参照公网 SSL 证书应用生态，打造内网 SSL 证书应用生态

证签品牌内网 SSL 证书今天正式上线了，从去年 5 月计划开发内网 SSL 证书，到今天内网 SSL 证书上线，历时将近一年。大家一定会很好奇，为何需要耗时这么久？因为这是在打造一个全球还没有的内网 SSL 证书应用生态，而不仅仅是简单的签发一张 SSL 证书。本文详细讲解零信技术是如何打造这个生态的。

一、 内网 HTTP 流量安全问题很严重

目前内网 HTTP 流量的现状是：要么明文 HTTP 裸奔，要么部署一个所有浏览器都不信任的自签证书，两种情况所有浏览器都会提示“不安全”。某零信浏览器用户已经在内网部署了浏览器不信任的 SSL 证书，问我们怎样才能消除这个不安全警告，我们告诉用户把签发此内网 SSL 证书的根证书手动安装信任即可，结果还是不行，就让用户把他们系统部署的 SSL 证书发给我们看看，一看才知道为何即使手动信任根证书还是有安全警告了。因为这张 SSL 证书有如下多个重大安全问题：

(1) 证书公钥为 RSA 1024 位，非常不安全！国际标准要求 2010 年 12 月 31 日停止签发 1024 位证书，并于 2013 年 12 月 31 日禁用 1024 位证书，国家密码管理部门也已发类似通知要求，但是居然这么重要的内网系统在十三年后的今天还在使用 1024 位 RSA 算法 SSL 证书！

(2) 证书签名算法为 SHA-1，非常不安全！国际标准要求在 2015 年 12 月 31 日停止签发 SHA1 证书，7 年后的现在一个非常重要的内网系统还在使用 RSA 算法 SHA-1 证书！

(3) 证书没有使用者可选名称(SAN)字段，只有 CN 字段=10.142.xx.xx 的 IP 地址，这是一个大问题，因为浏览器验证 SSL 证书绑定的域名或 IP 地址是读取 SAN 字段信息的，没有这个字段就无法判断证书绑定的 IP 地址是否同用户正在访问的网站 IP 地址一致，当然会有“不安全”警告。

(4) 证书没有“服务器身份验证和客户端身份验证”的增强密钥用法(EKU)，那一定是无法实现双向认证的。

(5) 证书没有必须有的(Critical)“密钥用法”，这也是一个非常严重的问题。

(6) 证书没有证书策略字段，也没有证书透明 SCT 列表。

(7) 证书没有可访问的吊销列表和授权信息访问(AIA)网址，反正是内网无法访问外网，这还可以接受。

(8) 这张 SSL 证书在内网使用，绑定的是内网 IP 地址 10.142.xx.xx，这个不是问题，但是这张 SSL 证书已经过期一年多了，现在还在使用，这是大问题。

这么多严重安全问题的 SSL 证书居然还在非常重要内网机密管理系统使用，用户反问我们：某某浏览器能正常使用，为何零信浏览器就不能正常使用呢？我们客服被问住了，只好问我应该怎么回答用户的问题，我也是一时无语，心想这个能“正常”使用的浏览器还能称之为“浏览器”吗？网站部署的 SSL 证书有这么多不安全的问题，这个浏览器居然仍然还能正常访问？可见这家浏览器厂商也正是为了适应用户的应用环境一点安全底线都没有，这实际上是在害用户！

