# 《证书透明规范》商密标准与商密证书透明生态

由零信技术牵头制定的商密标准《证书透明规范》已经批准立项制定，本文讲讲这个标准的制定过程，也讲一讲大家关心的与标准相关的一些关键技术，并结合讲一讲零信技术成功打造的商密证书透明生态产品。具体话题有：

(1) 为什么必须制定证书透明商密标准？

(2) 《证书透明规范》与 RFC6962 国际标准有哪些不同？

(3) 零信技术打造的商密证书透明生态产品有哪些？是否符合《证书透明规范》？

(4) 哪些产品厂商应该支持《证书透明规范》商密标准？零信技术能提供哪些支持？

## 一、 为什么必须制定证书透明商密标准？

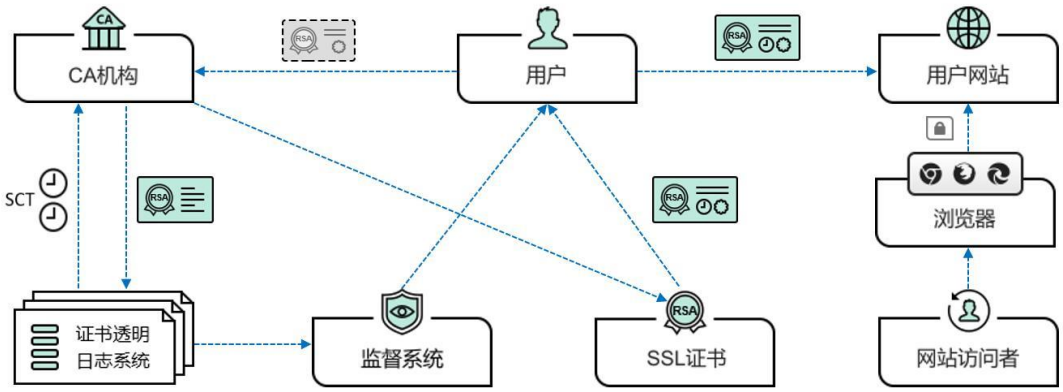
2022 年 2 月 24 日发生了俄乌冲突，美国 CA 就开始吊销了俄罗斯政府和银行网站使用的 RSA 算法 SSL 证书，20 天内吊销了三千多张，几乎覆盖了所有政府网站和银行网站，并同时不再为这些网站签发新的证书。这个“断供”和“禁用”SSL 证书的恶性互联网安全事件非常值得我国高度警惕，在当前非常不确定的国际局势下，我国政府网站和银行网站部署的 RSA 算法 SSL 证书也极有可能同样遭遇“禁用”和“断供”！所以，我国必须未雨绸缪，把普及商密算法 SSL 证书来保障我国互联网安全提高到第一紧急处理任务上来，这也是《密码法》合规的迫切需求。

而要想普及应用商密 SSL 证书，我们必须同国际 SSL 证书的普及应用对比分析差距，我们还缺什么？已经有 CA 机构能签发商密 SSL 证书，已经有浏览器支持商密 SSL 证书和商密算法实现商密 HTTPS 加密，那商密 SSL 证书还缺什么？还缺证书透明保障机制！

大家都知道，根证书信任计划是保障 SSL 证书安全的一个重要技术和管理手段，浏览器和操作系统只信任通过苛刻标准认证的根证书签发的 SSL 证书。而目前通过四大浏览器(谷歌、苹果、微软和火狐)认证的 CA 机构和 CA 根证书有上百个，如果这些 CA 机构工作失误而错误签发了浏览器信任的 SSL 证书怎么办？如果这些 CA 系统被攻击而恶意签发了浏览器信任的用于攻击的 SSL 证书怎么办？

据统计，google.com 和 gmail.com 是恶意签发 SSL 证书最多的域名之一，为了解决这个令谷歌头疼的问题，谷歌就发明了证书透明(Certificate Transparency)，并牵头成为了 RFC6962 国际标准，要求所有 CA 机构签发的每一张 SSL 证书都必须在签发用户证书之前把预签证书提

