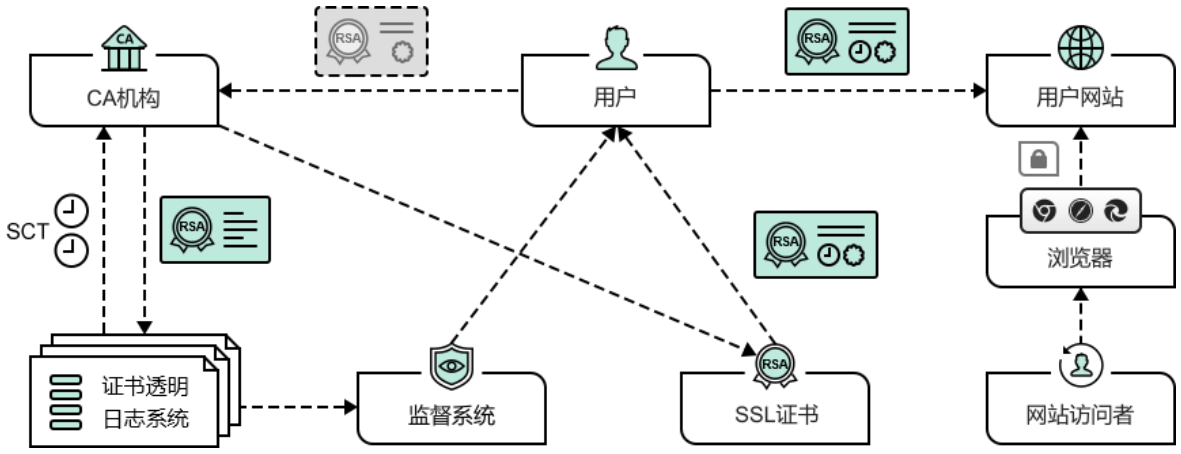
谁来保障国密 SSL 证书的安全?

随着《密码法》的深入贯彻实施，国密 SSL 证书已经在我国有了快速部署应用的发展趋势，笔者在《国密 SSL 那些事儿》一文中已经指出了目前国密 SSL 证书存在的各种问题，这些都是一些技术问题，是很容易解决的。笔者在文末写道“还有一个很重要的问题比较复杂，非三言两语说得清楚，下次独立写一篇文章来讲”，这就是本文了。这个话题的确有点复杂，所以，笔者在此之前就先专门写了篇介绍证书透明的博文-《谁在保障全球 73 亿张 SSL 证书的安全?》，详细介绍了证书透明机制的原理和作用，这个由谷歌牵头的证书安全保障体系已经成功保障了全球 73 亿张 RSA/ECC 算法 SSL 证书的安全，笔者强烈推荐读者在阅读本文之前先阅读那篇证书透明入门文章。

还是先简单总结一下那篇文章的内容。所有全球信任的国际算法 RSA/ECC SSL 证书都由证书透明机制来保障证书的安全，为了后续比较说明，我把这个机制称之为“国际证书透明”。这个机制要求每一张全球信任的 SSL 证书都必须在证书签发之前先把预签证书提交到谷歌指定的证书透明日志系统中去备案并拿到用于证明已备案的证书透明日志数字签名数据(SCT)，CA 机构必须把 SCT 数据嵌入在 SSL 证书的扩展字段中，才能签发正式证书给用户，浏览器才会信任这张 SSL 证书，第三方监管机构就可以通过查询证书透明日志数据库实时监督每一张 SSL 证书的签发行为。这是一个有多方参与的证书透明生态体系，是对 CA 系统和 CA 机构的证书签发行为的零信任，有力保障了全球信任的国际算法 SSL 证书的安全。