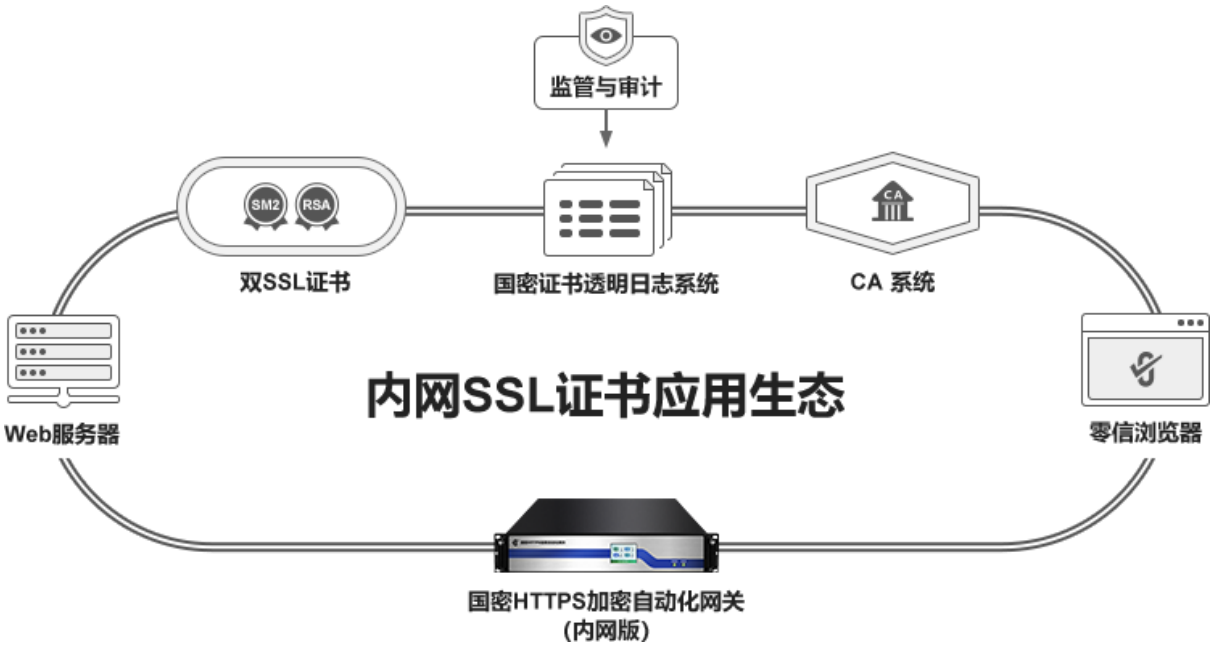
也许用户也是无奈，因为用户用的有这么多严重安全问题的 SSL 证书似乎是某个 CA 签发的，有些用户自己自签的 SSL 证书问题可能更多，甚至还有用 RSA 512 位密钥和 MD5 签名的证书。这触动了笔者决定为用户提供内网专用 SSL 证书，我们必须急为用户所急，必须解决用户的难题，为用户提供参考国际标准的 RSA 算法内网 SSL 证书和参考国密标准的 SM2 算法内网 SSL 证书，唯一不同的只能是支持内网 IP 地址和内部域名，其他技术参数必须遵循相关国际标准和国密标准。

二、 零信技术打造内网 SSL 证书应用生态

大家可以看到证签内网专用 SSL 证书顶级根证书的生成日期是 2023 年 6 月 6 日，也就是从去年 5 月份开始决定为用户签发内网 SSL 证书，发现事情并没有那么简单，不只是签发一张 SSL 证书的问题，实际上是一个生态建设问题。不仅需要 CA 系统能签发内网 SSL 证书，而且需要浏览器信任和能验证内网 SSL 证书，同时内网 SSL 证书也需要支持证书透明。这只是解决了内网 SSL 证书的供给问题，内网 SSL 证书同样需要自动化部署，因为有些使用多年的内网 Web 服务器可能不支持或不方便安装 SSL 证书，但是内网无法连接互联网，没法采用公网 SSL 证书自动化管理一样的端云一体解决方案。

大家看到了这些工作，就应该能理解为何我们花了将近一年时间才上线内网 SSL 证书，我们不仅成功打造了内网 SSL 证书应用生态所需的所有产品，而且我们还把这个生态开放给全球 CA 机构，推出了零信浏览器内网 SSL 证书可信根认证计划，让全球 CA 都能依据我们制定的内网 SSL 证书基线要求为全球用户签发内网 SSL 证书，共同为全球用户解决内网 Web 流量安全难题。

零信技术打造的内网 SSL 证书应用生态涉及到 CA 系统、双 SSL 证书(SM2 算法 SSL 证书和 RSA 算法 SSL 证书)、证书透明日志系统、零信浏览器、零信国密 HTTPS 加密自动化网关(内网版)等产品，由于国际标准不允许 CA 机构签发绑定内网 IP 地址的 SSL 证书，因为这些内部 IP 地址谁都可以用，无法验证合法拥有控制权，这就是整个内网 SSL 证书应用生态的难题所在。



既然国际标准不允许公网信任的根证书签发内网 SSL 证书，就得有专用于签发内网 SSL 证书的根证书，我们参考国际标准和国密标准生成了内网专用 RSA 顶级根证书和 SM2 顶级根证书密钥(Root Key Ceremony)，并从这些顶级根证书签发了内网 DV/OV/EV SSL 中级根证书，RSA 根证书采用 2048 位公钥，而不是 4096 位，主要是考虑到可能某个内网服务器系统版本很老而不支持 4096 位，2048 位已经能保证密钥安全。而用户证书采用的符合国际标准的 2048 位公钥和 SHA-256 签名，其他证书字段当然都是符合国际标准的。国密 SM2 根证书和用户证书都采用 SM2 算法，各个证书字段都参考国际标准。

第一个难题就是如何验证内网 IP 地址和内部域名，这个全球没有先例。我们必须研究和探索一个可行的方案。经过反复研究和测试，我们拿出了一个可行的解决方案：证书 CN 字段必须绑定一个公网域名，此公网域名必须按照国际标准完成域名控制权验证，包括指定管理员邮箱验证、CNAME 域名验证和 Web 文件验证，完成了 CN 字段域名的验证，用户才可以在 SAN 字段添加内网 IP 地址、内网主机名和内网域名，这些内网 IP 地址和内部域名无需验证，但只要是 SAN 字段中有公网域名和公网 IP 地址则都需要按照国际标准完成验证。CN 字段要求必须绑定一个公网域名的目的是为了确认这张内网 SSL 证书属于谁，谁有权拥有这张内网

