国密重器，国庆钜献

2022 年 10 月 6 日，王高华于深圳

国庆节是举国同庆的节日，笔者认为除了“庆”，重点应该是“献“，拿什么给国庆献礼，这个更重要，因为国家的繁荣富强需要每个人和每个企业的奉献才能实现。

一、国庆献礼国密重器，很是欣慰

零信技术 9 月 30 日全球首发国密证书透明生态系统的两个核心产品-零信国密证书透明日志系统和支持国密证书透明日志系统的零信浏览器，两个创新产品都是全球独家率先创新发布。虽然这两个产品都是免费产品，不能带来直接的经济效益，但其社会效益和价值是巨大的，能有力保障我国国密 SSL 证书的安全，从而保障我国互联网安全。这就是零信技术的国庆钜献，能赶在国庆节发布的国密重器，很是了却了笔者多年的心愿，很是欣慰。

早在 2018 年 12 月份由中央网信办网络安全协调局、国家密码管理局指导，中国电子信息产业发展研究院主办的“**2018 网络空间可信峰会**”主题演讲中，我提出了建设“**中国网络空间可信生态建设框架**”的构想，其中的核心思想是参考国际体系建设我国基于国密算法的网络空间可信生态体系，当然核心是国密算法数字证书的全面应用，其中最重要的是国密 SSL 证书的部署应用。

峰会后，笔者带领研发团队重点研发国密 SSL 证书相关产品，并于 2019 年 4 月发布了全球首个中文国密算法根证书--国密 SM2 根证书，从那时起就计划参考国际证书透明系统研发国密证书透明系统，但是很遗憾的是由于种种原因一直未能付诸行动。去年 6 月份重新创业，终于可以没有任何约束的想做什么就做什么了，经过一年多的艰苦努力，克服了种种困难，终于把 4 年前想做的事情在普天同庆的国庆节完工上线了，笔者很是高兴和很是欣慰，特撰文同广大读者朋友分享这份快乐和相关知识。

证书透明为何重要，为何是谷歌牵头搞了一套证书透明系统并做成了 RFC 国际标准，这还得从谷歌自身作为 SSL 证书滥发的受害者说起，大家搜一下新闻就能发现多起非法签发 gmail.com, google.com 的 SSL 证书的报道，这些非法签发的全球信任的 SSL 证书当然是用于非法攻击 Gmail 邮箱，用于非法窃取邮箱密码和邮件机密信息。于是，谷歌就牵头搞出了证书透明系统，要求全球信任的 CA 在签发每一张 SSL 证书之前必须先把计划签发的 SSL 证书(预签证书)提交到谷歌证书透明日志系统来备案，公开透明披露每一张

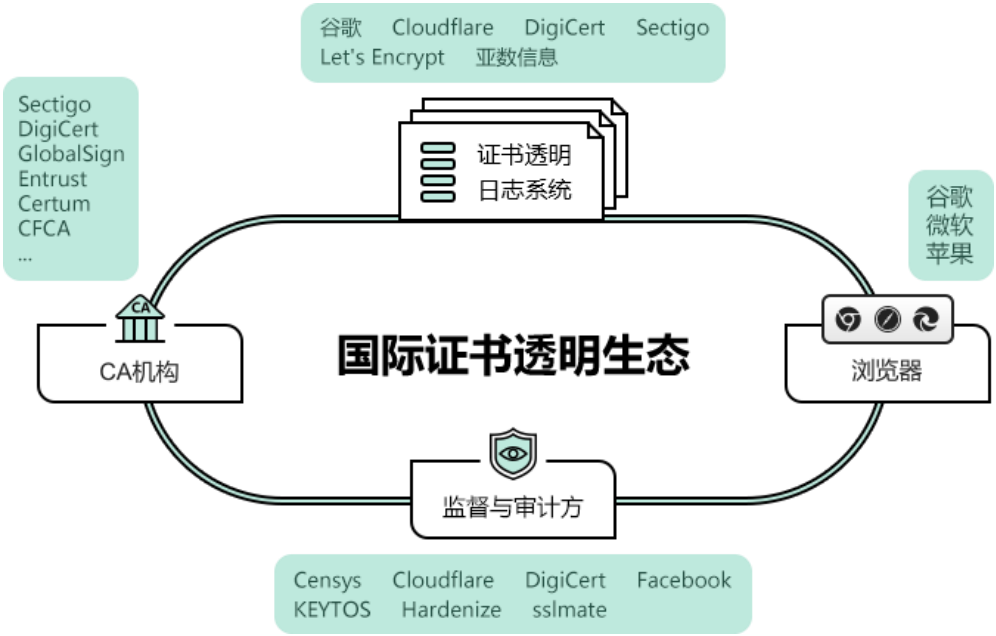
SSL 证书的签发行为，这就是为何叫“证书透明“。提交备案后证书透明日志系统会给 CA 系统返回一个已备案证明-一个由证书透明日志系统私钥签名的数字签名数据-SCT 数据，CA 系统必须把这个 SCT 数据嵌入在正式签发的 SSL 证书中，这张 SSL 证书才会被谷歌浏览器信任，这张 SSL 证书才有使用价值。