交到证书透明日志系统去备案，拿到日志系统的一个证书签发时间戳数据(SCT)并把此数据写到签发给用户的 SSL 证书中，谷歌浏览器才会信任这张已经透明公示和备案的 SSL 证书。第三方监督和审计机构就可以在 SSL 证书签发交付给最终用户之前获得某个 CA 给某个域名签发了 SSL 证书的信息，就可以实时监督这张 SSL 证书是否是用户自己申请的证书还是错误签发或恶意签发的 SSL 证书，如果是错误签发或恶意签发的 SSL 证书就可以要求 CA 机构及时吊销这张证书，从而避免了错误签发的 SSL 证书被使用。




这套非常有效的公开透明公示 CA 系统的证书签发行为机制自 2013 年开始已经成功保障了全球 **114** 亿多张 SSL 证书的安全，但是这套非常好的保障机制不支持商密算法和商密 SSL 证书。所以，为了保障商密 SSL 证书的安全，我国必须建设支持商密算法和商密 SSL 证书的证书透明机制，这个机制的核心就是要先制定证书透明商密标准，标准先行，使得整个证书透明保障体系就可以依据标准来建设，从而保障商密 SSL 证书的自身安全和保障商密 HTTPS 加密的安全。

也就是说，通过对标分析国际 SSL 证书的信任体系和保障体系，我们发现商密 SSL 证书的普及应用还缺证书透明保障机制，那我国就应该建设这个保障机制，也就必须先制定证书透明商密标准。

## 二、 《证书透明规范》与 RFC6962 国际标准有哪些不同？

上面分析了我国必须参考证书透明国际标准制定自己的证书透明商密标准，所以，《证书透明规范》商密标准草案就是完整地参考和采用了国际标准 RFC6962，但把证书透明日志系统的日志签名密钥算法和日志签名算法由 ECC 算法改为 SM2 算法，哈希算法由 SHA-256 改为 SM3 算法。这是最主要的修改，也是最主要的不同之处。证书透明日志系统是一个同区块链技术一样的采用默克尔哈希树实现只能追加数据不能修改数据的哈希链，这种数据库的核心是使

用何种算法计算数据的哈希和使用何种算法给哈希数据签名。国际标准是采用 ECC 算法和 SHA-2 算法来实现，而商密标准则采用 SM2 算法和 SM3 算法来实现。两个标准的所有不同之处对比表如下表。

| | 证书透明规范 | RFC 6962 | 备　　注 |
|---|---|---|---|
| **签名算法** | 5.1.4 | SM2 算法 | 2.1.4 | ECC 算法或 RSA 算法 | 目前运行的国际 CT 服务器都是用 ECC 算法 |
| **4 个专用 OID** | 1.2.156.10197.2.4.2<br>1.2.156.10197.2.4.3<br>1.2.156.10197.2.4.4<br>1.2.156.10197.2.4.5 | 1.3.6.1.4.1.11129.2.4.2<br>1.3.6.1.4.1.11129.2.4.3<br>1.3.6.1.4.1.11129.2.4.4<br>1.3.6.1.4.1.11129.2.4.5 | 红色部分为建议新分配的 4 个 OID，后面的 3 位数字可能为其他数字 |
| **默克尔哈希树的根** | sm3_root_hash | sha256_root_hash | SM3 哈希 |
| **TLS 和 SSL 名词** | SSL 证书 | TLS 证书 | SSL 证书已经成为了一个约定俗成的名字，本标准并没有同步改为 TLS 证书，由于 SSL 证书可以用于物联网设备，所以称之为服务器证书也不妥。 |
| **SSL 客户端** | 8.3 | 通常是指支持商密算法 SSL 证书的浏览器或移动 APP<br>10.1 | 要求浏览器不信任未透明的证书 | 5.2 | 通常指浏览器<br>7 | 建议浏览器不信任未透明的证书 | 常用 APP 必须支持商密 SSL 证书，因为现在用 APP 多于浏览器。<br>实际上谷歌浏览器现在就是不信任未透明备案的证书，制定标准的时间点不一样。 |
| **CA 机构** | 引言 | 预置信任根 | 1 | 预置信任根 | 仅限于提交信任根签发的证书 |
| **日志监视方** | 8.4<br>10.3 | 域名所有者和密码管理机构 | 5.3<br>7.2 | 只有域名所有者 | 可以是任何方，建议纳入密码主管部门的日常监管工作中 |
| **日志审计方** | 8.5 | 5.4 | 可以是任何方，建议审计标准把 CT 数据作为审计依据之一 |
| **日志运营方** | | | 本标准并没有对日志运维方提出要求，谷歌浏览器有一些要求，如：系统可用性，这块可以考虑加到商密标准中。 |
| **其他** | | RFC 勘误表 | 已更新勘误表内容到商密标准 |

