商用密码 HTTPS 加密生态建设

本篇文章来源于**赛迪密码信息安全**公众号，作者：王高华，2023 年 1 月 17 日

摘要：

我国正在大力推广商用密码在各行各业的全面应用，取得了一些可喜的成绩，很多应用都几乎已经完全替代了国际密码算法。但是，在网站 HTTPS 加密应用上进展缓慢，几乎所有政务网站和网银系统仍然还是采用国际密码 RSA/ECC 算法实现 HTTPS 加密。而俄乌冲突发生后，大量的俄罗斯政府网站和银行网站部署的 RSA 算法 SSL 证书都被吊销和断供，这警示了我国必须加速普及商用密码 SSL 证书的部署应用。但是，我国的商用密码 SSL 证书起步晚，各种相关的技术规范和解决方案都很不完善，并且相关系统软件都必须改造支持商用密码算法，这势必影响了商用密码 SSL 证书的快速普及应用。本文详细介绍了如何建立我国商用密码 SSL 证书供给生态和应用生态，能有效地完善我国商用密码 HTTPS 加密生态体系，从而实现商用密码 SSL 证书的快速普及应用，普及应用商用密码来可靠地保障我国互联网数据通信安全。

一、 引言

在赛迪研究院主办的“2018 网站空间可信峰会”上，作者首次提出了“中国网络空间可信生态建设框架”的构想，并提出了商用密码 SSL 证书的应用思路--先“双轨制”再慢慢变成“单轨制”，这个“双轨制”就是部署双算法双 SSL 证书过渡，在商用密码应用生态成熟后就很自然地实现了“单轨制”(仅需部署商用密码 SSL 证书)。通过密码业界在过去的 4 年的不断努力，特别是《密码法》在 2020 年 1 月 1 日的正式施行，商用密码 SSL 证书的各种生态产品和生态建设都得到了长足发展，并且日趋完善。

普及应用商用密码 SSL 证书的触发点就是去年 2 月份的俄乌冲突发生后的一周内俄罗斯政府和银行网站使用的 RSA 算法 SSL 证书被吊销了三千多张，导致大量的政府网站和银行网站无法正常访问而瘫痪，同时俄罗斯政府网站和银行网站也不再允许申请新的 SSL 证书，这就是 SSL 证书的“断供”，也让俄罗斯措手不及！这给我国政府网站和银行网站敲响了安全警钟，因为我国政府网站和银行网站也都是在使用国际密码体系的 RSA 算法 SSL 证书！这个互联网安全事件让政府主管部门、安全业界都充分认识到了普及应用我国商用密码算法的商用密码 SSL 证书的重要性和紧迫性！所以说，这个事件让业界上下都形成了共识，这个非常重要！

作者早在 2019 年第七届互联网安全大会的演讲上指出“我国做好 RSA SSL 证书断供和吊销的准备了吗？”，当时就有“专家”反驳，说是“危言耸听”！而现在，这事真实发生在俄罗斯身上了，让大家马上都有了共识，这就是商用密码 SSL 证书到了普及应用阶段的触发点！深深地触动了密码业界达成共识，并开足马力增强商用密码 SSL 证书的供给能力，提供充足的能满足各个应用方的部署需求的解决方案。

