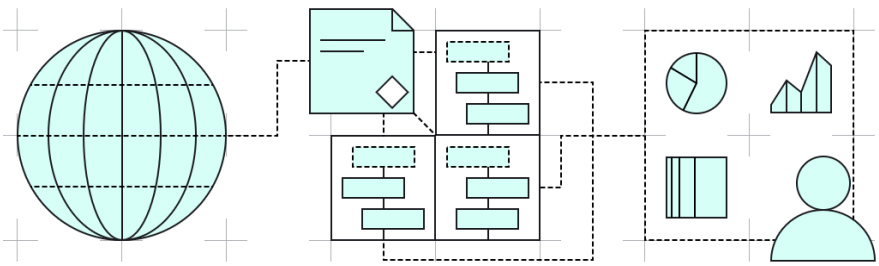
谁在保障全球 73 亿张 SSL 证书的安全?

大家都知道网站安全离不开 SSL 证书，要实现 https 加密必须有 SSL 证书，那么谁在保障 SSL 证书的自身安全？有人会说当然是签发 SSL 证书的 CA 机构哦，CA 机构必须保证签发 SSL 证书的系统安全，这个没错。但是，如果 CA 系统被恶意签发了不该签发 SSL 证书，或者 CA 机构操作失误而错误签发了不该签发的 SSL 证书，怎么办？如何能及时发现恶意或错误签发的 SSL 证书？这些都是本文要问答的问题。

笔者已经在 CEO 博客发布了 3 期《中国 SSL 证书市场发展趋势分析简报》，简报中的数据来源是“根据谷歌证书透明日志系统数据统计”，曾有读者私信问我：什么是证书透明？什么是谷歌证书透明日志系统？为什么说采用谷歌证书透明日志数据就是权威数据？我当时只是简单地回复“百度一下”，不好意思，现在我自己也百度了一下，没有发现一个讲清楚了这个问题的文章。

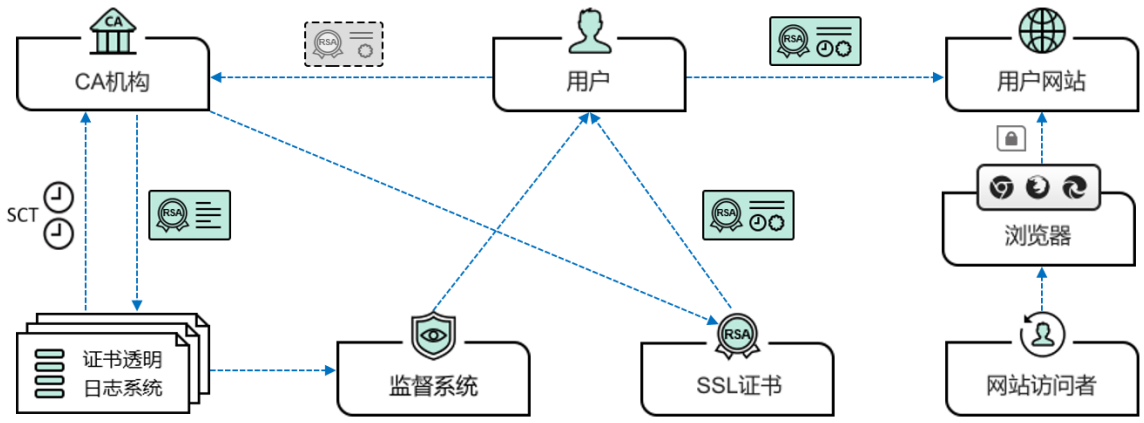
请别以为上面两段文字毫无关联，怎么刚刚说如何发现错误签发的 SSL 证书，突然又讲起了 SSL 证书市场简报呢？别急，这两个问题其实是一个问题，第一段提出的问题的解决方案就是证书透明，本文就把证书透明讲透，大家不仅能了解如何及时发现错误签发的 SSL 证书，而且也就清楚了为何笔者按季度发布的《中国 SSL 证书市场发展趋势分析简报》中的数据是权威可信数据。两段文字提出的问题只需一个答案，那就是证书透明！证书签发行为透明公示，公示的数据就是真实数据，就可以用于分析，这是证书透明的一个重要应用。

证书透明的英文是“Certificate Transparency”，也可以翻译为“证书透明度”。其实，大家对“透明度”这个词并不陌生，如：“提升国有企业*股权*交易*透明度*”、“提高企业内部管理的透明度”等等。那什么是证书透明？或什么是证书透明度？顾名思义，就是签发证书行为的透明公开，这里主要是指用于网站 https 加密的 SSL 证书的透明度。这是由谷歌牵头发起的一个 RFC 6962 国际标准，是一个能及时发现恶意或错误签发不是用户自愿申请的 SSL 证书的透明度管理系统。



申请过 SSL 证书的读者一定知道，签发 SSL 证书的关键步骤是必须验证证书申请人的域名控制权，可以通过三种方式来证明用户拥有这个域名的控制权，一个是给特定的 5 个邮箱(包括：admin@域名，administrator@, postmaster@, webmaster@, hostmaster@)发送验证码，二是把验证码作为一条 CNAME 域名解析，三是把验证码放在网站中的特定目录的特定文件中。这些控制措施能有力保障只能是有权控制域名的人才能为这个域名申请 SSL 证书。但是，如果 CA 机构不按照这个要求来操作就签发了绑定某个域名的 SSL 证书怎么办？如果签发 SSL 证书的 CA 系统被黑，绕过了域名验证机制而签发了绑定某个域名的 SSL 证书怎么办？在证书透明系统出来之前还真的没有任何办法知道这些错误签发证书的行为。

