内网 SSL 证书也必须支持证书透明

为了保障 SSL 证书的安全可信，除了必须有浏览器可信根认证计划外，还必须有证书透明机制用于及时发现错误签发或恶意签发的 SSL 证书，两者都是缺一不可的，每一张全球信任的 SSL 证书从 2013 年起都支持证书透明，内网 SSL 证书也理应如此。

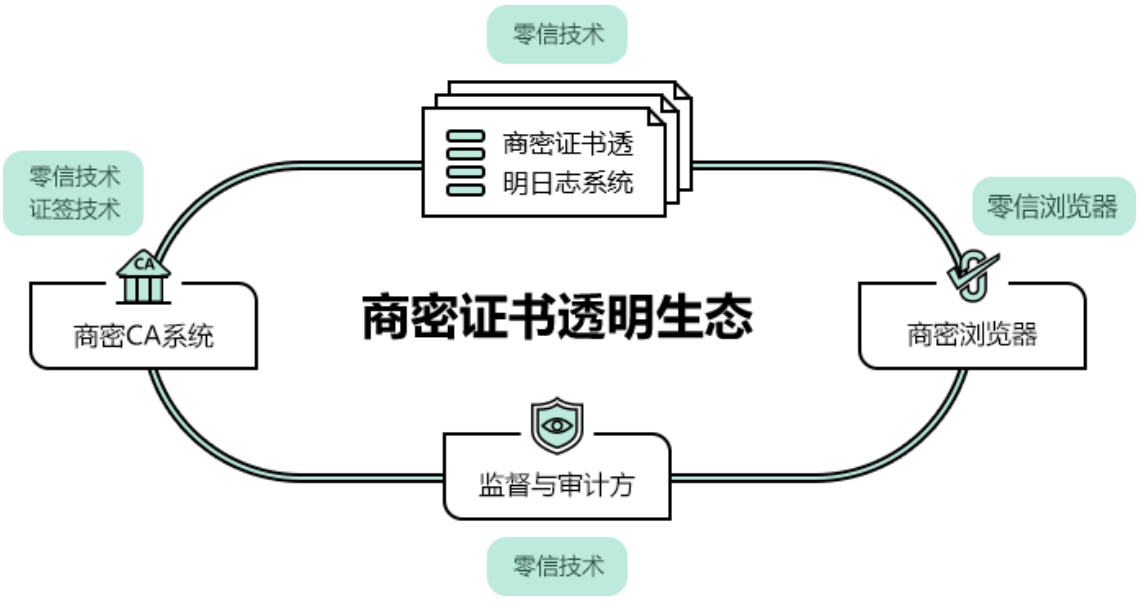
一、零信技术已成功打造商密证书透明生态

为了让国密 SSL 证书也能像国际 SSL 证书一样支持证书透明，零信技术已于 2022 年 11 月在乌镇世界互联网大会全球首发零信国密证书透明日志系统，已经持续一年半在为证签品牌和零信品牌国密 SSL 证书和其他 CA 签发的国密 SSL 证书提供透明备案公示服务，有力保障了我国国密 SSL 证书的自身安全可信。

同时，零信浏览器全球率先支持商密证书透明，已预置信任零信技术运营的 3 个商密证书透明日志系统，能实时验证内嵌商密证书透明日志签名数据，并在加密锁标识详情中展示这张商密 SSL 证书的证书透明详细信息。

同时，零信技术升级 CA 系统，能签发支持商密证书透明的商密 SSL 证书，每一张商密 SSL 证书都提交到零信商密证书透明日志系统获得证书透明日志签名数据，并内嵌到每一张签发的商密 SSL 证书中，实现每一张商密 SSL 证书的透明公示，有力保障商密 SSL 证书的自身安全可信。

零信技术全球率先打造了商密证书透明生态所需的全线产品，用商密算法完美实现了商密 SSL 证书的证书透明。不仅如此，零信技术参考国际证书透明标准(RFC6962)牵头立项制定《证书透明规范》商密标准，携手生态相关厂商依据商密标准共同打造商密证书透明生态，共同保障商密 SSL 证书的自身安全可信，共同为保障商密 HTTPS 加密安全做贡献，共同为商用密码保障我国网空安全做贡献。