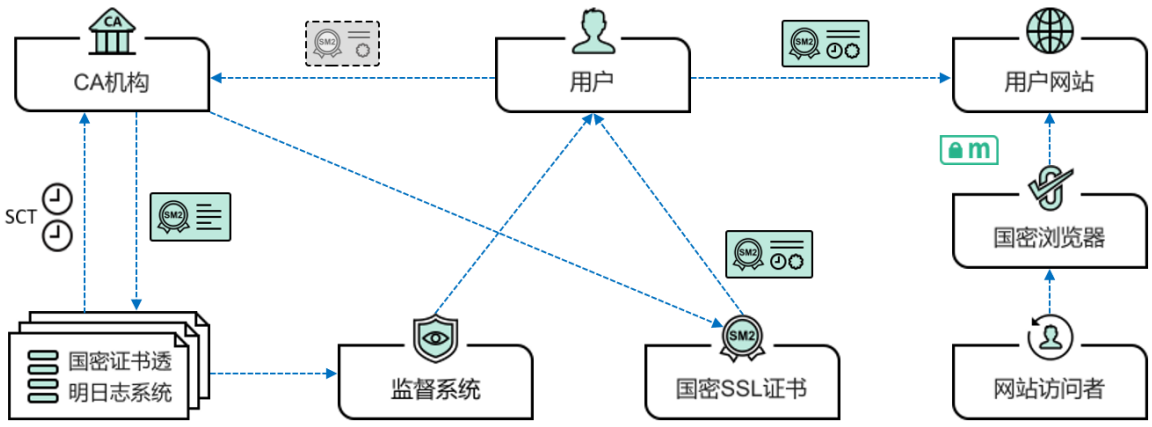


但是，这个很好的保护 SSL 证书安全的机制无法用于保障我国国密 SSL 证书的安全，因

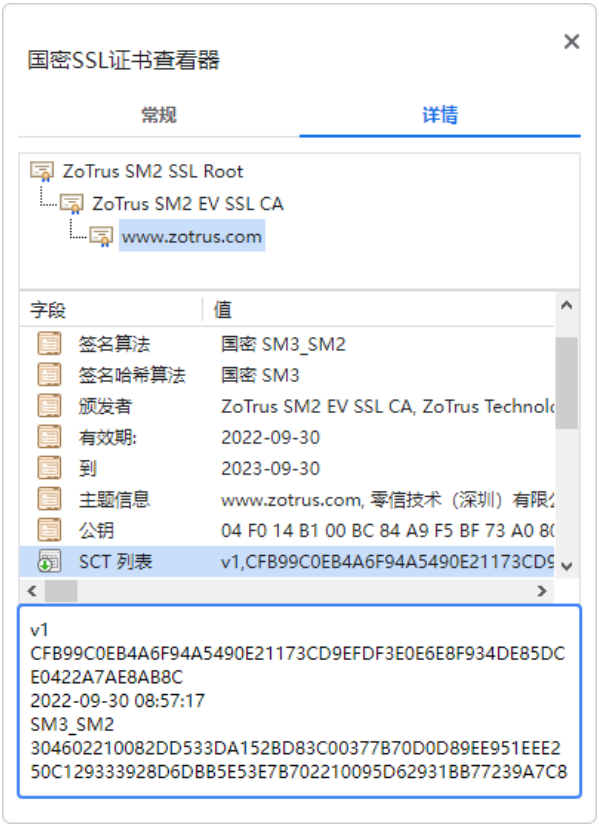
为国际证书透明日志系统不支持国密算法和国密 SSL 证书，所以，目前市场上的所有国密 SSL 证书都不支持证书透明，怎么办？当然是我国也必须有自己的“国密证书透明”机制，核心是采用国密算法实现数字签名透明日志数据和支持国密 SSL 证书。零信技术投入研发力量，历时一年多，成功研发国密证书透明全生态产品，全球独家率先发布的国密证书透明日志系统就是证书透明机制的核心系统，参考了国际证书透明日志系统，重点攻关把国际证书透明日志系统的密码算法由原先的 ECC 算法改为 SM2 算法，并全面支持国密 SSL 证书。

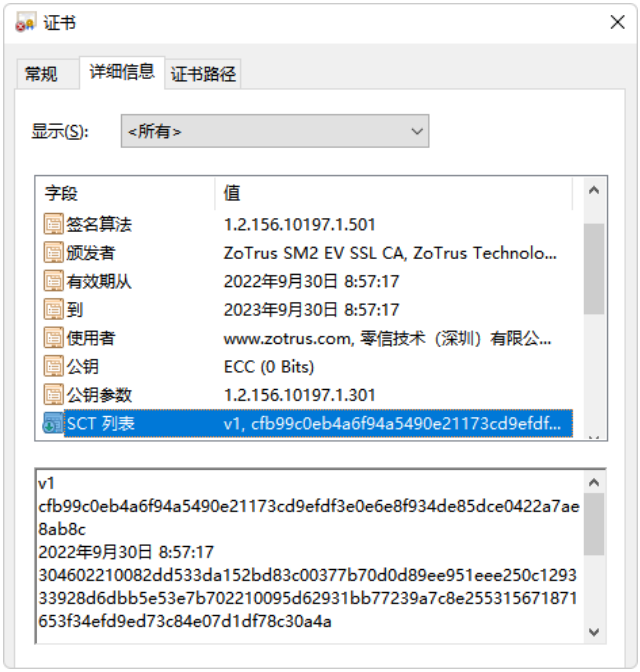
要建设国密证书透明体系，光有国密证书透明日志系统是不够的，必须有 CA 系统能签发支持国密证书透明的国密 SSL 证书，CA 系统把签发的国密 SSL 预签证书提交到国密证书透明日志系统，实现透明备案并拿到国密 SCT 签名数据，但是目前市场上还没有这样的国密 CA 系统。俗话说，求人不如求己，零信技术继续投入研发力量，创新研发了零信云 SSL 系统，这是我国乃至全球首个支持国密证书透明的国密 CA 系统，其签发的每一张国密 SSL 证书都已经包含了国密证书透明签名数据。零信云 SSL 系统会把预签证书提交到零信国密证书透明日志系统，拿到证书透明签名数据后写入到国密 SSL 证书中，用户拿到这张国密 SSL 证书后部署到用户网站上实现国密证书透明 https 加密。