请对证书透明感兴趣的读者朋友参阅笔者的其他证书透明相关博客文章，本文不再重复已经写过的内容，仅讲一讲证书透明生态的各个参与者还有谁，以及应该如何建立我国国密证书透明生态。

二、国际证书透明生态，大获成功

为了方便下文的比较，本文把目前为全球 SSL 证书提供证书透明服务的生态体系称之为“国际证书透明”，这个生态体系从 2013 年开始已经成功保障了全球 75 亿张国际算法 RSA/ECC SSL 证书的安全。

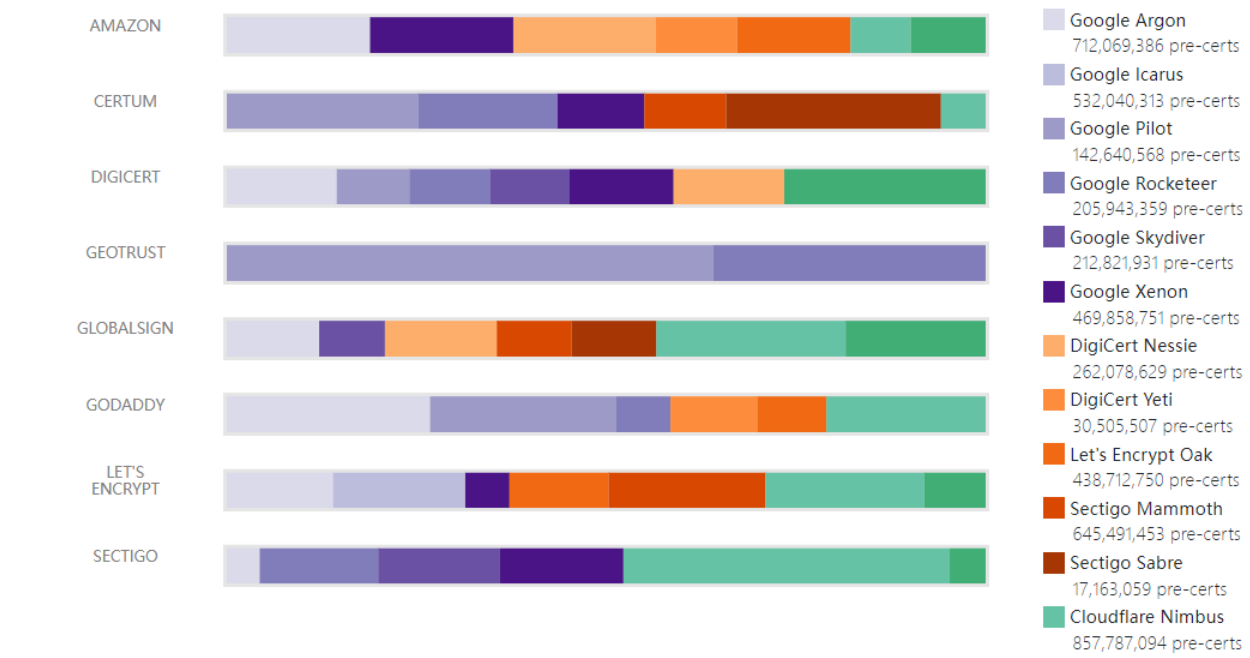
那么，国际证书透明生态是什么样的？有哪些参与者？当然第一个是谷歌。谷歌之所以能牵头搞成证书透明这事，当然离不开谷歌浏览器的影响力和市场占有率，谷歌发布了证书透明日志系统，首先就占领了道德高地—“透明”，其次当然是利用其浏览器的影响力拿出了杀手锏—如果 CA 签发的 SSL 证书不支持证书透明，谷歌浏览器就不信任，会有“不安全”警告！后来苹果浏览器也加入了助力证书透明的阵营，一样的不信任如果 SSL 证书不支持证书透明！再后来就是微软 Edge 浏览器的加入，也是一样有警告如果 SSL 证书不支持证书透明！这三大浏览器的全球市场占有率分别排名前一二三，合计高达 88%，曾经高达 40% 占有率的火狐浏览器不知为何不支持证书透明而跌到了第四位(3%)，从这个侧面可能反映出用户对证书透明的认可和重视，浏览器不支持证书透明就等于信任不透明签发的用于恶意攻击的 SSL 证书，这样的浏览器怎么能保障浏览器用户的上网安全呢？用户当然会抛弃它！浏览器是证书透明生态的第一个重要参与者。