二、 升级商密证书透明日志系统，支持内网 SSL 证书的证书透明

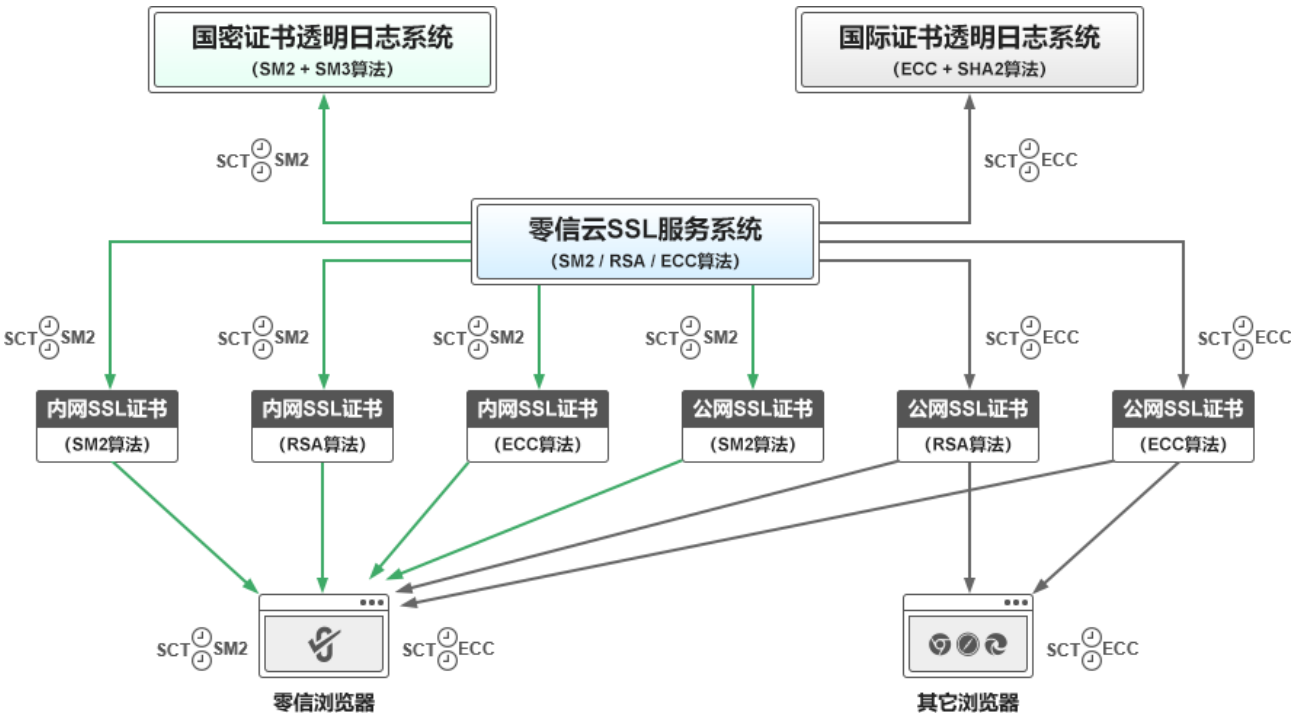
零信技术运营的 3 个国密证书透明日志系统仅支持国密 SM2 算法签发的国密 SSL 证书的透明公示，不支持 RSA 算法和 ECC 算法的 SSL 证书。为了使得证签技术为内网用户签发的 RSA 算法内网 SSL 证书也能支持证书透明，零信技术继续投入研发力量，升级改造现有的国密证书透明日志系统，使其支持 RSA 算法和 ECC 算法的 SSL 证书，这是有一点点挑战的研发工作，但经过研发团队的技术攻关，升级后的正在运营的 2024 版本零信国密证书透明日志系统已经支持三种算法 SSL 证书，实现全算法 SSL 证书支持国密证书透明，这又是一个商用密码的技术创新，值得笔者专门撰文讲一讲为何国密证书透明日志系统必须支持 SM2/RSA/ECC 三种算法 SSL 证书。

零信国密证书透明日志系统在升级之前仅支持国密算法 SSL 证书，因为日志系统签名密钥算法和哈希算法只能选一种算法，国际证书透明日志系统采用的是 ECC+SHA2 算法，零信国密证书透明日志系统采用的是 SM2+SM3 算法。现在，为了保障内网 Web 系统安全，我们签发了内网专用 RSA 算法 SSL 证书，以供无法改造内网 Web 服务器支持国密算法的用户选用。

内网 RSA 算法 SSL 证书支持证书透明，有两个技术路线可选：一是继续使用国密证书透明日志系统，增加支持 RSA 算法 SSL 证书，二是新设立一套国际证书透明日志系统。选择第二个方案是最简单的方案，直接使用谷歌开源的证书透明日志系统部署一套即可用于 RSA/ECC 算法 SSL 证书的透明公示，但我们需要运维两套证书透明日志系统，大大增加了运维成本。

如果我们选择第一个方案，则需要做大量的研发工作，不仅国密证书透明日志系统需要做大量的改造来支持 RSA/ECC 算法 SSL 证书，而且零信浏览器也需要改造支持验证 RSA/ECC SSL 证书中的国密算法签名的 SCT 数据，原先由开源 Chromium 负责验证 RSA/ECC SSL 证书的 SCT 数据的代码已经无法使用，因为原验证代码不支持验证国密 SCT 签名数据。