证书透明日志系统可以简单地理解为每签发一张证书都必须在这个系统公开披露，通俗地讲就是在 SSL 证书诞生之前必须先公示并申请“准生证”，CA 系统在签发证书之前把预签证书提交到证书透明日志系统获得证书透明签名数据(SCT)，就等于拿到了“准生证”，CA 系统必须把这个 SCT 数据作为一个 SSL 证书的扩展项写到正式签发的 SSL 证书中(随身携带准生证备查)，这张 SSL 证书就可以正式诞生了，等于“已经上户口了”，就可以给用户去部署使用，浏览器才会信任这张证书，因为这张证书已经在证书透明系统公开披露并备案成功了。而为何要把“准生证”数据嵌在证书中，当然是为了方便浏览器可以实时验证是否已经公开披露和验证是否在指定的系统公开披露。同时，第三方监督系统就可以通过检索证书透明日志系统的数据库就能实时监控和分析每张签发的 SSL 证书，一旦发现有非法签发证书，则可以实时通知用户。这是对 CA 系统和 CA 机构的零信任，是一个能有效保障 SSL 证书安全的零信任安全措施。



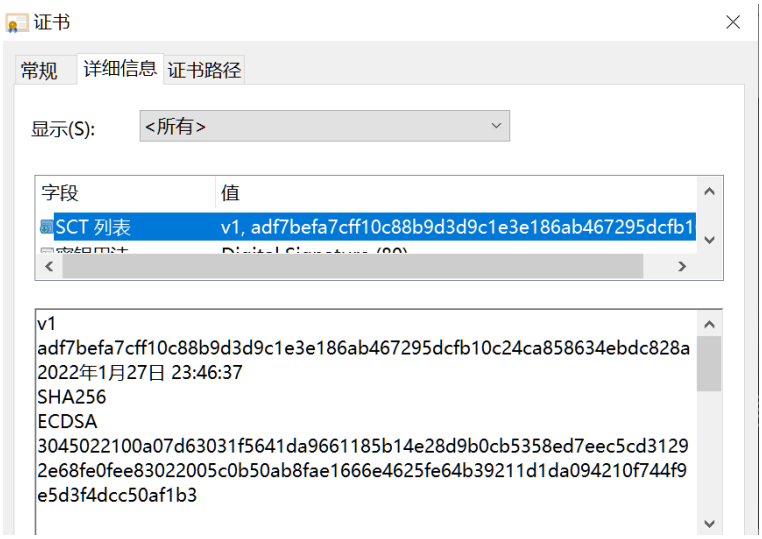
证书透明机制也可以类比为我国的 ICP 备案机制，网站域名要启用，必须先备案。要签发 SSL 证书，也必须先到证书透明日志系统去备案。不同的是：“证书透明”的取名比较高大上，备案手续要简单些，只需自动获取备案系统的数字签名即可。但机制都是一样的，提高透明度，

降低风险，增强监管。也就是说，是证书透明机制在保障每一张 SSL 证书的安全。

我们再看看证书透明日志系统的统计数据，从 2013 年开始，已经记录了 73 亿多张全球信任的 SSL 证书，谷歌浏览器从 68 版本开始(2018 年 5 月)就已经强制要求全球所有 CA 签发的每一张 SSL 证书都必须提交到指定的证书透明日志中才会被谷歌浏览器信任。笔者发布的季度分析简报中的 SSL 证书数据就是查询谷歌证书透明日志系统数据整理的，由于每一张 SSL 证书都有库可查，所以笔者引用的数据绝对是可靠可信数据，这就是为何笔者在简报中说明了数据来源是“根据谷歌证书透明日志系统数据统计”。

如果某张 SSL 证书没有到谷歌指定的证书透明日志系统去备案会怎么样？谷歌浏览器会不信任这张 SSL 证书，如下图所示，浏览器地址栏会显示红色“不安全”警告，默认页会提示“ERR_CERTIFICATE_TRANSPARENCY_REQUIRED”(错误_要求证书透明)。点击“高级”会显示“该服务器提供了一个未通过证书透明度政策公开披露的证书。某些证书必须通过证书透明度政策进行公开披露，以确保它们值得信任且能保护用户免遭攻击。”也就是说：没有备案的 SSL 证书由于没有公开披露签发行为而让人怀疑可能是用于恶意攻击的 SSL 证书而不值得信任，所以，谷歌浏览器会有“不安全”警告。

那么，如何知道自己拿到的 SSL 证书已经备案了？或者说如何验证 CA 机构签发给用户的 SSL 证书是否已经公开披露而确保谷歌浏览器不会提示“不安全”？建议所有用户在拿到 SSL 证书后点击查看证书详细信息，看看证书中是否有一个“SCT 列表”的字段，如下图所示，如果有，则说明这是一张合格的正品。可以再看看有几段 SCT 数据，一般有两段或者三段下图显示的数据，每段数据中第一行是 CT 的版本号，目前全球各大 CA 都在用 V1 版本，证书透明 V2 版本国际标准 RFC 9162 还处于实验阶段。第二行是证书透明日志服务器 ID，第三行是证书透明日志系统的签名时间，第四行则是日志数据的签名算法(SHA256/ECDSA)，第五行就是 SCT 签名数据，这些数据用于浏览器验证这张 SSL 证书是在哪个证书透明日志系统备案的、是何时备案的、证书透明日志系统是否是浏览器信任的等等，只有通过验证，浏览器才会正常显示加密锁标识。



相信读者已经能看出，证书透明机制实际上也是一个生态体系，不仅要有证书透明日志系统，还要有浏览器、CA 机构、监管机构等相关产品和服务提供商的共同参与。所以，准确地讲，是证书透明生态体系在保障已经签发的 73 亿张全球信任的 SSL 证书的安全，从而有效地保障了 https 加密安全和全球互联网安全。

王高华

2022 年 9 月 13 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。