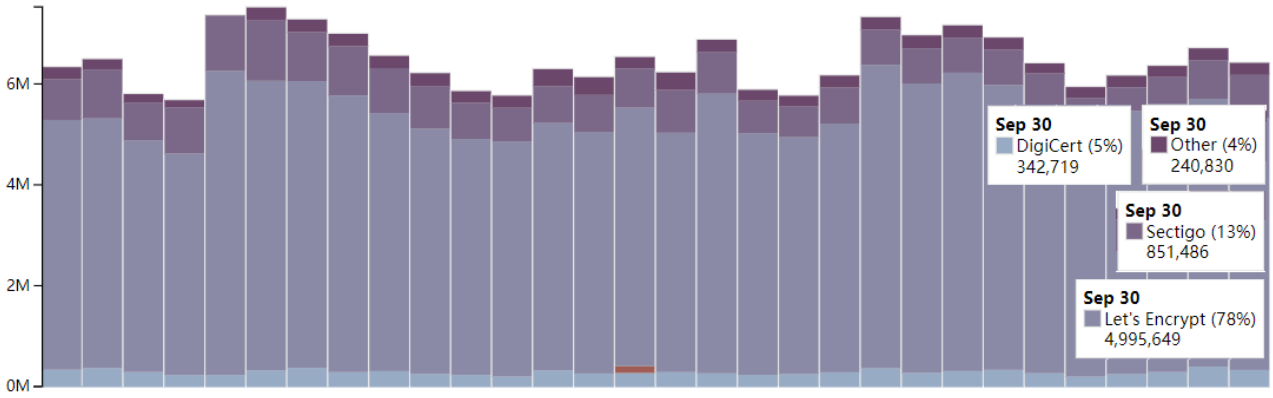
证书透明生态的第二个重要参与者当然是证书透明日志系统的运维者。必须先有证书透明日志系统，这是源头，还得由谷歌来牵头，谷歌不仅研发了证书透明日志系统，还把这个系统完全无条件开源了，鼓励大家一起来玩，鼓励多家部署和运维自己的证书透明日志系统来为 CA 机构提供证书透明日志服务。谷歌浏览器要求每张 SSL 证书必须有一个 SCT 来自谷歌自己的证书透明日志系统，其他 1 个或两个必须是其

他非谷歌运维的证书透明日志系统，以示公平公正和非独家。目前，通过谷歌浏览器认证并信任的证书透明日志系统参与者除了谷歌自己外还有：全球领先的 CDN 分发服务提供商 Cloudflare 和 4 家著名的 CA 机构：Sectigo、DigiCert、Let's Encrypt 和亚数信息。CA 机构运维自己的证书透明系统除了方便给自己签发的 SSL 证书实现证书透明日志服务外，也开放给其他 CA 机构免费使用。