考虑到运维两套算法证书透明日志系统的成本大大提升，同时考虑到目前的实际 HTTPS 加密部署应用中国际算法 SSL 证书和国密算法 SSL 在一定时期内会并存使用，零信技术作为国密证书透明标准制定的牵头单位和领先者，必须提前布局做好技术准备工作，使得国密证书透明日志系统同时支持国密算法 SSL 证书和国际算法 SSL 证书。所以，我们决定升级现有的国密证书透明日志系统同时支持三种算法(SM2/RSA/ECC)签发的 SSL 证书，只有这样才是一个最优最符合我国国情的 SSL 证书透明公示监管解决方案。现在的国际证书透明日志系统采用的是 ECC 算法，但同时支持 RSA 算法和 ECC 算法 SSL 证书，这实际上也是一个道理：一套系统支持多种算法的用户证书。



升级后的零信国密证书透明日志系统除了用于零信浏览器信任的所有 CA 机构提交国密 SSL 证书的透明公示外，还信任证签和零信所有公网 SSL 证书和内网 SSL 证书的 RSA 算法和 SM2 算法根证书，用于保障证签品牌和零信品牌内网 SSL 证书的安全可靠供给，保证内网 RSA/SM2 SSL 证书采用公网 SSL 证书一样的证书透明标准。零信国密证书透明日志系统不接受其他 CA 提交 RSA/ECC 算法公网 SSL 证书的证书透明公示，仅限于零信浏览器信任的

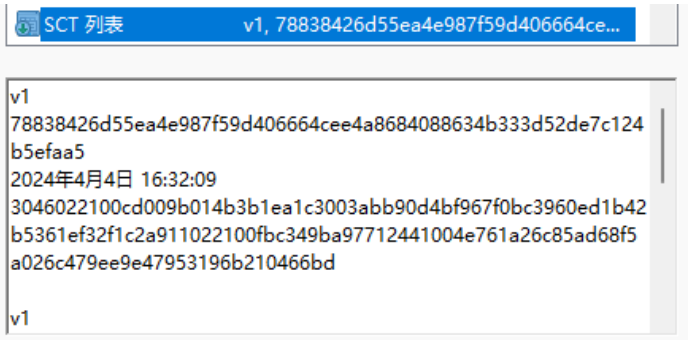
RSA/ECC 算法内网专用 SSL 根 CA 机构提交签发的内网 RSA/ECC 算法 SSL 证书。

三、升级零信浏览器，支持内网 SSL 证书的证书透明

零信云 SSL 服务系统把每一张证签内网 SSL 证书都提交到升级后的零信商密证书透明日志系统实现内网 SSL 证书的透明公示，这也是全球首创，不仅实现了内网商密 SSL 证书支持商密证书透明，而且零信浏览器也全球率先实现了支持 RSA 算法 SSL 证书内嵌商密算法证书透明日志签名数据的实时验证与展示。

如下左图所示，零信浏览器不仅信任展示内网 EV SSL 证书为绿色地址栏，点击加密锁标识，能看到这张内网 SSL 证书为 SM2 算法 SSL 证书，用 SM2 算法实现 HTTPS 加密，证书透明签名数据为 SM2 算法签名。如下右图所示，这张内网 EV SSL 证书为 RSA 算法 SSL 证书，一样支持商密证书透明，RSA 算法 SSL 证书实现 HTTPS 加密，但证书透明签名数据为 SM2 算法签名，这是全球首个实现了 RSA 算法 SSL 证书支持商密证书透明，并且零信浏览器全球率先实现了验证 RSA 算法 SSL 证书的商密证书透明签名数据，这又是一个技术创新。

由于谷歌浏览器并不验证内网 SSL 证书是否支持证书透明，也不解析内网 SSL 证书内置的证书透明 SCT 数据，所以不影响谷歌浏览器用户能正常访问部署了内网 RSA 算法 SSL 证书的网站，虽然谷歌浏览器不支持 SM2 算法，如下左图所示。Windows 证书查看器仍然能解析国密证书透明日志数据(SCT 列表)，只是不显示日志签名算法，如下右图所示。



四、 内网 SSL 证书支持证书透明，同公网 SSL 证书一样安全可信

零信技术全球独家率先实现了商密算法证书透明日志系统同时支持 SM2 算法、RSA 算法和 ECC 算法签发的内网 SSL 证书，让每一张内网 SSL 证书无论采用何种算法都可以实现证书透明公示，有力保障了内网 SSL 证书的安全可信，让用户可以像使用公网 SSL 证书一样放心使用内网 SSL 证书。

而无论 SSL 证书采用何种算法都支持商密算法实现证书透明，这个科研成果和应用实践，为我国将来建立国家级证书透明日志系统来统一监管在我国部署使用的国际 SSL 证书和商密 SSL 证书提供了非常好的技术探索和运维实践。

有诗为证：

服务器证书要安全，透明是关键。
商密证书安全，商密透明为必须。
商密证书透明，支持三算法证书，
证书全商密透明，商密保障安全。

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 159 篇(共 42 万 6 千多字)和英文 64 篇(7 万 8 千多单词)。