零信浏览器让证书透明更透明

证书透明是保障 SSL 证书自身安全的重要技术，能有效并高效地及时发现错误签发或恶意签发的 SSL 证书，截至到今天，证书透明已经成功为全球 101 亿多张国际算法 SSL 证书提供了证书透明公示服务。

但是，谁在为这 101 亿多张 SSL 证书提供证书透明服务呢？非专业人士可能对此一无所知，即使是 SSL 证书用户，他们只知道从哪个 CA 机构申请了 SSL 证书，但是至于证书透明可能都没有听说过，但是证书透明对于 SSL 证书用户来讲又非常重要，用户应该关心是否有 CA 机构在用户不知情的情况下为其网站域名签发了 SSL 证书，如果签发了非自己知晓的 SSL 证书该如何处理。证书透明是一个保护用户合法权益的透明公示机制，有点像公证服务，证书透明服务提供商就是公证处，证明某 CA 在何时为何域名签发了 SSL 证书，这是由密码算法来保证不可抵赖的和不可诬陷的。由此可见，证书透明服务提供商是谁，这似乎也是一个需要更加透明的事情。

零信浏览器作为全球首个同时支持国际证书透明和国密证书透明的浏览器，在此次升级之前只是增强显示了国密 SSL 证书的证书透明信息，并没有展示国际 SSL 证书的证书透明信息。

零信浏览器此次版本升级的亮点之一是：全球独家创新地在加密锁标识下面增加展示 SSL

证书的证书透明信息，同时支持展示国际 SSL 证书和国密 SSL 证书的证书透明详细信息，使用同一界面展示 RSA/ECC/SM2 三种算法 SSL 证书的证书透明信息，不再特别只展示国密证书透明信息，证书透明 UI 展示的信息包括证书透明日志签名数据的密码算法，证书内包含了几个证书透明日志签名数据，并列出所有证书透明日志系统的名称和日志系统运营单位名称。

如下左图所示，这张国际 SSL 证书的证书透明日志服务的密码算法为 ECC 算法，包括了 3 个证书透明签名数据(ECC, 3)，由谷歌和 Cloudflare 分别提供证书透明公示服务，其中谷歌有两个证书透明日志系统：Xenon2024 和 Argon2024，Cloudflare 证书透明日志系统是 Nimbus2024。如下右图所示，这张国密 SSL 证书的证书透明日志服务的密码算法为 SM2 算法，包括了 3 个证书透明签名数据(SM2, 3)，由零信技术和证签技术分别提供证书透明备案服务，其中零信技术有两个证书透明日志系统：SM2CTcn20204 和 SM2CTcom20204，证签技术证书透明日志系统是 SM2CT2024。

也就是说，零信浏览器不仅同时支持识别和验证国际 SSL 证书和国密 SSL 证书中的证书透明日志签名数据，不仅同时支持国际算法(ECC/SHA2)和国密算法(SM2/SM3)实现的证书透明，而且把证书透明日志签名数据相关的信息都汇总到一个用户界面上，让用户对所有密码算法的 SSL 证书的证书透明信息一目了然。

如果国际 SSL 证书没有内置证书透明日志数据，则零信浏览器同谷歌浏览器一样的提示“不安全”，如下左图所示。而对于国密 SSL 证书，考虑到国密证书透明标准还在制定过程中，各个 CA 机构还需要时间升级 CA 系统支持国密证书透明，如果国密 SSL 证书中没有内置零信浏览器信任的国密证书透明日志签名数据，则零信浏览器暂时只是提示“证书不透明”，如下右图所示。零信浏览器计划于 2024 年 1 月 1 日开始采用同谷歌浏览器一样的政策显示为“不安全”，希望各个零信浏览器信任的国密根 CA 机构能尽快完成 CA 系统升级，尽快签发内嵌零

信浏览器信任的国密证书透明日志数据的国密 SSL 证书。

零信浏览器这个 UI 创新的意义在于进一步提升证书透明服务的透明度，让证书透明更加透明，不仅让 SSL 证书用户了解其 SSL 证书是哪家公司为其提供了证书透明服务，而且能让网站访问者也能了解这个网站部署的 SSL 证书是由哪家公司供证书透明服务的，类似于了解纸质公证书是哪个公证处出具的，这不仅能提升证书可信度，而且能提升证书透明服务提供商的品牌知名度，让证书透明公益服务也能为公司带来品牌价值，有利于证书透明生态的健康发展。

王高华

2023 年 8 月 8 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。