SSL 证书。当然，推荐用户申请内网 OV/EV SSL 证书，证书主题中 O 字段锁定单位名称，这就更能证明这张绑定某个无法验证的内网 IP 地址或内网主机名是某个单位在使用，以保障内网 SSL 证书的安全可信。

内网 SSL 证书的验证问题解决了，第二个难题是证书透明支持。从 2013 年开始，每一张全球信任的国际算法 SSL 证书都支持证书透明，内网 SSL 证书是否也应该支持呢？答案是当然应该支持。但如何支持证书透明，这又是一个摆在我们面前的难题，因为我们只有采用国密算法实现的国密证书透明日志系统，仅支持 SM2 算法 SSL 证书，而内网 SSL 证书也是双 SSL 证书，一张 RSA 算法 SSL 证书和一张 SM2 算法 SSL 证书。经过研究和实验，我们最终选择了继续使用零信国密证书透明日志系统来同时为内网 SM2 算法 SSL 证书和内网 RSA 算法 SSL 证书提供证书透明服务，实现每一张内网 SSL 证书都提交到零信国密证书透明日志系统实现证书透明公示，这是全球独家率先实现了 RSA 算法 SSL 证书提交到国密算法证书透明日志系统获取国密算法 SCT 签名数据，并内嵌在内网 SSL 证书中，实现了双 SSL 证书的签发的全透明。

这就引出了第三个需要解决的难题，必须有浏览器信任内网 SSL 证书，包括 RSA 算法 SSL 证书和 SM2 算法 SSL 证书，同时必须有浏览器能验证内嵌在内网 SSL 证书中的国密证书透明日志签名数据。零信浏览器就承担了这个任务，零信浏览器不仅预置和信任证签内网 SSL 根证书，而且全球独家率先实现了验证 RSA 算法 SSL 证书的国密 SCT 签名数据，这又是一个技术创新。

也就是说，零信技术全球独家率先实现了国密算法证书透明日志系统同时支持 SM2 算法、RSA 算法和 ECC 算法签发的 SSL 证书，目前的国际证书透明日志系统的签名密钥是采用 ECC 算法实现数字签名 SCT 数据，并且仅支持 RSA 算法和 ECC 算法签发的 SSL 证书。零信技术让每一张内网 SSL 证书像公网 SSL 证书一样透明备案公示，有力保障内网 SSL 证书的自身安全可信。

第四个难题是内网 SSL 证书自动化，由于内网无法连互联网，无法采用公网 SSL 证书的自动化管理技术方案，唯一可行的方案是在内网部署网关，由网关实现内网 SSL 证书的自给、自动化部署和自动化实现 HTTPS 加密，并且是自适应加密算法，支持国密算法的零信浏览器采用国密算法实现国密 HTTPS 加密，不支持国密算法的其他浏览器采用 RSA 算法实现 HTTPS 加密。零信国密 HTTPS 加密自动化网关内网版仍然在研发和内测中，这是内网 SSL 证书应用生态中唯一一个还在研发中的产品。

三、内网 SSL 证书应用生态，保障内网 Web 流量安全

内网 Web 流量安全需要内网 SSL 证书，但是这不是一个简单的签发一张 SSL 证书的问题，而是要打造一个生态。零信技术在已经成功打造国密证书透明生态和国密证书自动化管理生态的基础上，又成功打造了第三个生态—内网 SSL 证书应用生态，用户可在证签官网选购 1-5 年有效期的内网 SSL 证书，买 5 年期内网 SSL 证书，用户拿到的就是 5 年有效期的双 SSL 证书，实现一次安装，5 年内网 Web 流量 HTTPS 加密安全。内网 SSL 证书支持多达 1000 个内网 IP、内网主机名、内网域名、公网 IP 和公网域名，全部都是双算法(RSA/SM2)双 SSL 证书，双证书都支持国密证书透明。

内网 SSL 证书应用生态的另一个重要产品是零信浏览器，信任证签内网 SSL 证书，优先采用国密算法实现 HTTPS 加密。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，用户仍然可以用这些浏览器实现 RSA 算法的 HTTPS 加密访问内网 Web 系统。

欢迎申请证签内网 SSL 证书，有完全免费的 90 天双证书和收费的 1-5 年证书有效期双证书。欢迎使用完全免费的国密浏览器-零信浏览器，切实保障内网 Web 流量安全，保障内网重要信息系统的机密信息安全。

有诗为证：

内网流量很机密，明文传输必泄密。
安全加密是关键，乱用证书不靠谱。
内网服务器证书，参照标准严签发。
零信浏览器信任，证书安全有保证。

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 158 篇(共 42 万 4 千多字)和英文 63 篇(7 万 7 千多单词)。