SSL 证书是网络空间安全的“卡脖子”产品

摘要

“卡脖子”技术很多，如大家都知道的芯片、操作系统等，“卡脖子”技术很多，如大家都知道的芯片、操作系统等，但是也许很多读者可能不知道 SSL 证书也是一个“卡脖子”的产品。本文将把 SSL 证书这个“卡脖子”的产品讲透彻，只有了解了 SSL 证书的技术原理和运作机制，才能真正理解为何 SSL 证书也是“卡脖子”产品，才会想办法尽快解决这个“卡脖子”难题！笔者提出的解决方案是参考国际 SSL 证书应用生态打造商密 SSL 证书应用生态，使得我国互联网安全根本不再依赖于目前“卡脖子”的 RSA 算法 SSL 证书实现 https 加密，全面采用商密 SSL 证书来保障我国互联网安全，只有这样才能真正解决“卡脖子”难题。

一、 引言

早期的互联网仅用于信息发布，所以互联网核心传输协议 HTTP 是一个明文传输协议。但是，随着互联网用户越来越多，人们就开始把互联网用于电子商务、网上银行等，这些应用不能是明文传输，必须加密机密的交易信息和账户口令等信息，所以当时的浏览器厂商美国网景公司(Netscape)于 1994 年就发明了 SSL 协议，并由全球第一个商业 CA 机构--VeriSign 开始签发 SSL 证书，这是密码技术在互联网的第一个非常成功的加密应用-HTTPS 加密，一个很巧妙地利用非对称算法来交换对称加密密钥的解决方案，巧妙地实现了从浏览器到 Web 服务器之间的交互信息的自动化加解密和服务器身份认证。

当然，这不是一个简单的单个密码产品应用，而是一个生态系统的支持和应用，做一个产品容易，做一个生态难，本文将重点讲这个生态。这个生态是如此的成功，以至于现在全球互联网的每一个应用都离不开这个密码产品(SSL 证书)，以至于这个密码产品成为了美国用于制裁他国的一个重要武器。

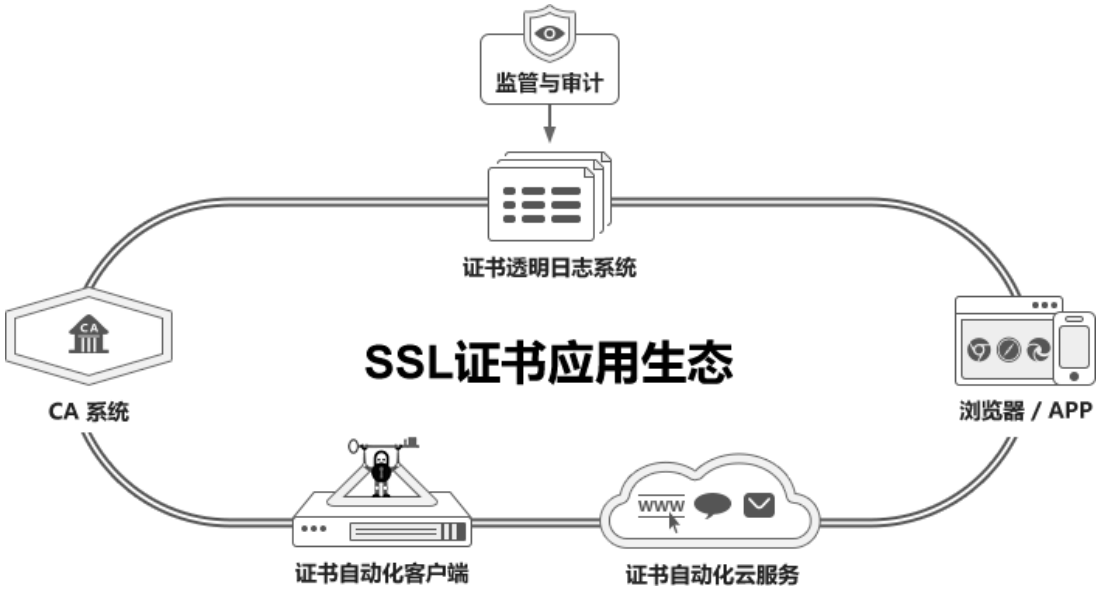
截止到 2023 年 4 月 15 日，全球已经记录在案的 SSL 证书总数为 **91.70 亿**多张，这是从 2013 年开始记录在谷歌证书透明日志系统的真实数据，其中未过期的有效 SSL 证书总数为 **5.29 亿**张，由此数据可以看出，SSL 证书是全球使用最广泛的最成功的密码产品，一个美国竭尽全力去维护其遥遥领先地位的密码产品！但是，我国互联网安全仍然 100%依赖这个 RSA 密码算法的密码产品来实现 https 加密，怎么办？

