证书透明就是对 SSL 证书签发的零信任

签发 SSL 证书必须先验证用户的域名控制权，但是，如果 CA 系统恶意或错误签发了没有验证的绑定某个域名的 SSL 证书怎么办？由谷歌牵头设计的证书透明机制就是为了解决这个问题的。

证书透明(CT)是一个用于记录和监视 TLS/SSL 证书颁发的系统。CT 极大地增强了每个人监控和研究证书颁发的能力，这些功能为 CA 生态系统和 Web 安全性带来了许多改进。因此，CT 正迅速成为关键基础设施。证书透明是用于监控和审计 SSL 证书的 Internet 安全标准。该标准创建了一个公共日志系统，旨在最终记录由公共信任的证书颁发机构颁发的所有证书，从而有效识别错误或恶意颁发的证书。最新的证书透明机制 2.0 版在实验阶段的 RFC 9162 中进行了描述，它淘汰了 RFC 6962 中描述的早期版本 1.0，目前各家 CA 机构都仍然在使用 1.0 版本。

如果一张 SSL 证书没有在谷歌浏览器要求的证书透明日志系统备案，则谷歌浏览器会有安全警告，如下图所示，会提示“ERR_CERTIFICATE_TRANSPARENCY_REQUIRED”(错误_要求证书透明)。这就是对国际 SSL 证书签发行为的零信任，不信任每一张没有证书透明的 SSL 证书，浏览器明确告诉网站访问者这是一张不能信任的 SSL 证书。

同理，为了保障国密 SSL 证书的自身安全可信，国密 SSL 证书也需要证书透明，但是由于目前的国际证书透明日志系统不支持国密算法，所以，我国必须有支持国密算法的国密证书

透明系统。零信技术投入研发力量，历时一年多，于今日全球率先推出了国密证书透明日志系统，此系统参照 RFC 9162 国际标准但采用了国密 SM2 算法实现 CT 数据的数字签名。零信国密证书透明日志系统已预置到零信浏览器信任，原计划是如果一张国密 SSL 证书没有在零信浏览器信任的证书透明日志系统备案，则零信浏览器会像谷歌浏览器一样显示一样的安全警告，如下图所示，会提示“ERR_SM2_CERTIFICATE_TRANSPARENCY_REQUIRED”(错误_要求国密证书透明)。这就是对国密 SSL 证书签发行为的零信任，不信任每一张没有证书透明的国密 SSL 证书，零信浏览器明确告诉网站访问者这是一张不能信任的国密 SSL 证书。

但是，考虑到各家签发国密 SSL 证书的 CA 机构需要时间升级证书签发系统，以支持签发的国密 SSL 证书中含有 SCT 数据，零信浏览器决定从 2023 年 7 月 1 日起执行上面的强制要求每张国密 SSL 证书都必须有 SCT 数据的计划，在此之前只是在国密合规标识提示中显示“国密证书不透明”，以提醒用户注意，并选择部署支持证书透明的国密 SSL 证书，以保障自己网站安全的合法权益。

国际证书透明系统已经累计成功保障了 74 亿多张全球信任的 SSL 证书的安全可信，这是从 2013 年到现在 10 年的总数据。今天，零信技术上线的国密证书透明日志系统和零信浏览器对国密 SSL 证书透明的支持，也必将能成功保障我国国密 SSL 证书的安全可信，欢迎国密 SSL 证书各相关方积极加入国密证书透明的生态系统中，只有每一张国密 SSL 证书都证书透明了，才能真正保障我国国密 https 加密的安全可信，真正安全实现国密 https 加密来保障我国互联网安全。

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。