RFC6962 是证书透明的 V1 版本，虽然是 2013 年发布的，但是目前的分类仍然是 Experimental (实验类)，而其状态是被 RFC 9162 证书透明 V2 版本 Obsoleted (废弃)，而 RFC9162 版本的分类也是实验类。这就不能理解有立项评审专家提出为何商密标准不直接基于最新的 RFC 9162 制定的疑问，相信读者朋友也会提出这个问题，笔者在这里解释一下这个问题。

RFC 标准分为三类：标准跟踪类、非标准跟踪类和当前最佳实践类(BCP)，其中标准跟踪类又分为建议标准(Proposed)、草案标准(Draft)和正式标准，目前只有很少部分能成为草案标准，

成为正式标准则更是非常少，互联网上被广泛使用的协议规范大多数处于建议标准这个级别。而非标准跟踪类又分为实验类(Experimental)、情报类(Informational)和历史类(Historic)，实验类是指使用范围很有限的协议；情报类是指一些有关特定议题的互联网社区的信息，并不代表是社区共识和建议，仅供下一步考虑和验证是否成为实验类标准，RFC8998-TLS1.3 商密加密套件属于这一类。而历史类则是已经没有任何价值的历史标准。这是 RFC 2026 定义的互联网标准制定流程的各种不同的标准分类。

目前已经被广泛使用的 RFC6962 和更新标准 RFC9162 仍然属于非标准跟踪类的实验类，大家可能不能理解，其实国际标准的制定基于共识原则，但是最终这个标准是否被启用取决于这个标准牵头单位是否能推动这个标准落地。谷歌牵头制定了 RFC6962 标准后，就利用了谷歌浏览器的强势地位强制要求所有 CA 机构必须遵循这个标准，否则谷歌浏览器不信任 CA 签发的这张证书，这就厉害了。也就是说 CA 机构的根证书预置浏览器信任还不够，必须同时支持证书透明，一张 SSL 证书必须同时满足这两个要求才被信任。这就是使得处于实验类的 RFC6962 标准实际上已经成为了事实上的正式标准，已经有 105 亿多张 SSL 证书都支持这个标准。

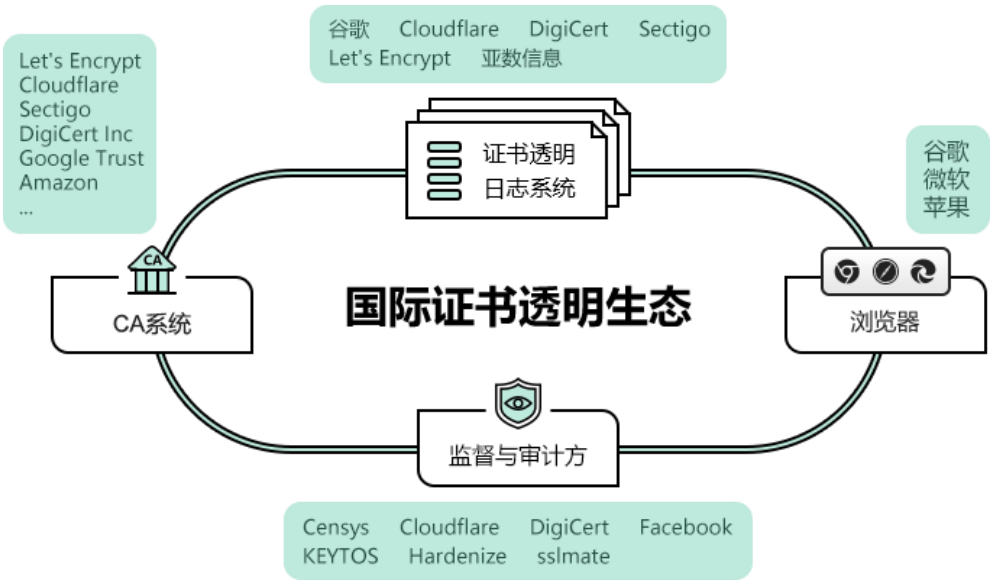
而为何零信技术牵头制定的证书透明商密标准是基于属于废弃状态的 RFC6962 标准？这主要是考虑到我国急需成熟的证书透明标准，因为目前所有浏览器信任的 CA 机构签发的国际 SSL 证书都是采用 RFC6962 V1 标准，V2 标准在国际上并没有正式启用，还没有 SSL 证书使用了 V2 标准的证书透明日志数据。如果将来 V2 标准成为了主流使用的标准，则商密标准也可以发布更新版本。