二、 SSL 证书应用生态是如何打造出来的？

习近平在 2021 年的两院院士大会和中国科协第十次全国代表大会上的讲话中说：基础研究更要应用牵引、突破瓶颈，从经济社会发展和国家安全面临的实际问题中凝练科学问题，弄通“卡脖子”技术的基础理论和技术原理。

SSL 证书是最重要的密码应用，所以我们要弄懂这个“卡脖子”产品的技术原理和应用生态，这样才能从国家网络空间安全面临的实际问题出发去理解和思考解决方案。我们必须弄清楚 SSL 证书是如何生产出来的，SSL 证书的应用生态是如何打造的，为何形成了生态就变成了无敌的“核弹”，从而启发我们思考我国应该如何打造基于商用密码的 SSL 证书应用生态，如何打造出我们自己的基于商用密码的无敌的保障我国网络空间安全的大国重器。

SSL 证书涉及到多个方面的产品和厂商，首先是 CA 系统能签发 SSL 证书，浏览器能验证 SSL 证书并用 SSL 证书实现 https 加密，当然这张 SSL 证书不仅必须是浏览器信任的根 CA 机构签发，而且必须是已经在浏览器信任的证书透明日志系统透明备案公示的，以便第三方监管机构和审计机构能实时了解和监督 SSL 证书的签发行为，保障 SSL 证书的自身安全可信。这里还有一个最重要的一项就是制定 SSL 证书的签发标准和审计标准，确保 CA 机构按照统一标准签发合格的 SSL 证书，这些标准主要包括 SSL 证书基线标准、CA 审计标准和证书透明标准(RFC6962)，从而有力保障 SSL 证书的可靠生产供给能力，为 SSL 证书在全球范围的广泛应用奠定了应用基础，也就是说首先必须保障这个被广泛应用的密码产品的可靠产能。



有了安全可靠的产能保障，就可以大规模的应用这个密码产品了。而要想一个产品能大规

模的应用只有自动化一条路，而要实现整个生态的所有系统的自动化应用，当然首先得有标准，大家按照统一的标准来实现自动化部署，这个标准就是 RFC8555(自动化证书管理环境,ACME)。有了标准，CA 系统就需要改造提供自动化证书管理 API，用于证书自动化管理客户端软件能对接 API 实现 SSL 证书的自动化申请、验证、部署和续期，用于各种需要 SSL 证书的云服务能对接 API 实现云服务所需的 SSL 证书的自动化申请、验证、部署和续期，用于各种需要 SSL 证书的物联网(车联网和工业互联网)设备能对接 API 实现物联网设备加密通信所需的 SSL 证书的自动化申请、验证、部署和续期，只有这样才能让每一个网站、每一个云服务和每一个设备都能自动化实现 https 加密，才能真正大规模的普及应用 SSL 证书这个密码产品来保障互联网、物联网和工业互联网的所有应用的通信安全和数据安全。也就是说，只有自动化才能为快速部署应用 SSL 证书提供了可靠的技术手段，才能具备 SSL 证书的快速部署应用能力。

目前全球范围已经有 5.29 亿张 SSL 证书在提供数据传输加密服务，保障全球互联网服务和交易的安全，这就是密码的威力，这就是密码产品的成功应用案例。总结一下其成功经验主要有三点：

(1) **密码算法是核心**：先有密码算法(RSA 密码体系)，就有了 PKI/CA 体系，就有了 SSL 证书，就有了 https 加密。

(2) **制定标准是关键**：首先必须制定标准，大家都按照这些标准参与到这个生态建设中来，只有这样才能建立其生态系统。

(3) **闭环生态是保障**：标准有了，大家都按照标准来生产和使用密码产品，这中间必须有监管和审计，有自动化监管和人工监管，这就形成了一个闭环，以确保各方都是按照标准来建设和维护这个生态的。

三、 SSL 证书用在哪？哪些地方是“卡脖子”的卡点？

这是一个非常重要的问题，必须单独列出一个段落来讲清楚这个问题。只有知道 SSL 证书这个密码产品用在哪，才能理解为何它是一个“卡脖子”产品，因为它用在了各种重要的位置，被卡住就有可能没命了！

SSL 证书的发明就是为了实现从浏览器到 Web 服务器之间建立一个数据加密通道，而目前各种互联网应用全部都是从客户端(浏览器或 APP)到服务端(云端)的应用，这个加密通道非常重要，没有这个加密通道就没有今天的这么繁荣的互联网应用，大家每天上网用的任何应用都是用 SSL 证书这个密码产品实现数据加密传输，这是密码在互联网的最重要的一个加密应用。这就是为何所有浏览器都会对明文传输的 http 网站显示为“不安全”，这不是浏览器在吓唬

