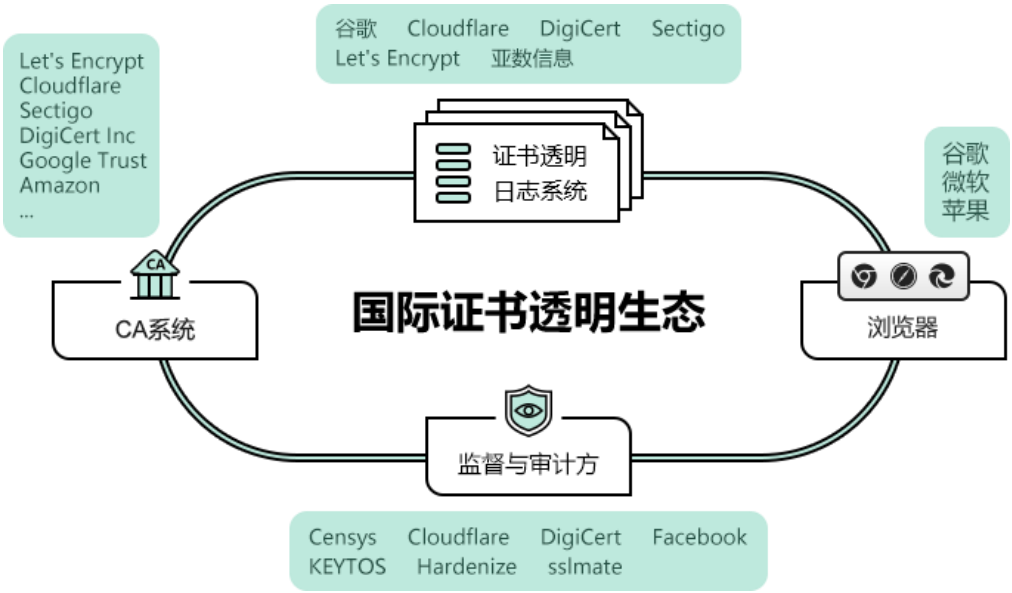
2023，国密 HTTPS 加密普及元年

笔者在“2018 网站空间可信峰会”(2008.12.17)上首次提出了“中国网络空间可信生态建设框架”的构想，并提出了国密 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，在国密应用生态成熟后就很自然地实现了“单轨制”(仅需部署国密 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，笔者有理由并且非常自信地认定今年是“国密 HTTPS 加密普及元年”。

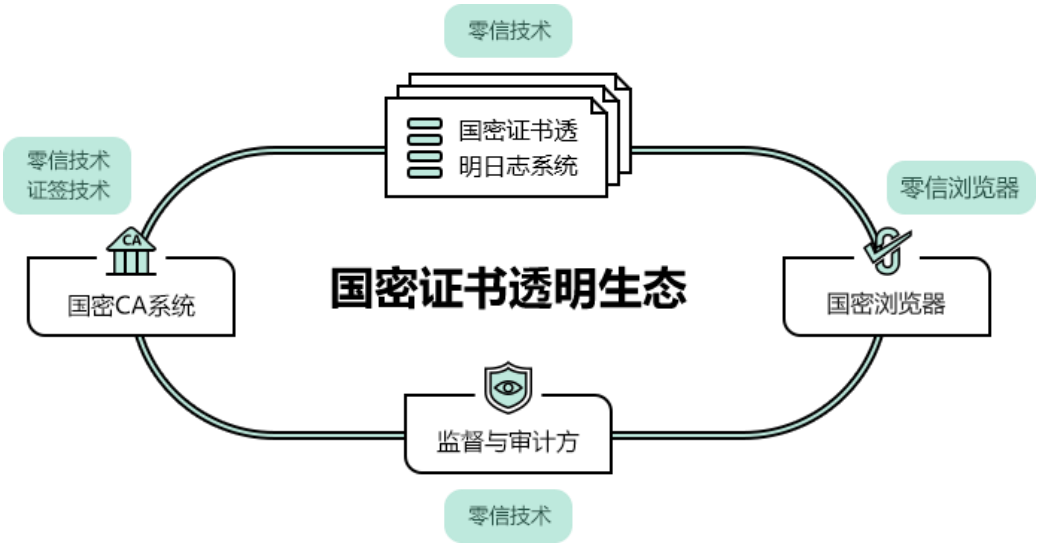
笔者的自信来自于公司鼎力打造的两大国密 SSL 证书生态：国密证书透明生态和国密证书自动化管理生态，前者是做好了国密 SSL 证书的可靠供给生态，后者则是做好了国密 SSL 证书的快速部署应用生态。这两个生态完全参考了已经签发了 84 亿张的国际 SSL 证书的成功路线，并根据国密算法的现状而定制打造，为我国普及国密 SSL 证书应用做好了充分的准备，普及国密 SSL 证书实现国密 https 加密也就是指日可待了，所以，笔者把 2023 年称之为“普及元年”。

“普及元年”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，并同时停止为俄罗斯政府网站和银行网站签发新的 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 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自主密码算法的国密 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！笔者早在 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，说我是“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，这就是国密 SSL 证书普及元年的触发点！深深地触动了密码业界的共识，并开足马力增强国密 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。

笔者先讲一讲国密 SSL 证书的可靠供给能力建设情况。国际 SSL 证书之所以能从 2013 年开始可靠地签发了 84 亿张 SSL 证书，可靠地保障了全球互联网的安全，是因为有证书透明生态，正是这个生态保证了国际 SSL 证书的可靠供给。有 CA 系统(SSL 证书提供商)可以签发支持证书透明的 SSL 证书、有浏览器能验证证书透明、有第三方监督和审计证书签发行为，这个生态闭环保证了国际 SSL 证书的可靠供给。