下图为 Cloudflare 证书透明日志服务网站发布的各个 CT 系统使用情况的统计图，谷歌 CT 系统有 22.74 亿张预签证书，Cloudflare 有 8.57 亿张，Sectigo 有 6.62 亿张，DigiCert 有 5.67 亿张，Let's Encrypt 有 4.38 亿张。



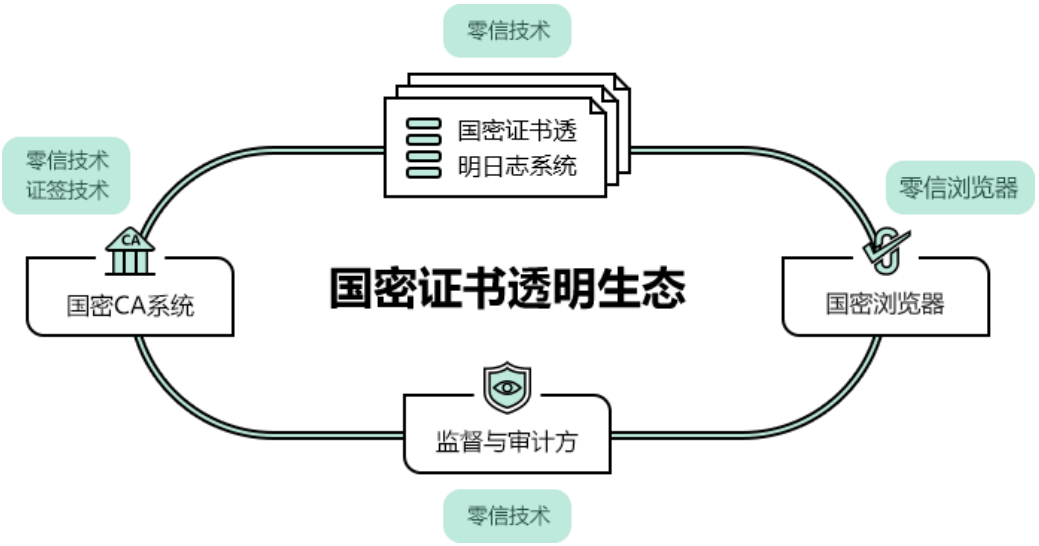
CA 机构是第三个参与者，既是证书透明生态的服务对象也是被监督的对象，目前全球有几十家 CA 机构签发的 SSL 证书都已经支持证书透明，所签发的每一种 SSL 证书都已经提交到以上通过谷歌认证和信任的证书透明日志系统中透明备案。下图为 9 月份每日在证书透明日志系统备案的全球 SSL 证书签发量直方图，9 月 1 日的全球签发量为 634.437 万张，9 月 30 日为 643.0684 万张，最高签发量为 9 月 6 日的 752.7091 万张。



最后一个重要的参与方为监督与审计方，这一方的职责是确保所有已经嵌入 SCT 数据的 SSL 证书在证书透明日志系统中可见，并观察日志中的可疑证书，用户可以订阅这些服务提供商的服务，以便及时收到通知。一些服务提供商提供 SSL 证书在线查询服务，有些如社交网络提供商-脸书(Facebook)为其用户提供一个监控服务—每次有 CA 机构签发了受监控的域名的 SSL 证书时，都会收到 Facebook 通知或 Webhook API 回调通知。这些服务都能帮助网站主及时发现可疑证书，有效保障网站主的合法权益。