## 三、 零信技术打造的商密证书透明生态产品有哪些？是否符合《证书透明规范》？

相信有读者朋友看了第二部分的内容可能会认为，制定证书透明商密标准并没有什么技术含量，不就是翻译国际标准并把标准中的密码算法更换为商用密码算法吗？这个似乎谁都可以做，为何是零信技术牵头做这个呢？这真的是一个非常好的问题，必须在这一部分好好讲一讲。

笔者在第一部分就讲过：要想普及应用商密算法 SSL 证书来保障我国互联网安全，必须完善其自身安全保障体系，这就是证书透明体系。而这个体系涉及到浏览器厂商、CA 机构、日志运营方和第三方监督审计，所以需要有一个标准，这就是谷歌在 2013 年推出的 RFC6962 标准。但是，光有标准是不够的，必须建立一个基于标准的生态系统来支持这个标准落地应用。谷歌的做法是自己首先开发证书透明日志系统并运营这个系统，让 CA 机构有日志系统可以提交获取证书透明日志签名数据，可以公示 CA 签发的 SSL 证书。光这个还不够，应该有多个单

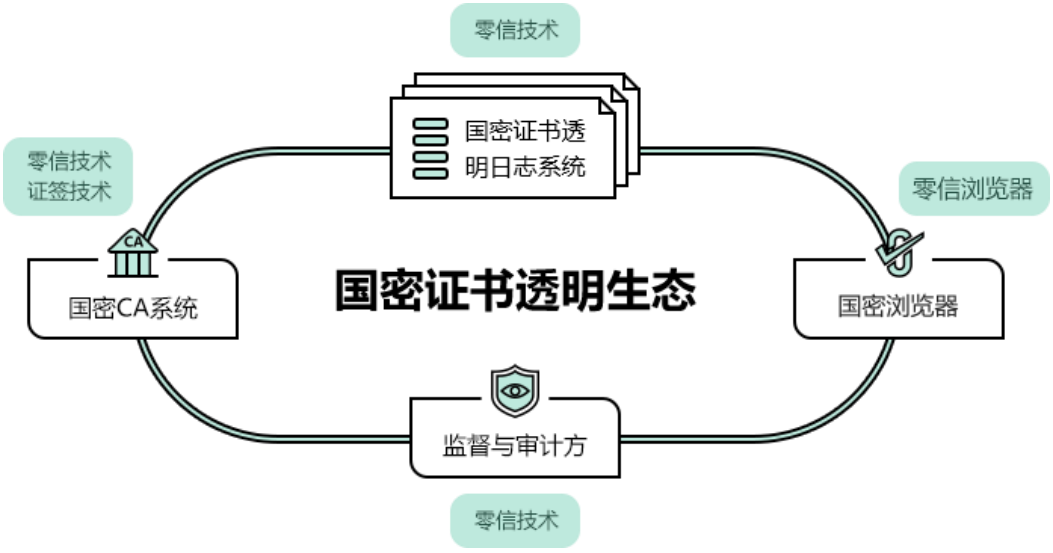
位运营证书透明日志系统，所以谷歌完全开源了证书透明日志系统，鼓励 CA 机构和其他第三方运营自己的证书透明日志系统，并要求 CA 机构必须同时把签发的预签证书提交到两家非谷歌运营的证书透明日志系统中获得 SCT 数据，并把这 3 个 SCT 数据同时写到 SSL 证书中，这样谷歌浏览器才会信任。这样就打造了一个有 CA 机构、CT 运营单位、浏览器厂商、监督和审计方等多方参与的一个生态系统，目前这个生态系统已经吸引了各方的多家公司参与，共同保障全球 SSL 证书的安全。为了打造国际证书透明生态，谷歌不仅牵头制定了 RFC 标准，而且运营了证书透明日志系统，谷歌浏览器支持证书透明，谷歌自己成立 CA 机构(Google Trust Service)为用户提供支持证书透明的 90 天免费 SSL 证书，自己带头打造证书透明生态的三个核心产品。