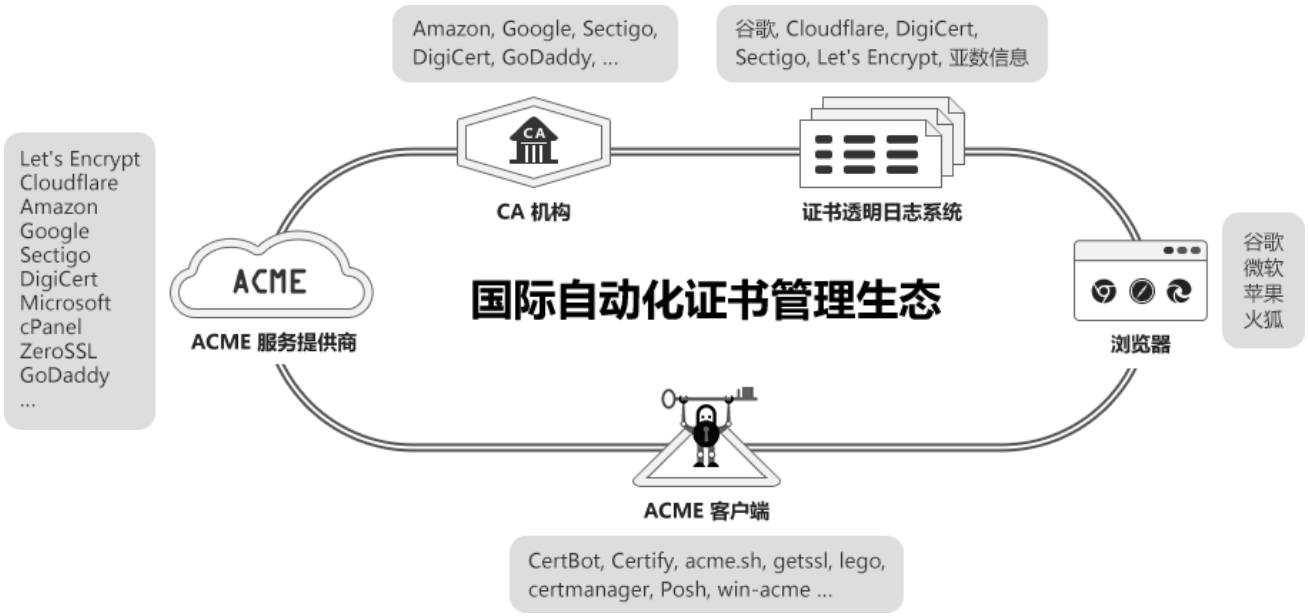
虽然从 2019 年开始有多家国内 CA 机构开始签发国密 SSL 证书，也有国产浏览器支持国密 SSL 证书，但是，这个生态中最重要的监管系统没有建立，没有支持国密算法的证书透明日志系统，国密 SSL 证书当然也就无从下手支持国密证书透明了，浏览器也就无从下手支持国密证书透明了，当然监管方也就无从下手获取证书签发数据而行驶监管职能了。笔者多年前就发现了这个关键问题，2021 年 6 月份重新创业后的第一件事就是要建立参考国际证书透明生态体系的国密证书透明生态体系，这个体系经过一年多的打造，终于于 2022 年 11 月 8 日在乌镇 2022 世界互联网大会上首发并启用了全球第一个国密证书透明日志系统，这个生态体系发布后得到了密码业界的认同和认可。



不仅零信技术和证签技术签发的国密 SSL 证书支持国密证书透明，已经有多家 CA 机构开始着手改造现有国密 CA 系统支持国密证书透明。不仅零信浏览器支持国密证书透明，已经有

几家国密浏览器开始计划升级支持国密证书透明。最可喜的是国密密码主管部门也有计划建设国家级国密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国密证书透明日志系统。也有第三方市场调查机构有兴趣提供基于国密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让笔者坚信国密证书透明生态一定能很快形成，一定能很快具有国密 SSL 证书的可靠供给能力，为国密 HTTPS 加密普及元年提供了安全可靠的“货源”。

再讲讲国密 SSL 证书的部署应用生态建设情况。全球 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：普及国密 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。



但是，这条自动化的新路不是我们的路，因为国际 ACME 协议不支持国密 SSL 证书，所以，零信技术又鼎力打造了国密 SSL 证书的第二个生态—国密证书自动化管理生态(SM2 ACME)，这个生态专为国密 SSL 证书的快速普及应用打造。这个生态包含了国密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，零信网站安全云服务，新增加国密 ACME 客户端和国密 HTTPS 网关两个新产品。

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，自动化实现国密 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国密 https 加密。而对于不想部署或无法部署硬件网关的用户，则可以选用网站安全云服务，只需做域名解析就可以零改造实现国密 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，普及国密 SSL 证书实现国密 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，普及国密 SSL 证书应用就指日可待了。这就是为何笔者称 2023 年为“国密 HTTPS 加密普及元年”的信心所在，必须在扫除了国密 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。

国密 HTTPS 加密普及元年来了，中国网站将开启国密算法保护年！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，因为我国网站根本就没有使用其制裁工具(RSA SSL 证书)！国密 HTTPS 加密普及元年来了，您准备好了？

王高华

2023 年 1 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。