用户，是真的不安全。没有使用 SSL 证书启用 https 加密就等于把用户的机密信息和网站的机密数据都通过明文在互联网传输，非常容易被非法截获和非法篡改，使得其他任何网络安全防护措施都等于零，因为安全防护的目的是为了保护数据。

从浏览器/APP 到服务端要实现正常的 https 加密，有多个环节会成为“卡脖子”的卡点。第一个卡点是 SSL 证书随时可以被吊销，CA 机构只需点一下鼠标即可。俄乌冲突发生后俄罗斯政府网站和银行网站遭遇的就是正在使用的 SSL 证书被非法吊销，使得用户正在访问的政府网站和网银系统瞬间无法访问。证书吊销机制本是为了保护用户的 SSL 证书私钥可能被泄露后 SSL 证书不会被滥用的安全机制，但是这是一个双刃剑，也可以用于“卡脖子”。

SSL 证书的第二个卡点是断供，俄乌冲突发生后俄罗斯政府网站和银行网站不仅遭遇正在使用的 SSL 证书被非法吊销，而且遭遇不再给这些网站签发新的 SSL 证书，也就是断供，不提供 SSL 证书给你，让你的网站系统裸奔！其实，这个断供一直存在，国际 CA 一直不被允许向古巴、朝鲜、伊朗、叙利亚等多个国家域名的网站签发 SSL 证书。

SSL 证书的第三个卡点是浏览器，签发一张 SSL 证书很容易，用 OpenSSL 等工具也就是一个命令行就能搞定的事情，但是为何 SSL 证书成为了“卡脖子”的产品呢？那是因为 SSL 证书还有一个信任机制，如果浏览器和操作系统不信任这张 SSL 证书的签发根证书，则这张 SSL 证书一文不值。所以，其价值体现在整个应用生态信任这张 SSL 证书，不仅是浏览器和操作系统信任，而且还有证书透明日志系统也必须信任，这是一个重要的卡点，浏览器不信任你签发的 SSL 证书，这张证书就是废纸一张。

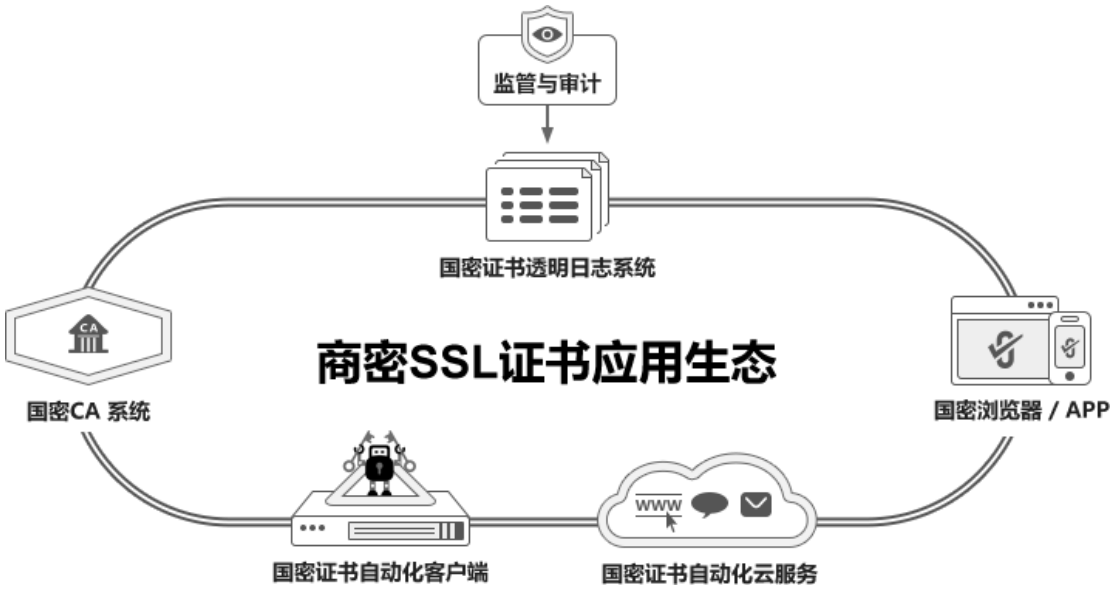
SSL 证书的第四个卡点是密码算法和证书标准，这是一个核心卡点，你签发的 SSL 证书用人家的密码算法，当然是否信任你签发的 SSL 证书人家说了算。即使今天我信任了你的 RSA 算法根证书，但是明天我可以不信任你的根证书，因为算法这个命根子掌握在我手中！即使你有自己的算法，用自己的算法签发了 SSL 证书，但是我可以说签发的这张 SSL 证书是非法的，不符合“国际标准”，我就可以制裁你，不再信任你的 RSA 算法根证书！