可以看出：谷歌作为制定证书透明标准的牵头单位是做了非常多的努力的，并且利用了其浏览器的垄断地位“迫使”CA 机构“就范”。谷歌不仅完全免费提供证书透明日志系统软件，而且完全开放日志系统数据库，鼓励多方参与，从而形成了证书透明生态。笔者在决定启动商密 SSL 证书支持证书透明这个项目时就是认为商密 SSL 证书要发展，也必须支持证书透明，但是零信技术既不是像谷歌这样的互联网巨头，而是一个 CA 老兵新创立的创业公司，也没有像谷歌那样拥有绝对市场份额的浏览器，那应该怎样才能推动商密证书透明这件事呢？

笔者的决定是自研商密证书透明生态所需的所有产品，自研产品形成这个生态体系，让商密证书透明生态在自家的产品体系中先落地，让业界不仅认识到建设这个生态体系的重要性，而且还能看到这个生态体系基于商密算法是可行的，这才有了今天大家看到了商密证书透明标准被密标委正式批准由零信技术牵头立项制定。

零信自研商密证书透明生态产品像谷歌一样当然也是必须先提供支持商密算法的证书透明日志系统，这是基于谷歌开源的证书透明日志系统研发，把日志签名密钥生成算法改为 SM2 算法，把日志数据的签名算法改为 SM2 算法，把默克尔树的哈希算法改为 SM3 算法，彻底改造开源的证书透明日志系统，从底层算法改造，自研完成商密证书透明日志系统，并运营 3 个商密证书透明日志系统，可以让商密 CA 系统提交商密 SSL 证书获取证书透明日志签名数据，实现商密证书透明备案公示。接着是自研商密 CA 系统，能签发支持商密证书透明的商密 SSL 证书，并把签发的预签证书提交到商密证书透明日志系统获取商密算法签名的 SCT 数据，把商密 SCT 数据写入到商密 SSL 证书中，就可以给用户交付支持商密证书透明的商密 SSL 证书了。这还不够，如果浏览器无法识别商密 SSL 证书中的 SCT 数据，证书透明保障体系仍然没有实现，所以又自研支持商密证书透明的浏览器，这就是基于谷歌开源 Chromium 开发的零信浏览器。这还不够，必须让用户能在线申请支持商密证书透明的商密 SSL 证书，并部署双 SSL 证书来落地使用支持商密证书透明的商密 SSL 证书，这就是已经上线的证签品牌 SSL 证书，这样零信浏览器才有实际部署的网站可以在实现商密 HTTPS 加密的同时验证商密证书透明日志数据。至此，零信技术实现了通过自研生态产品形成了商密证书透明生态体系，而任何有兴趣成为商密 SSL 证书监督和审计方都可以检索已经完全开放的零信商密证书透明日志系统的日志数据来监督已经签发的所有证签品牌和零信品牌商密 SSL 证书。




也就是说，零信技术是先依据国际标准采用商密算法成功研发了证书透明生态中的所有相关产品，证明了证书透明标准是可以改用商密算法来实现的。而为了能尽快证明这个生态的产品都能支持商密证书透明，我们不是仅仅提出这个概念去求各个相关厂商来支持商密证书透明，

而是全部自研产品验证其可行性，验证整个生态相关的产品的可行性。这样，即使我们没有谷歌那么多的强势资源，也一样能落地应用商密证书透明。当然，零信技术自己打造的商密证书透明生态产品只是一个自研生态，所以笔者非常感激密标委能在我们完成了自研生态产品后及时批准立项制定证书透明密码行业标准，这就弥补了零信技术所欠缺的像谷歌一样的强势市场地位的不足条件，使得商密证书透明能在我国尽快落地应用，而不是一个企业在自研自用。这必将加快商密证书透明的落地应用，使得商密证书透明能为保障商密 SSL 证书的安全真正发挥重要作用，从而实现普及商密 SSL 证书应用来保障我国网络空间安全。

