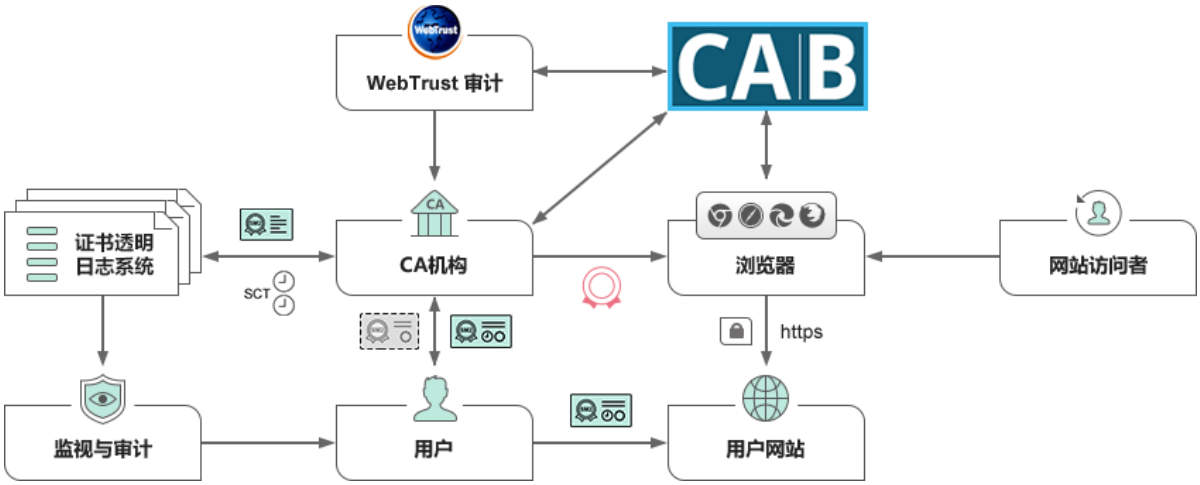
密码讲堂 | 第 9 讲 SSL 证书是如何生产出来的？

也许有读者看到这个题目就马上说，这还需要讲吗？也就是 OpenSSL 等工具一个命令行就能搞定的事情。这位同学回答正确也不正确，正确的是的确是一个命令行就能搞定，不正确的是这个搞定的 SSL 证书的使用价值为零。本文所要讲的 SSL 证书是指公共信任的 SSL 证书，也就是必须有浏览器信任的 SSL 证书。自己一个命令行搞定的 SSL 证书为自签证书，浏览器是不信任的，会有安全警告，不仅仅是技术上自签证书会有各种各样的安全问题，比如密钥太短、使用不安全的哈希算法等等，更重要的是这里面有一个信任机制和第三方监督机制来保证这张 SSL 证书的技术参数没有问题、身份信息正确、完成了域名控制权验证、接受公众监督等。本讲将详细讲一讲现在的全球信任的国际 SSL 证书是如何交付使用的，再讲一讲国密 SSL 证书对标国际 SSL 证书还有哪些差距和如何迎头赶上。

SSL 证书这个密码产品实际上是实现 https 加密的中间产品，其价值体现在浏览器是否信任上，浏览器是否能正常显示加密锁标识。这是一个围绕 SSL 证书实现 https 加密的生态系统，包括了 CA 机构、浏览器、CA/浏览器论坛、WebTrust 审计机构、证书透明日志系统、日志监视和审计方、网站主(SSL 证书用户)和网站、网站访问者等多个生态参与者。

俗话说“没有规矩不成方圆”，这个话出自于战国时期《孟子·离娄上》“离娄之明，公输子之巧，不以规矩，不能成方圆。”这是来自已经有两千三百多年的古人的中国智慧。对于 SSL 证书来讲，当然是必须按规矩来签发，这个规矩是由 CA/浏览器论坛(CA/Browser Forum)制定的两个标准—SSL 证书基线标准和 EV SSL 证书签发规范。CA/浏览器论坛是由全球知名的 CA 机构和主要浏览器厂商联合成立的一个没有注册的标准工作组，负责制定 CA 相关的国际标准规范，CA 必须按照这些规范来签发 SSL 证书，如果 CA 不按照这些规矩来签发 SSL 证书怎么办？还有一个机构-WebTrust 负责审计 CA 机构是否按规矩来签发证书，WebTrust 审计是由加拿大特许专业会计师协会(CPA Canada)主导联合美国注册会计师协会(AICPA)根据 CA/浏览器论坛制定的 CA 标准制定的一个审计标准，并认定一些知名的会计师事务所有资格从事 CA 审计业务。CA 机构每年都必须聘请这些事务所对 CA 机构进行技术和管理的审计，审计合格后由会计事务所出具一份审计报告给 CA，CA 可以在其官网展示 WebTrust 审计标识。为何 CA 机构甘心情愿地付钱请会计事务所来审计呢？当然是浏览器要求的，CA 机构的根证书要想浏览器信任，前提是必须提供 WebTrust 审计报告，这是前提条件，有了这个报告浏览器才会受理 CA 机构的根证书信任预置申请。



