内网 SSL 证书可信根认证计划，共同保障内网流量安全

所谓内网，就是不能通过公网访问的单位内部网络，内网有许多 Web 系统仅限于内网用户访问，大家往往认为在内网访问是安全的，无需 HTTPS 加密。但是，对数据安全有更高要求的政府单位和大型企业 IT 主管们已经认识到内网 Web 系统也需要 HTTPS 加密，也就是需要申请 SSL 证书和部署 SSL 证书来实现 HTTPS 加密。

但是，国际标准不允许 CA 机构签发包含内网 IP 地址和内部名称的 SSL 证书，因为此类名称和 IP 地址无法根据相关验证标准进行验证。也就是说 SSL 证书如果绑定了谁都可以随便使用的内部 IP 地址，CA 无法验证用户对这个内部 IP 地址的控制权和使用权，无法验证就不能签发包含这个 IP 地址的 SSL 证书，这是签发 SSL 证书的基本要求。怎么办？大家只好用自签证书，而自签证书所有浏览器都不信任，会有安全警告，用户只好忽略安全警告而信任自签证书，但是这个习惯一旦养成，则会给假冒网站使用自签证书埋下了安全隐患，这也不是一个好办法。怎么办？

零信技术提出了一个创新解决方案，不仅已经开始签发证签品牌内网 SSL 证书，而且零信浏览器信任签发此内网 SSL 证书的 RSA 算法根证书和 SM2 算法根证书，使得用户可以无缝地使用内网 SSL 证书实现内网 Web 流量的 HTTPS 加密。同时，我们把这个解决方案分享给全球 CA 机构，让全球 CA 机构都能为其用户签发有浏览器信任的内网 SSL 证书，彻底帮助用户从自签 SSL 证书的浏览器安全警告的困境中解脱出来，不仅解决了用户的难题，而且也给 CA 机构带来了新的利润增长点。

1. 什么是内网 SSL 证书？

内网 SSL 证书是指 SSL 证书的“使用者可选名称(Subject Alternative Name)”字段包含了内部名称和/或保留 IP 地址的 SSL 证书，内部名称和保留 IP 地址(或称内网 IP 地址、内部 IP 地址)遵循 SSL 证书基线要求国际标准 BR 1.6.1 中的定义。

(1) 保留 IP 地址：包含在任一 IANA 注册管理机构中任何条目的地址块中的 IP v4 或 IP v6 地址。

(2) 内部名称：SSL 证书的“公用名称”或“使用者可选名称”字段中的一串字符（不是 IP 地址），在颁发证书时无法验证为公共 DNS 中的全局唯一，因为它不以在 IANA 根区数

据库中注册的顶级域名结尾。简单讲就是指非公网域名。

2. 内网 SSL 证书的基线要求

国际标准为何不允许 CA 签发内网 SSL 证书，就是因为无法验证。零信浏览器是如何解决这个难题的呢？零信技术经过深入研究和实际证书签发实验，制定了如下的内网 SSL 证书基线要求。

(1) 内网 SSL 证书的“使用者(Subject)”字段或称“公用名称(Common Name)”必须是公网域名(FQDN)，不得包含内部名称或保留 IP 地址，此公网域名用于 CA 验证此内网 SSL 证书的所有权，CA 必须按照国际标准 TLS BR 的第 3.2.2.4 节或第 3.2.2.5 节要求完成域名控制权验证。这个要求解决了内网 SSL 证书包含的内网 IP 地址无法验证的问题。

(2) 内部名称或保留 IP 地址只能包含在 SSL 证书的“使用者可选名称”字段中，CA 无需验证这些内部名称和保留 IP 地址。但 CA 必须依据 TLS BR 标准验证“使用者可选名称”字段中所有包含的公网域名和公网 IP 地址。这个要求就解决了内网 SSL 证书如何包含内部名称和保留 IP 地址的问题。

(3) 内网 SSL 证书有效期可以是 1-5 年。这个也是考虑到内网是相对比较安全的仅供内部人员访问的系统，有内网安全防护系统的保护，能确保证书私钥在 5 年内使用是安全的。这就大大方便了用户一次安装 SSL 证书，5 年内都不用再去费力向 CA 申请和安装 SSL 证书。

(4) 鉴于目前只有零信浏览器信任的 3 个证书透明日志系统支持内网 SSL 证书，证书有效期小于或等于 180 天的内网 SSL 证书必须包含 1 个零信浏览器信任的证书透明 SCT 数据，大于 180 天的内网 SSL 证书必须包含 2 个 SCT 数据。如果以后市场上有更多的证书透明日志系统支持内网 SSL 证书，并通过零信浏览器认证和预置信任，则更新实施内网 SSL 证书证书透明策略同公网 SSL 证书政策。