SSL 证书的第五个卡点是生态，这也是一个非常要命又很难短时间解决的卡点。即使你有自己的算法，也可以用你自己的算法签发 SSL 证书，但是整个生态产品都不支持你的算法，让你的 SSL 证书根本就无法使用，也没有用户敢用。要想你的算法的 SSL 证书能用，必须有一个依据标准建立的生态，必须有一个非常易用的快速部署应用方案，并尽快占领足够的市场份额，用的地方多了，生态就起来了。

四、 我国应该如何解决这个“卡脖子”问题？

既然我们已经了解了 SSL 证书的生态是如何打造的，其“卡脖子”的卡点在哪里，并且认识到了这个“卡脖子”的确是很要命的，那么我们就应该打造出自己的 SSL 证书应用生态—商密 SSL 证书应用生态，彻底解决“卡脖子”问题。

同 RSA 密码体系的 SSL 证书一样，当然也是要打造一个采用商用密码 SM2 SSL 证书的应用生态，一个采用商密算法的由证书透明日志系统运营方、监管和审计方、CA 机构、浏览器厂商、证书自动化客户端厂商和证书自动化云服务提供商等多方共同组成的生态系统，各自共同努力就能实现商用密码 SSL 证书的快速部署应用而形成应用生态，从而彻底解决 SSL 证书的“卡脖子”难题。



而如何打造这个商密 SSL 证书应用生态，具体有如下三个方面的工作要做：

(1) **商用密码算法是核心**

这个工作已经完成，我国已经有了先进的商用密码算法 SM2/SM3/SM4 等，不仅有了相关的算法标准，而且也已经成为了国际标准算法，只是这些算法还没有成为 SSL 证书的国际标准，这个还需要业界继续努力。不过，这一点不影响我们使用商密算法打造商密 SSL 证书应用生态。

(2) **制定商密标准是关键**

我国已经制定了两个 SSL 证书相关的标准，一个是国密标准《GM/T 0024-2014 SSL VPN 技术规范》，另一个是国家标准《GB/T 38636-2020 信息安全技术传输层密码协议(TLCP)》，还有一个 RFC8998 商业标准。

我国还缺的标准有：SSL 证书基线标准、CA 审计标准、证书透明标准和自动化证

书管理标准，必须快速完成这些重要标准的制定工作，只有这些标准出来了才能让大家能依据这些标准参与到这个生态建设中来，共同打造安全可靠的商密 SSL 证书供给能力，共同打造商密 SSL 证书的快速部署应用能力，才能建立起商密 SSL 证书的应用生态。

这个生态建设是一个比较漫长的过程，以证书透明为例，从谷歌 2013 年提出 RFC6962 标准到 2018 年真正实现所有 SSL 证书的全透明备案，整整花了 5 年时间，所以我们必须尽快先拿出标准，给后面的生态建设赢得更多的宝贵时间。

(3) 闭环商密生态是保障

随着急需的商用密码标准的快速出台，相关产业界就可以按照这些标准来生产和使用商密 SSL 证书这个重要的密码产品了，这中间必须有监管和审计。商密证书透明日志系统的建立就是一个自动化监管手段，能高效地保证商密 SSL 证书的自身安全，能在 SSL 证书还没有给用户之前第一时间监测到是否有恶意签发和错误签发商密 SSL 证书的行为发生。

当然，人工监管也是必须的，可以通过分析商密证书透明日志系统的实时签发数据，实现对商密 SSL 证书签发行为的实时监管。自动化技术手段监管、第三方利用证书透明日志数据的监督审计，这就形成了一个闭环，以确保各方都按照标准来建设和维护这个生态。

五、 结束语

HTTPS 加密是网络空间安全的核心密码应用，而加密用的 SSL 证书的可靠供给能力和快速部署应用能力则是打造 SSL 证书应用生态的关键。而要打造这两个能力的关键是尽快建立相关的标准，这一点必须高度重视。有了标准，有了《密码法》和《密用密码管理条例》的保障，加上密码业界和网络安全业界的共同努力，我们坚信商密 SSL 证书的应用生态一定能够快速地建设起来，就一定能彻底解决 SSL 证书的 5 个“卡脖子”难题，就一定能充分使用密码来保障我国网络空间安全，保障我国国家安全。

王高华

2023 年 4 月 15 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。