也就是说，CA 机构如果要想签发 SSL 证书，必须向浏览器申请根证书信任预置，必须先通过 WebTrust 审计，浏览器才受理预置申请，浏览器受理后还需要接受公众的公开网上讨论和各种技术检查，只有通过至少 1 年的漫长的各种审查，浏览器才会预置 CA 根证书信任，并通过发布新的浏览器版本来更新新的 CA 根证书。由于主流的浏览器厂家有四家，各家都有自己的一套根证书预置信任申请流程，CA 必须分别向这 4 家浏览器申请根预置信任，各家处理时间也都是不一致的，处理标准也都是不一致的，所以，CA 根证书要想所有浏览器都信任，至少需要 5 年左右，甚至更长的时间。只有这 4 大浏览器都信任了 CA 的根证书，CA 机构才有资格签发公共信任的 SSL 证书，但为了确保老的设备能信任这个新预置的根证书，估计还得等上 3-5 年才能真正签发通用性比较好的 SSL 证书。可以看出，CA 机构要想能签发全球信任的 SSL 证书是真的要“过五关”(1 个审计关，4 个浏览器关)，熬上 5-10 年才能修得正果。

OK，现在 CA 机构可以签发所有浏览器信任的 SSL 证书了，用户就可以向 CA 机构申请 SSL 证书，CA 在收到用户提交的证书请求文件(CSR)和身份证明材料并完成身份鉴证后，就可以为用户签发 SSL 证书，但这时候还有最后一道工序是必须把预签证书提交谷歌浏览器指定的证书透明日志系统中，180 天以内的证书必须提交两个证书透明日志服务器，180 天以上证书必须提交三个日志服务器。只有提交了透明备案并拿到备案证明(SCT 签名数据)并把 SCT 数据写入到 SSL 证书的 SCT 列表字段，才能把 SSL 证书正式交付给用户。这时候才算完成了一张 SSL 证书的生产交付，但是这事还没有完，如果证书透明监视方和审计方发现这张 SSL 证书有问题—属于错误签发，则 CA 机构必须马上吊销这张 SSL 证书，重新为用户签发一张新的 SSL 证书。

用户拿到 SSL 证书后部署到网站上使用，网站访问者就可以使用浏览器实现 https 加密访问了，浏览器地址栏会显示加密锁标识，到了这一步才能算是 SSL 证书完成交付使用。当

然，CA 机构的责任还没有完，每次浏览器使用 SSL 证书实现 https 加密时会访问 CA 机构提供的证书吊销列表服务，查验这张 SSL 证书是否被吊销，也就是说 CA 机构必须在证书有效期内为用户提供吊销列表查询服务(CRL)和证书签发者证书(AIA)下载服务，并不是把证书交付给用户就完成任务了。同时，在证书有效期内用户可能由于各种原因需要申请证书吊销和证书重新签发，这也是 CA 必须为用户提供的服务。

上面完整地讲解了国际算法 SSL 证书是如何打造出来，应该能看出这是一个非常复杂的门槛很高的技术活，限于篇幅，笔者把 CA 机构在收到证书申请后如何给用户签发证书的过程一笔带过，因为绝大多数读者无需了解这个过程。但理解一张 SSL 证书如何生产出来的全局对如何安全可靠地生产国密 SSL 证书是非常有帮助的，毕竟我国需要全面普及应用国密 SSL 证书来保障我国互联网安全。对标国际 SSL 证书的签发过程，我们需要找差距和补短板，尽快具有国密 SSL 证书的可靠生产能力。

作为一个曾经完整走完国际 SSL 证书生产过程的亲历者、一个从 2018 年底就开始鼎力打造国密 SSL 证书生产能力的从业者，笔者认为我国在国密 SSL 证书生产能力上还需要努力的方向主要有如下四点：

(1) 必须尽快制定和发布国密 SSL 证书急需的 5 个标准：商密 SSL 证书基线标准、CA 系统网络安全规范、CA 审计标准、证书透明规范和自动化证书管理规范，前 4 个标准是为了保证 CA 机构能签发合格的商密 SSL 证书，后 1 个标准是为了保障商密 SSL 证书的快速部署应用能力。5 个标准缺一不可。

(2) 在这些标准还没有出台之前，业界实际上已经行动起来了，有了多个国产浏览器支持国密算法和国密 SSL 证书，有了多家 CA 机构能签发国密 SSL 证书，虽然由于缺乏统一标准而出现了各种不同的国密 SSL 证书，但已经达到了可用的水平。

(3) 证书透明是除了浏览器根证书信任机制的又一个保障 SSL 证书自身安全的有力保障技术，这一块还需要浏览器和 CA 机构共同努力尽快实现所有国密 SSL 证书和所有国密浏览器都支持商密证书透明。

(4) 有了标准，就需要有审计机构能审计 CA 机构是否按照标准来签发 SSL 证书，这一点也需要在制定审计标准阶段做好顶层设计。

总之，SSL 证书的生产与应用是一个生态系统，是一个密码算法的生态系统，只有生态系统中的每一员都支持这个算法并且只支持这个算法，才是真正建立了技术壁垒，才能真正成为一种密码利器，用于保障互联网安全而造福人类，当然也可能被恶意利用成为一种制裁

工具，成为了一个“卡脖子”的工具。我们必须从一个密码应用生态的高度来认识 SSL 证书这个全球最成功的密码产品，只有这样才能真正赢得国密 SSL 证书市场。

下一讲内容预告 | 第 10 讲 什么是 ACME？什么是国密 ACME？

第 9 讲讲了 SSL 证书是如何生产出来的，本讲将讲解如何把生产出来的产品能快速普及应用。ACME 协议是一个划时代的协议，一个仅用 3 年时间能把全球 SSL 证书普及率从 40%提升到 80%的利器，值得好好讲一讲。

王高华

2023 年 4 月 23 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。