密码讲堂 | 第 8 讲 什么是证书透明？什么是国密证书透明？

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。笔者在第五讲讲过什么是可信根认证计划，这是为了保证 SSL 证书的安全可信，由浏览器提出的信任计划，浏览器只信任通过严格认证的 CA 机构的根证书签发的 SSL 证书。但是，如果浏览器信任的 CA 系统被恶意签发了不该签发的 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？本讲就是要讲一讲这个解决方案。

大家对“透明度”这个词应该不陌生，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？这个名称翻译自英文的“Certificate Transparency”，为了简化名称，笔者翻译为“证书透明”，也有人认为翻译为“证书透明度”更确切，如果要讲确切的话，按照中文的语境和这个系统的用途，可以翻译为：证书备案，因为我国的网站备案就是一个透明公示网站的真实身份的系统。而证书透明则是一个透明公示 CA 机构已经为某个域名签发了 SSL 证书的系统。“透明”是一个非常西式并且显得高大上的名字，而备案则是一个非常中式而且通俗易懂的名字，各有侧重点。

证书透明，就是证书签发行为的透明公开，这里主要是指用于网站 https 加密的 SSL 证书的透明公示。这是由谷歌牵头发起的 RFC 6962 国际标准，是一个能及时发现恶意签发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，也可以理解为是一个 SSL 证书预签备案系统，有点像房屋预售备案系统，这是一个在证书签发给用户之前的备案，而不是事后备案。

我们还是先看看已经透明备案的 SSL 证书同没有透明备案的 SSL 证书有什么不同吧。建议大家现在就打开你正在访问的网站的加密锁标识查看一下 SSL 证书，一定有一个“SCT 列表”字段(Windows 查看)，如下左图所示。或者如下右图所示，证书详细信息中有一个没有解析的仅显示 OID 的字段“OID.1.3.6.1.4.1.11129.2.4.2”，这是因为谷歌浏览器从 105 版本开始，Windows 和 macOS 版本从原先使用操作系统的证书查看器改为使用谷歌浏览器自己的证书查看器，这个改变是因为谷歌推出了自己的不依赖于操作系统的可信根认证计划，但估计是仓促上线自己的证书查看器而使得查看器还没有解析这个 OID 为 SCT 列表，当然也不排除有其他的意义，但是笔者估计将来的版本应该会解析这个字段，否则这样显示很不友好。

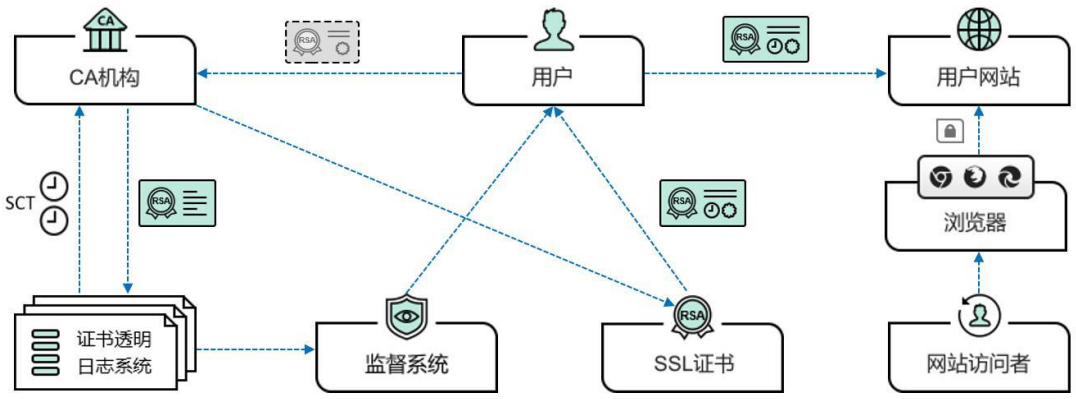
请大家看看上面这两个截图，同一证书字段信息，左边 Windows 解析出了证书透明日志签名数据，而右图则既没有解析 OID 是 SCT 列表，也没有解析这个字段中的具体数据是什么意思，只是列出的这一段二进制数据，这显然是非常不友好的。我们再看看 Windows 查看器显示的内容，第一行是证书透明版本号，目前全球各大 CA 和浏览器都在使用 V1 版本(RFC6962)，V2 版本国际标准 RFC 9162 还处于实验阶段。第二行是证书透明日志服务器 ID，第三行是证书透明日志系统的签名时间，第四行则是日志数据的签名算法(SHA256/ECDSA)，第五行就是证书透明日志的签名数据。这些数据用于浏览器验证这张 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，这个知识点笔者已经在密码讲堂的第 7 讲《浏览器是如何验证 SSL 证书的？》讲过，在第 5 步--验证 SSL 证书是否已透明公开披露。