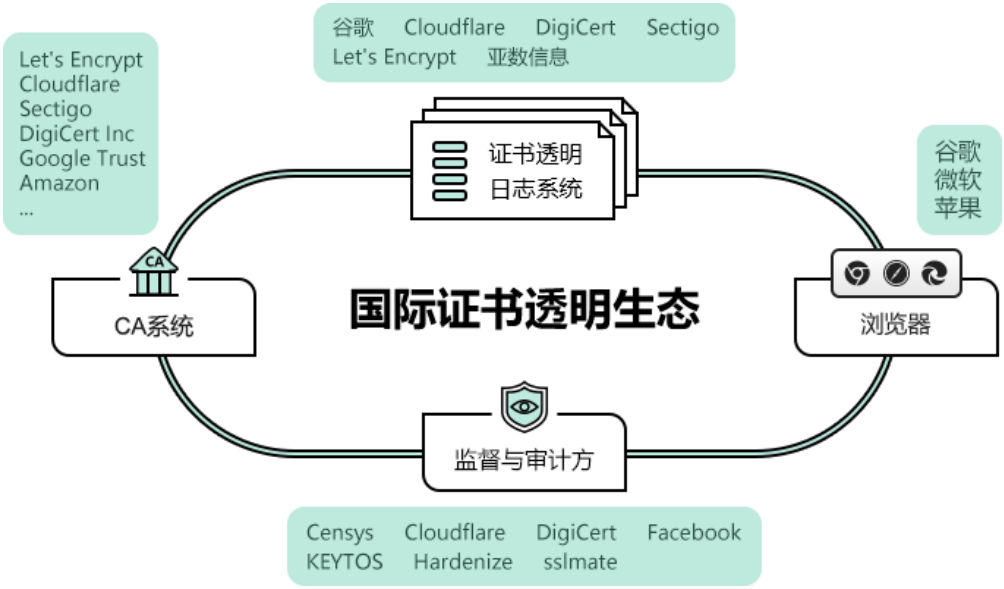
二、 国际密码 HTTPS 加密生态体系介绍

目前，基于国际密码体系实现的 HTTPS 加密在全球得到了普及应用，有力保障了全球互联网的数据通信安全，从 2013 年开始，已经可靠地签发了 84 亿张国际密码算法 RSA/ECC SSL 证书。国际 HTTPS 加密生态体系主要包括国际证书透明生态体系和国际证书自动化管理体系，这两个体系实现了国际 SSL 证书的可靠安全供给和快速部署应用。

2.1 国际证书透明生态体系

国际证书透明生态体系是国际密码 HTTPS 加密生态体系的第一个重要生态，这是由谷歌牵头设计的体系，包括证书透明日志系统(俗称：证书备案系统)、支持证书透明的浏览器、能签发支持证书透明的 SSL 证书的 CA 系统(证书提供商)和利用证书透明日志系统数据监测和监督证书签发行为的第三方服务。这个生态的四方都有多个厂家共同参与，共同保证了国际密码算法 SSL 证书的可靠供给。

国际证书透明生态的一个重要参与者是谷歌。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，一样的不信任不支持证书透明的 SSL 证书！再后来就是微软 Edge 浏览器的加入，也是一样对不支持证书透明的 SSL 证书不信任！如果浏览器不支持证书透明，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？浏览器是证书透明生态的第一个重要参与者。



国际证书透明生态的第二个重要参与者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，还是由谷歌来牵头，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，鼓励多家公司部署和运维自己的证书透明日志系统来共同为 SSL 证书提供商(CA 机构)提供证书透明日志服务。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的证书透明日志系统外还有：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。

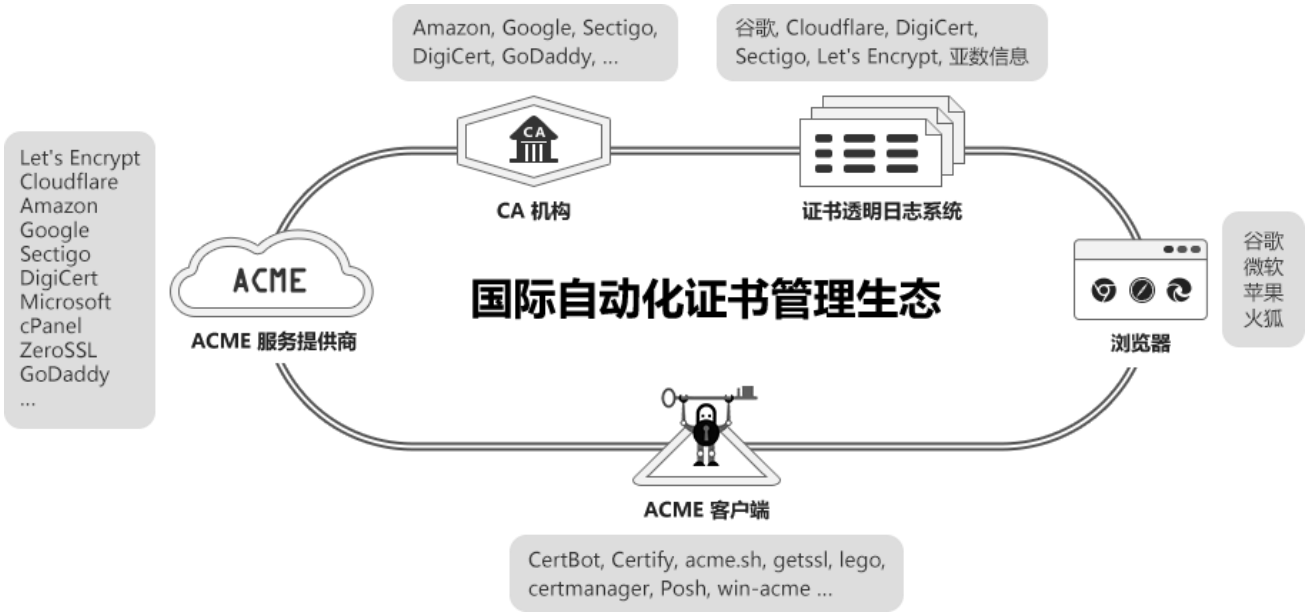
SSL 证书提供商(CA 机构)是第三个参与者，既是证书透明生态的服务对象也是被监督的对象，目前全球有几十家 CA 机构签发的国际 SSL 证书都已经支持证书透明，所签发的每一种 SSL 证书都已经提交到以上通过谷歌认证和信任的证书透明日志系统中透明备案。