不过，还缺一环，那就是浏览器的支持，同样，目前市场上也没有支持国密证书透明的浏览器，零信技术继续投入研发力量，实现了零信浏览器全球独家率先支持国密证书透明，信任并预置零信证书透明日志系统，支持验证国密 SSL 证书中的国密证书透明签名数据，这就通过各个自研系统形成了一个可实际运转的国密证书透明生态系统，一个全链条都采用国密 SM2 算法的证书透明机制就这样由零信技术全球独家打造出来了！最后一个环节就是第三方的监督系统，零信国密证书透明日志系统已经按照 RFC6962 国际标准开放了 API 查询接口，供第三方调用监督。零信技术也将在国密证书透明官网提供了一个实时在线查询界面，让用户可以实时查询国密证书透明日志系统中所有已备案的国密 SSL 证书，及时发现可疑的国密 SSL 证书。



国密证书透明机制采用同国际证书透明机制一样的技术和同样的标准，唯一不同的是采用了 SM2 算法实现证书透明数据的数字签名，而不是 ECC 算法，并在浏览器支持验证 SM2 算法的 SCT 数据。欢迎大家使用零信浏览器访问零信官网，点击加密锁查看国密 SSL 证书，如下左图所示，证书中增加了一个新的字段：SCT 列表，会显示这张证书的 SCT 数据。而如果用 Windows 证书查看器查看这张国密 SSL 证书，如下右图所示，也一样会显示 SCT 列表字段和显示 SCT 数据。但不同的是，由于 Windows 不支持国密算法，所以，在 SCT 签名时间下一行不会显示 SCT 数据的签名算法，而用零信浏览器查看则会显示 SCT 数据的签名算法为国密算法 SM3_SM2，能明确告诉用户 SCT 数据是采用国密算法签名的。





从 2022 年 4 月 15 日起，谷歌浏览器要求证书有效期小于或等于 180 天的 SSL 证书必须包含 2 个 SCT 数据，大于 180 天的 SSL 证书必须包含 3 个 SCT 数据，也就是说，必须同时在 2 个或 3 个证书透明日志系统备案，因为谷歌对证书透明日志系统也是采取零信任的政策，必须一个是谷歌自己的，另外一个或两个是其他方提供的，当然也都是谷歌浏览器信任并预置的。零信浏览器的国密证书透明政策也计划采用一样的政策，证书有效期小于或等于 180 天的国密 SSL 证书必须包含 2 个国密 SCT 数据，大于 180 天的国密 SSL 证书必须包含 3 个国密 SCT 数据，其中必须包含一个零信国密证书透明日志数据。但是，鉴于目前只有 3 个零信国密证书透

明日志系统可用，暂时只要求前者含一个国密 SCT 数据，后者含两个国密 SCT 数据。如果以后市场上有更多的国密证书透明日志系统通过零信浏览器认证并预置信任，则施行同谷歌浏览器一样证书透明策略。

今天，笔者很高兴地看到，通过零信技术一年多的努力，全球首个基于国密 SM2 算法的证书透明机制已经建设完成并投入使用，不仅有力保障了由证签技术和零信技术签发的所有国密 SSL 证书的安全可信，包括免费国密 SSL 证书和收费的国密 SSL 证书，而且有力保障了零信浏览器信任的 CA 机构签发的已经内置国密证书透明数据的国密 SSL 证书的安全可信。欢迎所有签发国密 SSL 证书的 CA 机构加入这个保障国密 SSL 证书安全的国密证书透明日志系统，只有所有国密 SSL 证书都支持证书透明机制才能真正保障我国国密 SSL 证书的安全可信，未加入证书透明机制的国密 SSL 证书必将被认为是一个可能用于攻击的不安全的国密 SSL 证书，因为没有公开披露这种已签发的证书。国密证书透明机制能有效防止恶意签发的用于攻击和欺诈的国密 SSL 证书，从而保障国密 SSL 证书本身的安全，只有国密 SSL 证书自身安全有保障，才能真正保障国密 https 加密的安全，从而真正保障我国互联网安全可信可控。当然，欢迎更多的支持国密算法的浏览器也支持国密证书透明机制，共同为保障国密 SSL 证书的安全做贡献。

最后，考虑到 CA 机构改造国密证书签发系统需要时间，零信浏览器目前对没有包含国密证书透明日志数据的国密 SSL 证书仅提示“国密证书不透明”。从 2023 年 7 月 1 日起，零信浏览器将采用谷歌浏览器一样的证书透明政策，对没有包含零信浏览器信任的国密证书透明数据的国密 SSL 证书显示“不安全”警告，从而真正实现从国密证书透明机制上保障国密 SSL 证书的安全可信。

王高华

2022 年 9 月 30 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。