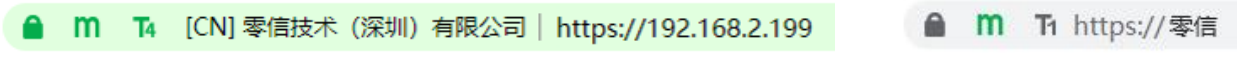
内网 SSL 证书，内网 Web 安全必配

内网就是单位内部网络，但是实际上，很多大单位已经是一个跨城市的广域网，至少也是一个园区跨楼的大局域网，或者是一个同一栋楼跨楼层的内部局域网。这些大单位一般都是重要的关键信息基础设施运营单位，内网 Web 服务器上有大量的内部办公机密信息，这些大量的机密信息都是使用 HTTP 明文传输，非常容易在办公室电脑、楼层交换机或跨楼交换机中被非法采用包侦听软件窃取所有机密信息！内网流量实现 HTTPS 加密必须尽快提上日程！美国 2022 年 1 月 26 日发布的《联邦政府零信任战略》明确要求所有内网流量都必须采用 HTTPS 加密，这非常值得我国借鉴。

但是，实现内网流量的 HTTPS 加密需要 SSL 证书，而按照国际标准，严格要求 CA 不允许给内网 IP 地址签发 SSL 证书，因为内网 IP 地址谁都可以用，CA 无法验证。这使得内网系统根本无法申请到全球信任的 SSL 证书，大家只好部署自签证书，但是自签证书浏览器提示不信任，如果让内网用户点击信任，则非常容易因为证书警告的惯性忽略而遭遇假冒网站证书的恶意攻击。常见解决方案是把自签证书的根证书安装到所有内网用户电脑中去。所有这些都是内网实现 HTTPS 加密的技术障碍，导致只好任其采用 HTTPS 明文传输方式使用各种重要的内部管理信息系统，只能在心里祈祷不会发生内网机密数据泄露事件的发生。

我国《密码法》、《网络安全法》、《数据安全法》等多个法律法规都要求关键信息基础设施系统都必须采用商用密码来实现信息加密，保障重要机密数据的安全。这些合规要求和内网 HTTPS 加密的技术障碍形成了一个很难解决的矛盾，急煞了信息主管们！怎么办？今天上线的证签内网 SSL 证书由证签技术和零信技术联合鼎力打造，给出了一个完整的创新解决方案。

先看看我们的创新方案的效果，如下图所示，192.168.2.199 是一个内网 IP 地址，“零信”是一个中文主机名，证签内网 SSL 证书支持此内网 IP 地址和主机名，把这张内网 SSL 证书部署在 Web 服务器上后，用零信浏览器访问，则采用 SM2 算法实现 HTTPS 加密和显示““m”国密加密标识，零信浏览器信任这张内网 SSL 证书。左图为内网 EV SSL 证书显示效果，右图为内网 DV SSL 证书显示效果。