讲到这里，大家只需了解 RFC6962 国际标准是在 X.509 V3 版本数字证书标准中增加了一个新的字段用于显示证书透明日志签名数据，由于这个标准是谷歌牵头于 2013 年 6 月提出的，所以从自己的 OID 体系中定义了 4 个 OID 分别用于标识相关字段：SCT 列表(1.3.6.1.4.1.11129.2.4.2)、预签证书毒丸(1.3.6.1.4.1.11129.2.4.3)、预签证书签名证书(1.3.6.1.4.1.11129.2.4.4) 和 OCSP 装订(1.3.6.1.4.1.11129.2.4.5)，大家能看到的就是第一个 OID，这是包含在 SSL 证书的，其他字段用于其他用途，这里就不具体细讲了，有兴趣的读者可以读一下 RFC6962 国际标准了解详情。

了解到 SSL 证书增加了一个新的 SCT 列表字段后，就具体讲一讲证书透明是如何实现的，为何这个机制能保障 SSL 证书的自身安全。而了解了这个安全机制后，就能理解为何零信技术投入研发力量研发了国密证书透明来保障国密 SSL 证书的自身安全，并且正在推动制定证书透明国密标准。

谷歌于 2013 年 6 月推出 RFC6962 标准后就开始打造证书透明生态，这个生态由证书透明日志系统、浏览器、CA 系统和监督系统等四个部分组成。浏览器谷歌有，没有问题，所以谷歌首先是研发和开源了证书透明日志系统，就是证书备案系统，要求 CA 在签发每一张 SSL 证书给用户之前把这张预签证书提交到证书透明日志系统上获得一个日志系统的签名数据(SCT)，

