零信浏览器将信任自签根签发的 SM2 算法内网 SSL 证书。这两个自签根签发的内网 SSL 证书的证书链如下图所示，中级根名称同零信浏览器信任的根签发的中级根名称命名规则一致，只是后面多了一个字母 S。

四、 内网流量更需要 HTTPS 加密，唯有自给自足才是终极解决方案

公网 SSL 证书自动化管理的英文是 ACME，这个英文单词是“顶峰、终极”的意思，意思是这是终极解决方案。但是，这个解决方案解决不了内网 SSL 证书自动化难题。零信技术的内网 SSL 证书自动化解决方案实现了内网 SSL 证书的自给自足和自动化，这才是内网 SSL 证书自动化的终极解决方案。不仅解决了合规内网 SSL 证书的自动化签发难题，而且解决了浏览

器的信任难题，同时还解决了我国许多大型单位内网不规范使用公网 IP 地址而导致的内网 SSL 证书申请难题，让用户无需投资巨款建设内部 CA 系统，只需部署零信内网网关即可自动化实现内网流量 HTTPS 加密保护，满足用户国密合规、兼容国际算法和后量子密码迁移的应用需求。

王高华

2025 年 12 月 1 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 240 篇(共 71 万 5 千多字)和英文 103 篇(14 万 1 千多单词)。