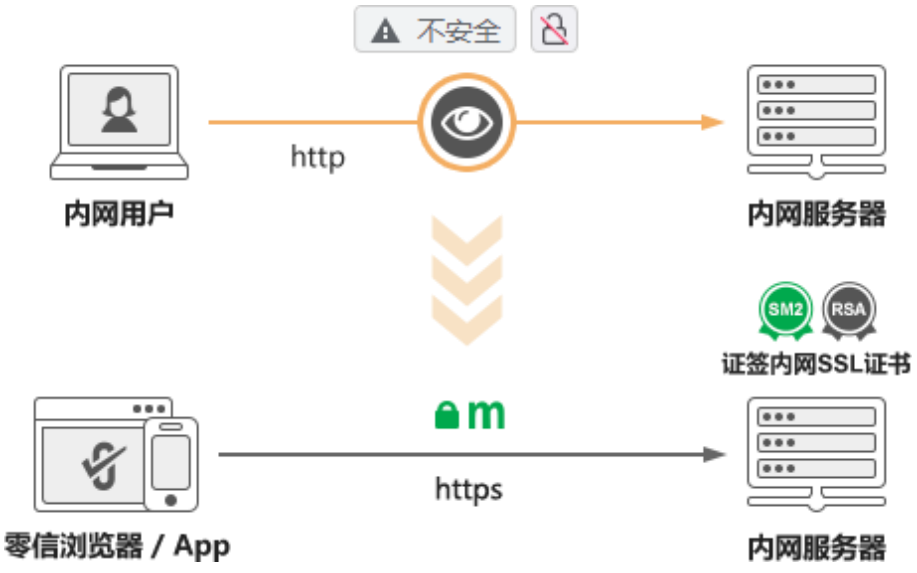


证签内网 SSL 证书同公网 SSL 证书一样也是双算法双 SSL 证书，如下左图所示，使用谷歌浏览器访问同一网站，信任并正确实现 HTTPS 加密，支持内网 I 地址和内部主机名。如下右图所示，使用微软 Edge 浏览器访问，信任并正常显示加密锁标识。谷歌浏览器和 Edge 浏览器采用 RSA 算法实现 HTTPS 加密。

证签技术和零信技术是如何做到的呢？是如何解决这个技术难题的呢？

要解决内网 Web 流量加密问题，首先必须解决内网 SSL 证书的供给问题，证签技术专门创建了内网专用国密 SM2 算法和国际 RSA 算法根证书和升级了证书签发系统，用于签发双算法内网 SSL 证书，这个内网 SSL 证书签发系统可以给内网 IP 地址、内部域名和主机名签发国密 SM2 SSL 证书和国际 RSA SSL 证书，证书有效期可以是 1-5 年，用户可以选购 5 年有效期的 SSL 证书，实现 5 年内不用重新换证书的不间断的 HTTPS 加密，可以是 RSA HTTPS 加密，如果内网服务器无法国密改造支持国密算法的话；推荐实现国密 HTTPS 加密，如果内网服务器支持升级改造支持国密算法的话，满足密保合规和等保合规要求。

内网 SSL 证书的供给问题解决了，但这只是解决了一半，因为这个内网 SSL 证书的 SM2 根证书和 RSA 根证书和并不是常用浏览器信任的，浏览器仍然有不安全警告，所以全面解决问题还得有浏览器信任内网 SSL 证书。零信浏览器就可以发挥大作用了，零信浏览器已经预置信任证签国密 SM2 算法和国际 RSA 算法的两个内网专用根证书，能正常显示这两个内网根证书签发的内网国密算法 SSL 证书和内网 RSA 算法 SSL 证书，没有安全警告地正常验证和显示加密锁标识，在浏览器地址栏展示 OV SSL 证书和 EV SSL 证书的单位信息，让用户像使用公网 HTTPS 加密一样在内网轻松实现 HTTPS 加密，保障内网 Web 流量安全。



零信浏览器不仅信任证签内网 SSL 证书，而且是完全免费的支持国密算法的国产国密浏览器，有 Windows 版本和国产操作系统麒麟和统信版本(即将推出)，完全免费，使得内网用户实现一举两得，一得是实现了可信的内网 HTTPS 加密，有力保障了内网 Web 流量安全；二得是用户无需花钱购买国密浏览器就实现了内网的国密合规。用户需要做的只是申请和部署一张 5 年期内网 SSL 证书，给每台内网电脑免费安装零信浏览器即可。一旦安装了零信浏览器，则其他浏览器也同时信任证签内网 RSA 算法 SSL 证书，用户仍然可以使用这些浏览器访问内网 Web 系统，这是第三得。

内网 Web 安全需要内网 SSL 证书，同时需要信任内网 SSL 证书的国密浏览器。证签内网 SSL 证书加完全免费的国密浏览器—零信浏览器完美解决内网 HTTPS 加密难题，助力内网用户彻底解决内网数据明文传输的安全隐患，助力用户用国密 HTTPS 加密来保障内网机密数据安全。

欢迎选用 证签内网 SSL 证书 和 免费 下载 使用零信浏览器。

有诗为证：

内网明文流量，急需加密。
内网证书，加密内网流量。
零信浏览器信任内网证书，
自动优先国密加密保安全。

王高华

2024 年 4 月 22 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 157 篇(共 42 万多字)和英文 62 篇(7 万 4 千多单词)。