内网 SSL 证书首选 OV SSL 证书

内网 SSL 证书是指为内网 IP 地址和内部域名签发的 SSL 证书，大家常用的 SSL 证书是公网 SSL 证书，这个全球信任的公网 SSL 证书是不被允许绑定内网 IP 地址和内部域名的，因为内网 IP 地址和内部域名无法验证所有权和使用权。本文讲一讲内网 SSL 证书同公网 SSL 证书有什么不同，如何选择合适的内网 SSL 证书。

一、 内网 SSL 证书和公网 SSL 证书有什么不同？

内网 SSL 证书是指绑定内网 IP 地址和主机名的仅用于内网 Web 服务器实现 HTTPS 加密的 SSL 证书。而公网 SSL 证书则是指绑定公网域名和公网 IP 地址的用于公网 Web 服务器实现 HTTPS 加密的 SSL 证书，大家经常说的 SSL 证书一般都是指公网 SSL 证书。

内网大家一般都会认为是一个安全的网络，因为仅限于有限内部人员访问，所以，其内部业务管理系统一般都没有启用 HTTPS 加密。但是，现在是万物互联时代，一切业务都实现无纸化管理，原先的内网已经成为了一个内联网，一个覆盖范围很广的网络。大的内网如国家政务外网是一个覆盖全国各部委和各省市的国家级大网，小的内网如医院管理信息系统，这是一个覆盖整个医院大楼到每个科室、每台智能终端设备的一个内部网络系统，这些内网的数据流如果是 HTTP 明文传输流通，则非常容易被非法窃取和非法篡改，必须同公网网站一样部署 SSL 证书实现 HTTPS 加密。

但是，目前国际标准不允许全球信任的公网 SSL 证书绑定内网 IP 地址，因为 CA 无法验证谁都可以使用的内网 IP 地址，所以才有了内网 SSL 证书这个能绑定内网 IP 地址的新产品。这就是内网 SSL 证书和公网 SSL 证书的唯一不同之处。

二、 内网 SSL 证书是如何验证内网 IP 地址的？

内网管理员自己签发的自签 SSL 证书用于内网 HTTPS 加密，这不是一个产品，只是一个用于保障内网流量安全的技术手段。内网 SSL 证书要想成为一个产品，必须有其价值，正如公网 SSL 证书有其价值大家都愿意付钱购买一样。

内网 SSL 证书的价值同公网 SSL 证书一样在于浏览器信任，没有不安全警告，用户无需手动信任网站部署的 SSL 证书。国际标准之所以不允许签发绑定内网 IP 地址的 SSL 证书，是因为无法验证绑定的内网 IP 地址。零信技术创新解决了这个难题，那就是：SSL 证书中的公

用名称(CN 字段)必须绑定可验证的公网域名，而内网 IP 地址和主机名绑定在 SAN 字段，无需验证，因为无法验证。所以，用户在申请证签内网 SSL 证书时要求同申请公网 SSL 证书一样必须完成域名控制权验证，完成了证书绑定的公网域名验证，说明用户可以控制这张证书的私钥，用户就可以任意添加内网 IP 地址和主机名，不用验证。这就完美地解决了内网 IP 地址无法验证的难题，这是一个全球业界都没有解决的难题，零信技术全球率先创新解决了。

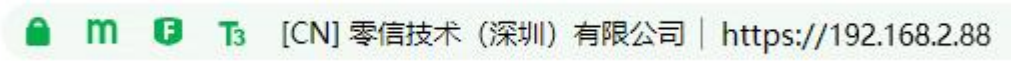
用户了解了这个核心要点后，用户就不会在申请证签内网 SSL 证书时反复询问客服为何申请内网 SSL 证书时必须填写公网域名并完成验证了。因为这是唯一可以使用的能证明用户控制证书密钥的方法，并且采用符合国际标准的验证方式完成验证。零信技术抓住了 SSL 证书签发的核心是验证用户证书密钥控制权，内网 SSL 证书也只要完成这个控制权的验证，CA 就可以安全可靠地为用户签发内网 SSL 证书。

三、 为何内网 SSL 证书首选 OV SSL 证书？

为了区分公网 SSL 证书和内网 SSL 证书，也为了满足公网根证书不能签发内网 SSL 证书的合规要求，零信技术专门设立了独立的内网专用 RSA 算法和 SM2 算法根证书，用户可在线申请的证签内网 SSL 证书的双算法根证书为：CerSign Intranet SM2 Root 和 CerSign Intranet RSA Root，零信内网网关自动配置的双算法 SSL 证书的双算法根证书为：AAA Intranet SM2 Root 和 AAA Intranet RSA Root，之所以取一个中立的根证书名称，是为了为其他有兴趣定制内网 SSL 中级根证书用于销售其自己品牌的内网 SSL 证书的合作伙伴设计一个中立名称，因为浏览器信任的内网 SSL 证书是一个新的 SSL 证书市场，一个比公网 SSL 证书更广阔的新兴市场，一个还未开垦的黄金市场。

内网 SSL 证书同公网 SSL 证书一样，也分为内网 DV SSL 证书、内网 OV SSL 证书和内网 EV SSL 证书，由于内网 SSL 证书仅内部用户使用，就不再需要增强信任的 EV SSL 证书了，所以不在首选之列。至于仅验证域名所有权的内网 DV SSL 证书，由于证书中不含单位名称信息，仅凭内网 IP 地址也无法判断所属单位，不利于内网用户辨识内网系统的真实单位身份，也不在推荐之列。

内网 HTTPS 加密首选和推荐的是含单位名称的 OV SSL 证书，因为内网 IP 地址谁都能用，只有单位名称是唯一能标识这个内部网站的身份信息的，这样，内网用户使用零信浏览器访问该内网系统时会在地址栏显示单位名称，方便用户识别正在访问的内网系统的真实身份信息，这就是首选内网 OV SSL 证书的主要原因。也就是说，内网 SSL 证书公用名称(CN 字段)的公网域名用于验证用户对内网 SSL 证书密钥的控制权，而证书 O 字段的单位名称则是证明这个内网 Web 系统身份的唯一标识。



四、 零信内网国密 HTTPS 加密自动化网关默认配置双算法 OV SSL 证书

为了实现内网 SSL 证书也能像公网 SSL 证书一样的自动化申请和自动化部署，零信技术创新地推出了内网国密 HTTPS 加密自动化网关，这也是全球首创，是一个能自动化为内网网站申请和部署使用内网 SSL 证书的硬件网关设备，自动化配置的双算法 SSL 证书是双 OV SSL 证书，绑定网关用户单位名称，内网用户既可以用公网域名 HTTPS 访问内网系统(必须解析到内网 IP 地址)，也可以直接使用内网 IP 地址访问，还可以使用主机名访问，不仅零信浏览器信任并在地址栏展示单位名称，其他常用浏览器也信任，实现自适应密码算法的最大兼容。

零信内网网关自动化配置的双算法 OV SSL 证书不是一年期或者多年期证书，而是 90 天有效期的 OV SSL 证书，最多支持为 510 个内网网站系统自动化配置双算法内网 SSL 证书，每个网站都是独立密钥和独立证书，每 80 天更新一次密钥和证书，确保内网 SSL 证书能满足即将到来的同公网 SSL 证书一样的 90 天有效期安全策略，有力保障内网 HTTPS 加密安全。

王高华

2025 年 4 月 21 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 210 篇(共 62 万 1 千多字)和英文 91 篇(12 万 1 千多单词)。