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，这些服务都能帮助网站业主及时发现可疑证书，有效保障网站业主的合法权益。

2.2 国际证书自动化管理体系

国际证书透明生态体系有力保障了全球 SSL 证书的可靠可信供给。但是，国际 SSL 证书的部署在 2015 年之前发展都比较缓慢，每年平均增长 5%左右，这个缓慢的增长速度的关键制约因素是申请和部署 SSL 证书太难了。但是，2015 年 Let's Encrypt 开始实现自动化提供免费 SSL 证书后，短短的三年就把 SSL 证书普及率从 30%快速提升到 80%。特别是在 2019 年出台

了 RFC8555 ACME(自动化证书管理环境)国际标准后，使得现在的全球 SSL 证书中自动化申请和部署比例已经高达 85%。这给了我们很大的启示，那就是：普及商用密码 SSL 证书不能走传统的人工申请和部署证书的老路，必须走自动化申请和部署证书的新路。



三、 商用密码 HTTPS 加密生态体系建设

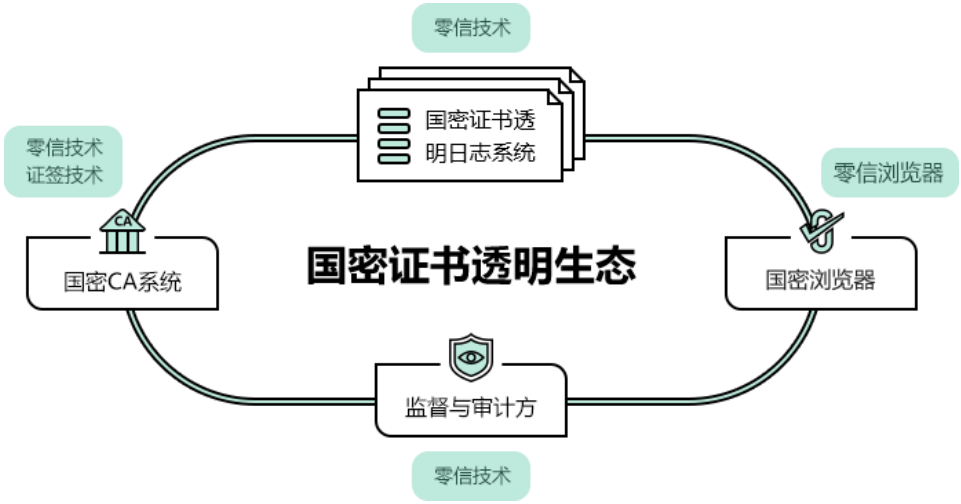
国际密码 HTTPS 加密生态体系保障了全球 84 亿张国际算法 SSL 证书的安全可信，成功实现了国际算法 https 加密来保障全球互联网的数据通信安全。但是，这个体系不支持商用密码算法，无法用于保障商用密码 SSL 证书的安全，无法用于快速部署应用商用密码 SSL 证书来实现商用密码算法 HTTPS 加密。我国必须参考这个国际体系来建设支持商用密码算法的体系，包括商用密码证书透明体系和商用密码证书自动化管理体系，以确保能成功实现安全可靠的商用密码 SSL 证书供给和快速部署应用实现商用密码 HTTPS 加密。

3.1 商用密码证书透明体系建设

虽然从 2019 年开始有多家国内 CA 机构开始签发商用密码 SSL 证书，也有国产浏览器支持商用密码 SSL 证书，但是，这个生态中最重要的监管系统没有建立，没有支持商用密码算法的证书透明日志系统，商用密码 SSL 证书当然也就无从下手支持商用密码证书透明了，浏览器也就无从下手支持商用密码证书透明了，当然监管方也就无处获取证书签发数据而行驶监管职能了，我国必须建立参考国际证书透明生态体系的商用密码证书透明生态体系。可喜的是，

零信技术于 2022 年 11 月 8 日在乌镇 2022 世界互联网大会上首发并启用了全球第一个商用密码证书透明日志系统，并发布了商用密码证书透明相关生态产品，成功打造了国密证书透明生态(SM2 CT)，这个生态体系发布后得到了密码业界的高度认同和认可。