三、国密证书透明生态，闪亮登场

由于国际证书透明生态只支持国际密码算法 RSA 和 ECC SSL 证书，不支持我国的国密算法 SM2 SSL 证书，所以，为了保障我国国密 SSL 证书的安全，我们也必须建立国密证书透明生态。那么，我国的国密证书透明生态建设情况如何呢？国密证书透明生态由零信技术全球独家提出，并于国庆节前一天闪亮登场，全球首发相关国密证书透明生态的两个重磅产品，包括全球首个支持国密算法的证书透明日志系统—零信国密证书透明日志系统和全球首个支持国密证书透明的浏览器—零信浏览器。而全球首个能签发包含国密 SCT 数据的国密 SSL 证书的国密 CA 系统已经研发完成，正在内测中，不久就会正式对外签发国密 SSL 证书。至于监督与审计方，目前零信证书透明日志系统已经提供基于 RFC6962 国际标准的证书透明日志数据查询 API，供有兴趣的各方公开查询，并计划提供 Web 方式在线查询服务。



相信读者可以看出，目前我国的国密证书透明生态才刚刚起步，零信技术独家打造整个生态的相关产品和服务，但是仅仅一家公司是无法真正建立起一个生态系统的。希望我国能建设国家级国密证书透明日志系统，把国密 SSL 证书的透明备案提高到同网站域名备案一样的高度和重视程度。也希望有更多的公司也能提供国密证书透明日志服务，希望有更多的支持国密 SSL 证书的浏览器支持国密证书透明，希望所有能签发国密 SSL 证书的 CA 机构尽快支持国密证书透明，希望有更多的公司能提供国密 SSL 证书的监督和审计服务，因为证书透明生态需要多个证书透明相关的系统和服务共同协作工作，从而发挥更大的国密 SSL 证书和国密 https 加密的安全保障作用，从而切实有力保障我国互联网安全。

四、真实体验国密证书透明生态

请想了解和体验国密证书透明生态产品是什么样的读者 下载 安装零信浏览器，并使用零信浏览器访问零信官网：https://www.zotrus.com，亲身体验一下国密证书透明生态是什么样的。