CA 把这个签名数据写到 SSL 证书中就是上面大家看到的 SCT 列表字段的数据，写入 SCT 列表数据后的 SSL 证书才能给用户部署使用。



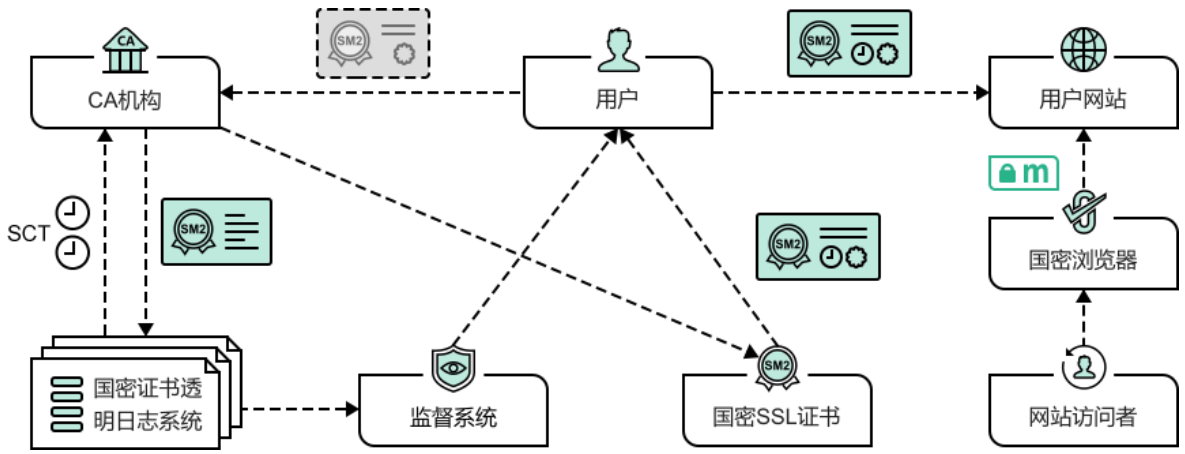
由于 CA 签发的 SSL 证书已经在给用户之前就已经在证书透明日志系统备案，而这个日志系统是全球公开可查询的数据库，并且是采用区块链一样的默克尔树哈希技术，使得 CA 的证书签发行为是不可否认的，因为这个基于默克尔树的数据库是只能追加数据而不能修改数据的。这个公示证书签发行为之所以称之为透明就是因为这个数据全球实时公示，这个签发行为的公示就可以为这个生态中最重要的一环—监督系统提供可核查的数据了，任何人包括网站域名所有者都能在证书正式签发部署使用之前就能实时发现这张证书是否是网站域名所有者同意签发的 SSL 证书，这就高效地保证了任何错误签发或者恶意签发的 SSL 证书都能在第一时间被发现和被制止。笔者不得不佩服谷歌工程师们的巧妙解决方案，并在此对 RFC6962 标准的 3 位起草者 Ben Laurie(谷歌英国)、 Adam Langley(谷歌美国)、 Emilia Kasper(谷歌瑞士)表示敬意！

这个非常有效的能防止 SSL 证书滥发或误发的机制能成功运行，不仅需要有证书透明日志系统可用，而且浏览器也必须支持验证 SCT 数据，最重要的是 CA 机构在签发 SSL 证书必须支持这个机制，而很多 CA 机构的证书签发系统是第三方开发的 CA 系统，不支持这个新增加的字段。怎么办？谷歌拿出来杀手锏—如果证书中没有谷歌信任的证书透明日志系统签名的 SCT 数据，则浏览器不信任此 SSL 证书！这是因为谷歌浏览器已经拥有了超过 50%的市场份额，这个杀手锏是有威力的。即便如此，从 2013 年 6 月谷歌提交 RFC6962 标准，谷歌就开始推广证书透明机制，但是直到 2018 年 7 月 24 日才从谷歌浏览器 68 版本真正实现了不信任没有 SCT 数据的 SSL 证书，显示为“不安全”，如下左图所示，大家可以实际访问一下截图的网址并查看一下这张 SSL 证书是否有 SCT 列表这个字段(当然没有)。从谷歌发布 RFC6962 到谷歌浏览器不信任没有透明备案的 SSL 证书，这个过程整整花了 5 年时间，谷歌在此之前多次推迟实施强制证书透明政策的截止日期!可见这个实施过程有多难。但谷歌还是把这事干成了，

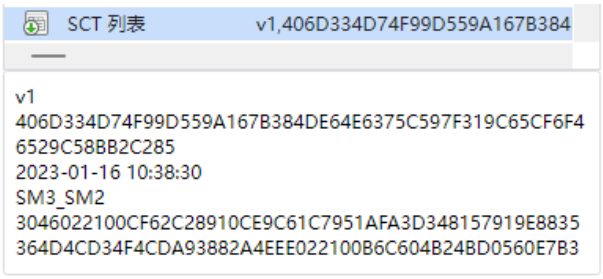
如下右图所示，截止到本讲文章发布的今天(2023 年 4 月 10 日)，已经有超过 91 亿张国际算法 SSL 证书都实现了证书透明！