(5) 内网 SSL 证书其他技术要求同公网 SSL 证书相关国际标准和国密标准。

3. 零信浏览器是如何验证内网 SSL 证书的？

如果只是 CA 能签发内网 SSL 证书而没有浏览器信任是行不通的，还需要有浏览器像处理公网 SSL 证书一样严格验证内网 SSL 证书，不仅有内网 SSL 证书信任根认证计划，最关键的是必须像公网 SSL 证书一样的支持证书透明，向全球公示每一张签发的内网 SSL 证书，只

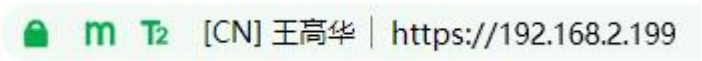
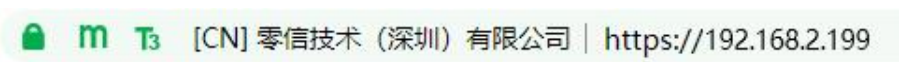
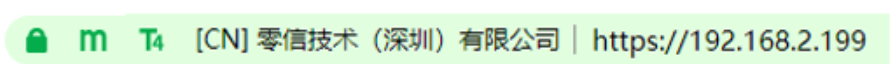
有这样才能保障内网 SSL 证书的自身安全可信。

所以，零信浏览器不仅有内网 SSL 证书信任根认证计划，制定了签发内网 SSL 证书的基线技术要求，而且免费开放零信国密证书透明日志系统给所有通过认证的 CA 机构，使其能像签发公网 SSL 证书一样提交预签证书到证书透明日志系统获取证书透明日志签名数据，并把日志签名数据写入到内网 SSL 证书中，让全球用户可以像监督公网 SSL 证书签发行为一样监督内网 SSL 证书的签发行为。零信浏览器只信任内嵌了零信浏览器信任的证书透明日志系统签名的 SCT 数据的内网 SSL 证书，保障所有内网 SSL 证书用户的合法权益。

由于谷歌浏览器信任的证书透明日志系统不支持内网 SSL 证书，所以，CA 目前只能使用零信国密证书透明日志系统，日志签名算法采用 SM2 算法，CA 机构无论是签发 RSA/ECC 算法 SSL 证书还是 SM2 算法 SSL 证书，都提交到采用 SM2 算法的证书透明日志系统获取日志签名数据。CA 如果不知道如何解析返返回的 SCT 数据，也可以不用关心，只需把 SCT 数据写入证书中即可。当然，在正式颁发内网 SSL 证书之前，必须部署内网 SSL 证书并使用零信浏览器访问是否可信和是否正常解析和显示证书透明日志信息。如下左图所示，零信浏览器显示 SSL 证书的算法为 SM2，证书透明日志签名算法为 SM2，这表明这张 SM2 内网 SSL 证书已经正确内嵌 SM2 签名 SCT 数据。如下右图所示，零信浏览器显示 SSL 证书的算法为 RSA，证书透明日志签名算法为 SM2，这表明这张 RSA 内网 SSL 证书已经正确内嵌 SM2 签名 SCT 数据。

零信国密证书透明日志系统同时支持 RSA、ECC 和 SM2 三种算法的 SSL 证书，零信技术不计划单独为 RSA/ECC 算法内网 SSL 证书设立一个 ECC 算法的证书透明日志系统，统一使用零信国密证书透明日志系统。欢迎 CA 机构运营一个专用于内网 SSL 证书的 ECC 算法证书透明日志系统，零信浏览器将在测试合格后快速预置信任，这样全球 CA 签发的 RSA/ECC 算法内网 SSL 证书有 ECC 算法证书透明日志系统可用了。

零信浏览器除了验证内网 SSL 证书是否可信、是否支持证书透明外，还会根据不同的证书类型展示不同的地址栏 UI。但是，用于公网 SSL 证书的证书类型国际 OID 无法用于内网 SSL 证书，所以，零信浏览器指定了 4 个 OID 用于分别标识内网 SSL 证书类型，具体如下表所示。如果内网 SSL 证书中不包含这些证书类型 OID，则默认 UI 为内网 DV SSL 证书，显示 T1 认证标识。

证书类型	证书类型 OID	零信浏览器地址栏 UI 展示效果
DV SSL	1.2.156.157933.81	
IV SSL	1.2.156.157933.82	
OV SSL	1.2.156.157933.83	
EV SSL	1.2.156.157933.84	

4. 欢迎全球 CA 申请内网 SSL 证书可信根认证计划，共同保障全球内网 Web 流量安全。

内网流量安全需要内网 SSL 证书，更需要有浏览器信任 CA 签发的内网 SSL 证书，也需要有签发内网 SSL 证书的基线要求，这就是零信浏览器内网 SSL 证书可信根认证计划。

欢迎全球 CA 申请 零信浏览器内网 SSL 证书可信根认证，预置内网 SSL 证书专用根证书(RSA/ECC/SM2)，为全球用户签发内网 SSL 证书，共同保障全球用户的内网 Web 流量安全。

王高华

2024 年 4 月 24 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 160 篇(共 42 万 8 千多字)和英文 65 篇(7 万 9 千多单词)。