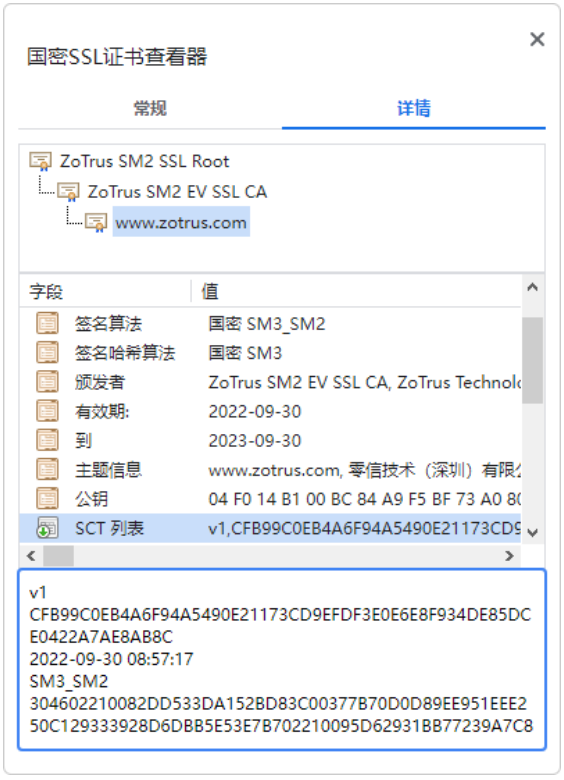
1. 体验支持国密证书透明的浏览器是如何展示国密证书透明的

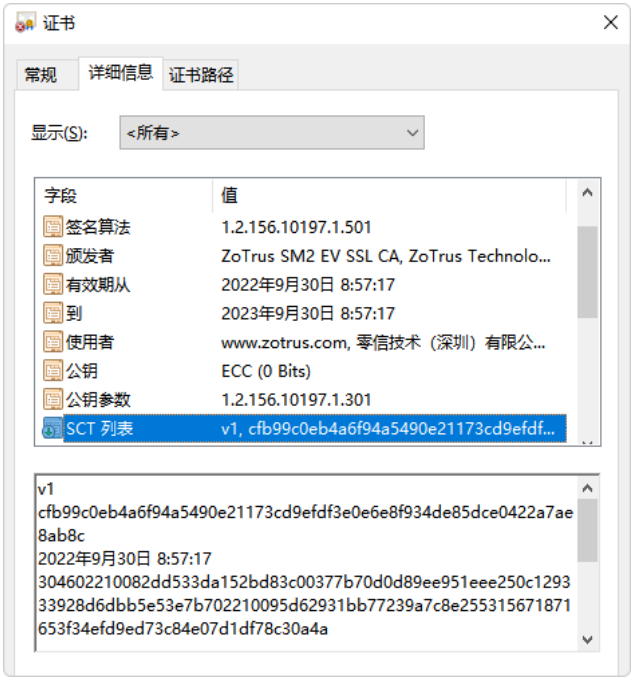
如下图所示，点击浏览器地址栏的国密加密标识(m)，会显示此网站是采用国密加密的，是国密合规和密保合规的。第二部分是展示此网站部署的国密 SSL 证书支持国密证书透明，并且内嵌了 3 个国密证书透明日志服务的 SCT 数据，并显示具体 3 个证书透明日志服务的服务网址，请注意这些网址是国密证书透明日志服务系统网址，是不能通过浏览器来访问的，但是去掉/2023 的网址是可以使用浏览器来访问的，会跳转到国密证书透明官网(sm2ct.cn)。可以点击下面的了解详情，可以详细了解国密证书透明标识的含义。

大家再使用零信浏览器访问一下中国银行的个人网银系统：https://ebsnew.boc.cn/boc15/login.html，这是我国目前唯一一个部署了国密 SSL 证书采用国密算法加密的网银系统，点击浏览器地址栏的国密加密标识(m)，会显示此网站是采用国密加密的，是国密合规和密保合规的。第二部分是展示此网站部署的国密 SSL 证书是否支持国密证书透明，显示“国密证书不透明”，说明这个网站部署的国密 SSL 证书目前还不支持国密证书透明。这个目前来看，仍属于正常状态，因为之前我国并没有国密证书透明日志系统可以用于各家 CA 机构获取国密证书透明日志 SCT 数据。现在，我国已经有了可用的国密证书透明日志服务，笔者相信签发此证书的 CA 机构会尽快支持国密证书透明的。

2. 体验支持国密证书透明的国密 SSL 证书是什么样的

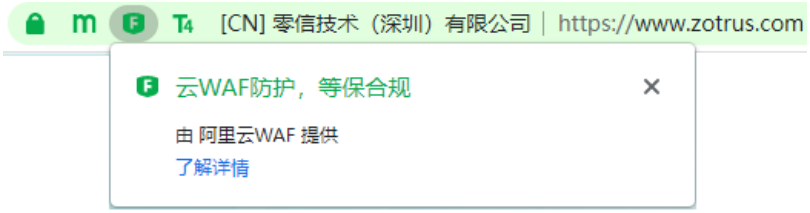
如下图所示，点击加密锁标识，可以查看国密SSL证书，点击详情就可以向下滚动就能看到国际SSL证书一样的SCT列表，会显示证书中嵌入的3个国密证书透明SCT数据，其中第4行显示“SM2_SM2”表明SCT数据的签名算法为SM2算法。而国际证书透明SCT数据会显示为“SHA256 ECDSA”。这张国密SSL证书由全球首个能签发包含国密证书透明日志数据的国密SSL证书的零信国密CA系统签发，是全球第4张包含了国密证书透明SCT数据的国密 EV SSL证书，第1张是给测试网站sm2test.zotrus.cn 签发的国密SM2 OV SSL证书。