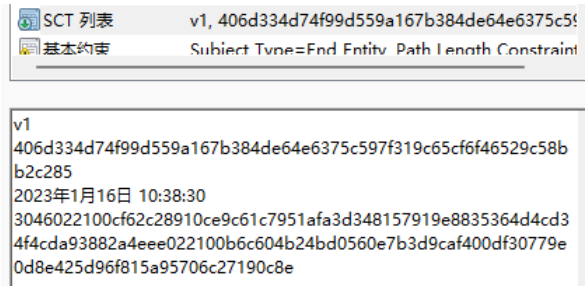
从上面的讲解，相信读者已经了解了证书透明是什么，并且已经了解了证书透明的作用。这个非常有效的能保障 SSL 证书自身安全的机制，很可惜在我国制定首个 SSL 证书国密标准《GM/T 0024-2014 SSL VPN 技术规范》和国家标准《GB/T 38636-2020 信息安全技术传输层密码协议(TLCP)》中并没有体现。但是，这并不表明国密 SSL 证书不需要证书透明，当然一样需要！所以，笔者就决定研发证书透明体系产品来证明和展示国密 SSL 证书的安全也需要证书透明，也是可以实现证书透明的，这就是国密证书透明体系。

同谷歌发起证书透明体系一样，零信技术也是从开发和部署国密证书透明日志系统开始，必须先有这个，这是基于谷歌开源的证书透明日志系统开发的，从系统底层改造支持国密算法，用国密算法生成日志签名密钥对，用国密算法数字签名日志数据。同时研发浏览器支持国密证书透明，研发 CA 系统能签发支持国密证书透明的国密 SSL 证书，从而独家打造了国密证书透明体系所需的所有产品和系统，这是因为我们没有谷歌这样的实力去强制要求 CA 机构和其他浏览器厂商必须支持国密证书透明，只能自己独立研发来验证和实施这个闭环系统。



大家可以使用零信浏览器查看一下国密 SSL 证书中的 SCT 列表是什么样的，如下左图所示。也可以用 Windows 证书查看器看看是什么样的，如下右图所示。对比可以看出，零信浏览器证书查看器和 Windows 证书查看器都能解析出国密 SCT 列表信息，只是由于 Windows 不支持国密算法而无法识别日志签名数据的算法而未显示签名算法，而零信浏览器则能明确告诉用户此 SCT 数据是采用国密 SM3_SM2 算法。





但是，零信浏览器并没有像谷歌浏览器一样对不支持证书透明的国密 SSL 证书显示为“不安全”，只是提示“国密证书不透明”，如下左图所示，这是因为除了我们自己的 CA 系统签发的国密 SSL 证书支持证书透明外，如下右图所示，显示“国密证书透明”和列出 SCT 列表中包含了哪几个国密证书透明日志系统，其他 CA 还不支持，零信浏览器信任的 CA 机构还在对接测试国密证书透明日志系统和升级国密 CA 系统中。谷歌花了 5 年时间实现了显示“不安全”，估计我国至少需要一年时间，原计划 2023 年 7 月 1 日以后零信浏览器会像谷歌浏览器一样对不支持证书透明的 SSL 证书显示为“不安全”，估计这个计划会推迟实施。希望随着证书透明国密标准的建立，能加快普及实现国密证书透明的步伐。

总之，为了保障 SSL 证书的安全可信，不仅需要浏览器的可信根认证计划，而且还需要证书透明备案计划，前者是为了保证 SSL 证书在签发之前的安全，CA 有能力签发 SSL 证书，而后者则是保证 SSL 证书在签发后的安全，这两个计划相辅相成，缺一不可，也就是大家常听到的“事前审批、事中和事后监管”，只有这样才能保证 SSL 证书的安全可靠供给，国际 SSL 证

书如此，国密 SSL 证书也应该如此。

下一讲内容预告 | 第 9 讲 SSL 证书是如何生产出来的?

本讲详细讲解 SSL 证书是如何生产出来并交付给用户的，当然包括国际 SSL 证书和国密 SSL 证书，只有了解了这整个生产过程才会理解为何中国 SSL 证书市场由西方 CA 所垄断，才会思考如何避免国密 SSL 证书市场不会全盘沦陷。

王高华

2023 年 4 月 10 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。