目前，商用密码证书透明体系已初见成效。不仅零信技术和证签技术签发的商用密码 SSL 证书支持商用密码证书透明，已经有多家 CA 机构开始着手改造现有 CA 系统以支持商用密码证书透明。不仅零信浏览器支持商用密码证书透明，已经有几家国产浏览器开始计划升级支持商用密码证书透明。最可喜的是，商用密码主管部门也有计划建设国家级商用密码证书透明日志系统以行使作为主管机构的监管职能，也有几家企业有兴趣运营商用密码证书透明日志系统。也有第三方市场调查机构有兴趣提供基于商用密码证书透明日志数据的证书市场分析服务。这些可喜的一致行动会快速形成商用密码证书透明生态，我国一定能很快具有商用密码 SSL 证书的可靠供给能力，为商用密码 HTTPS 加密普及应用提供了安全可靠的“货源”。



3.2 商用密码证书自动化管理体系建设

国际 SSL 证书的快速普及应用得力于国际 SSL 证书自动化管理生态体系的建设，包括 ACME 国际标准(RFC 8555)的建立和多个厂商提供国际 SSL 证书自动化管理服务。这是一条能实现快速部署 SSL 证书的新路，但是，国际证书自动化管理体系只支持国际密码算法 RSA/ECC SSL 证书，不支持商用密码算法 SSL 证书，这条自动化的新路不是我们的路，我国也必须建立支持商用密码算法的证书自动化管理之路。

可喜的是，零信技术鼎力打造了商用密码 SSL 证书的第二个生态—国密证书自动化管理生态(SM2 ACME)，这个生态专为商用密码 SSL 证书的快速普及应用打造。这个生态包含了商用密码证书透明生态中的多个产品，包括增加了国密 ACME 服务系统的零信云 SSL 系统、双

算法双 SSL 证书、国密证书透明日志系统、零信浏览器，同时创新研发了国密 ACME 客户端、国密 HTTPS 网关和网站安全云服务。

国密 ACME 客户端和国密 ACME 服务系统参考国际 ACME 标准设计，用户只需在服务器安装国密 ACME 客户端软件-SM2cerBot，一键实现国密 SSL 证书和国际 SSL 证书的双算法双 SSL 证书的自动化申请和部署，自动化实现商用密码 https 加密。而对于无法在服务器上安装国密 ACME 客户端软件的用户，则可以选用部署内置国密 ACME 客户端实现自动化部署双 SSL 证书的国密 HTTPS 网关，实现原 Web 服务器零改造和零安装证书的商用密码 https 加密。而对于不想部署或无法部署硬件网关的用户，则可以选用零信网站安全云服务，只需做域名解析就可以零改造和零安装证书的实现商用密码 https 加密、云 WAF 防护、CDN 分发和网站可信认证四位一体的网站安全服务。

有了国密证书自动化管理生态产品和解决方案，普及商用密码 SSL 证书实现商用密码 HTTPS 加密就变成非常容易了，就可以实现像国际 SSL 证书在实现了自动化部署后一样的快速增长，普及商用密码 SSL 证书应用就指日可待了，必须在扫除了商用密码 SSL 证书的使用障碍后才能得到快速普及使用，这一点已经在国际 SSL 证书的快速普及得到验证和印证。

四、 结束语

国际 SSL 证书之所以在保障全球互联网数据通信安全大获成功，得力于两个生态体系的建设，一个是国际证书透明生态，有力保障了国际 SSL 证书的安全可靠供给；一个是国际证书自动化管理生态，为快速部署国际 SSL 证书提供了技术手段和解决方案。我国必须参考这个两

个生态建设商用密码证书透明生态和商用密码证书自动化管理生态，才能保障商用密码 SSL 证书的快速健康发展。零信技术打造的国密证书透明生态是一个保障商用密码 SSL 证书的可靠供给的生态，国密证书自动化管理生态则是一个实现商用密码 SSL 证书的快速部署应用的生态。这两个生态完全参考了已经签发了 84 亿张的国际 SSL 证书的成功路线，并根据商用密码算法的现状而定制打造，为我国普及商用密码 SSL 证书应用做好了充分的准备，普及商用密码 SSL 证书实现商用密码 https 加密也就是指日可待了，中国网站将开启商用密码算法保护年！这样，即使将来的某一天也同样遭遇俄罗斯一样的 SSL 证书被断供和被吊销的局面，也不会对我国网站造成任何影响，因为那个时候的我国网站根本就没有使用其制裁工具(RSA SSL 证书)！商用密码 HTTPS 加密普及元年来了！

请关注公司公众号，实时推送公司 CEO 精彩博文。