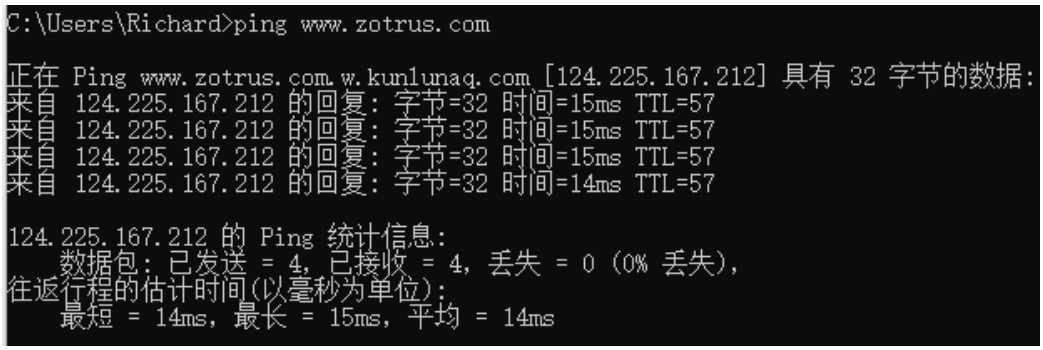




3. 体验零改造国密 https 加密和云 WAF 防护是什么的

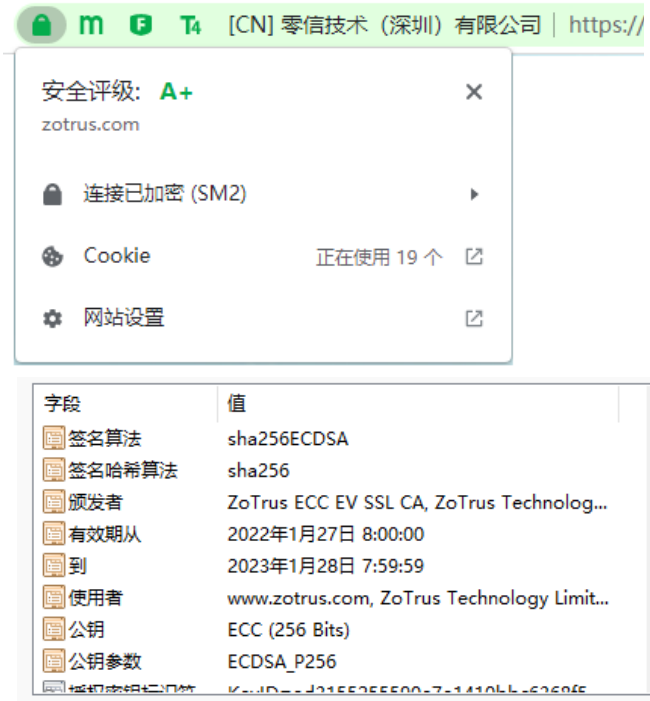
如下图所示，点击云 WAF 防护标识(F)，会显示这个网站由阿里云 WAF 提供安全防护，并显示“云 WAF 防护，等保合规”。零信官网使用的是全球首个支持全自动部署内嵌国密证书透明 SCT 数据的国密 SSL 证书实现国密 https 加密的零信网站安全云服务，用户只需设置 3 次域名解析，零改造实现国密 https 加密。这是零信技术基于阿里云 CDN+WAF 服务提供的 API 接口打造的全自动配置国密 SSL 证书的零改造网站安全云服务，不仅一键实现国密 https 加密，而且一键实现云 WAF 防护和 CDN 高速内容分发服务，多维度保障网站安全。





4. 体验双证书自适应加密算法 https 加密是什么样的

也许有读者会说：很好，零信官网已经部署了支持国密证书透明的国密 SSL 证书实现了国密 https 加密，但是如果我使用不支持国密算法的谷歌浏览器还能访问零信官网吗？当然是可以的。如下左图所示，这是使用零信浏览器访问零信官网的截图，点击加密锁标识，会显示“连接已加密(SM2)”，意思是同服务器的连接采用了国密 SM2 算法实现 https 加密。如下中图所示，这是使用谷歌浏览器访问零信官网的截图，点击加密锁标识，会显示“连接是安全的”，继续查看证书则可以看出这是一样 ECC SSL 证书。也就是，零信官网部署的双算法双 SSL 证书，会根据用户使用不同的浏览器自适应加密算法实现 https 加密。这是最佳 https 加密部署实践，即保证了网站的国密合规要求，保证了网站在 RSA/ECC SSL 证书在不可预见的不可控情况下被吊销而不受任何影响，同时保证了最大的兼容，使得所有浏览器都可以实现无缝的 https 加密体验。



王高华

数字签名者：王高华
日期：2022.10.06 09:43:37 +08'00'