那么，零信技术自研的商密证书透明生态产品是否全部遵循了《证书透明规范》商密标准草案呢？答案当然是肯定遵循的。但是，我们是自研产品在先，制定标准在后，所以，目前的产品应该属于仅遵循企业标准，标准草案还需要在各参与单位和业界的共同努力下尽快定稿，零信技术所有产品第一时间更新为遵循《证书透明规范》商密标准的产品。目前唯一待定的只有一项，就是证书透明规范中涉及到 4 个 OID 待定，标准草案建议由密标委在其 OID 体系中分配 4 个。而目前零信技术的所有商密证书透明产品仍然是使用国际标准中定义的 OID，其中这个 OID 属于谷歌的，所以，我们在起草标准时就建议像密码算法 OID 一样启用我国自己的 OID，待商密标准 OID 确定后更新所有相关产品即可实现全部遵循《证书透明规范》商密标准草案。

## 四、 哪些产品厂商应该支持《证书透明规范》商密标准？零信技术能提供哪些支持？

《证书透明规范》既然已经批准立项，我们就当现在的标准草案是一个等于 RFC 6962 国际标准分类—实验类，既然实验类的国际标准能成为事实标准，已经成功保障了全球 **114** 亿多张 SSL 证书的安全，那我们相信即使商密证书透明标准还没有正式发布，但只有大家都用起来，一样能保障商密 SSL 证书的安全，标准草案只有在大家不断使用过程中才能得到不断完善，才能到时正式发布一个真正适合我国国情的商密标准。

笔者在此诚邀商密证书透明生态相关的厂商现在就积极加入到商密证书透明生态建设中来，而不是等到发布正式标准时，现在参与制定和完善标准草案就有机会增加满足自己的产品的应用需求的内容。相关厂商包括但不限于：签发商密 SSL 证书的 CA 机构、支持商密 SSL 证书的浏览器厂商、有意运营商密证书透明日志系统的厂商、提供商密 CA 系统的厂商、有意监督和审计商密 SSL 证书和分析商密 SSL 证书签发情况的厂商等等。由于零信技术已经自研了商密证书透明生态的核心产品，所以零信技术有能力为生态厂商提供如下但不限于的最有力的支持：

(1) 为 CA 机构提供签发支持商密证书透明的商密 SSL 证书的技术支持，不仅已经开放了 3 个正式运营的商密证书透明日志系统可供零信浏览器信任的 CA 机构免费使用，用于提交预签商密 SSL 证书并获得商密 SCT 签名数据。并已设置开放一个测试专用的商密证书透明日志系统免费供各家 CA 机构测试，零信浏览器已预置信任这个测试 CT，供 CA 机构自测是否成功内嵌商密 SCT 数据和零信浏览器是否能验证内嵌的商密 SCT 数据。

(2) 对于为 CA 机构提供商密 CA 系统的厂商，欢迎遵循《证书透明规范》标准草案更新其 CA 系统，支持签发支持商密证书透明的商密 SSL 证书，提升其 CA 系统的核心竞争力。

(3) 对于有意提供商密证书透明日志服务的厂商，零信浏览器可以在测试合格后预置信任其商密证书透明日志服务，信任其签署的商密证书透明日志数据，CA 机构可以选择使用其商密证书透明日志服务。

(4) 对于有意支持商密证书透明的商密浏览器，可以测试已经内嵌商密证书透明 SCT 数据的零信官网，测试其浏览器是否能正常解析和验证 SCT 数据，并欢迎这些浏览器预置信任 3 个正在使用的零信商密证书透明日志服务系统。

(5) 对于有兴趣提供商密 SSL 证书监督和审计的厂商，欢迎依据《证书透明规范》标准草案通过 API 方式查询零信商密证书透明日志数据库，分析所有入库的商密 SSL 证书数据，提供各种商密 SSL 证书签发数据分析增值服务。

商密证书透明生态需要各方的积极参与，只有大家一起齐努力，才能真正让商密证书透明标准发挥最大的商密 SSL 证书自身安全保障作用，共同把保障商密 HTTPS 加密安全做贡献，共同为商用密码保障我国网空安全做贡献。

有诗为证：

证书透明保证书，生态建设是关键。

商密证书需透明，标准先行生态建。

王高华

2023 年 12 月 12 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。