以商密标准推动商密应用，以商密应用完善商密标准

今天，笔者非常高兴收到正式文件通知：零信技术牵头制定的两个商密标准-《证书透明规范》和《自动化证书管理规范》已经列入国家密码行业标准化技术委员会下达的 2023 年度密码行业标准制修订任务(商用密码领域)，这标志着我国商密 SSL 证书的商用密码产品标准化水平又上了一个新台阶，将为保障商密 SSL 证书的可靠供给和普及应用提供标准支撑，将加速商密 SSL 证书的普及应用部署，加速采用商用密码来保障我国网络空间安全。

笔者作为牵头单位的负责人特撰文对密标委所有立项评审老师和有关领导为我国密码标准事业的辛勤付出表示最诚挚的感谢，特别对基础组老师们说声“您们辛苦了，感谢支持！”。并特别在此感谢标准组组长刘平老师和副组长汪宗斌老师的大力支持，没有您们的战略眼光和智慧，这两个标准就不可能立项成功，我国就没有相应的标准来保障商密 SSL 证书的自身安全可信，没有标准来实现商密 SSL 证书的自动化部署和快速应用。同时，笔者借此也一并感谢 17 家标准制定参与单位的大力支持，只有生态各方都支持这两个标准，才能真正让标准落地成为有用的标准。零信技术将不负众望让这两个标准早日正式发布，让这两个标准早日为保障我国网络空间安全发挥标准保障作用，并期待能为一带一路国家的网络空间安全提供中国创新方案。

本文从以下六个方面来论述：

(1) SSL 证书是网络空间安全的“卡脖子”产品

(2) 中国网络空间安全需要、应该、必须用商密 SSL 证书来保障

(3) 制定商密 SSL 证书密码行业标准是最关键的一步

(4) 制定商密 SSL 证书密码行业标准需要各利益相关方共同参与

(5) 制定标准和建设符合标准的应用生态必须同步进行

(6) 以商密标准推动商密应用，以商密应用完善商密标准

一、 SSL 证书是网络空间安全的“卡脖子”产品

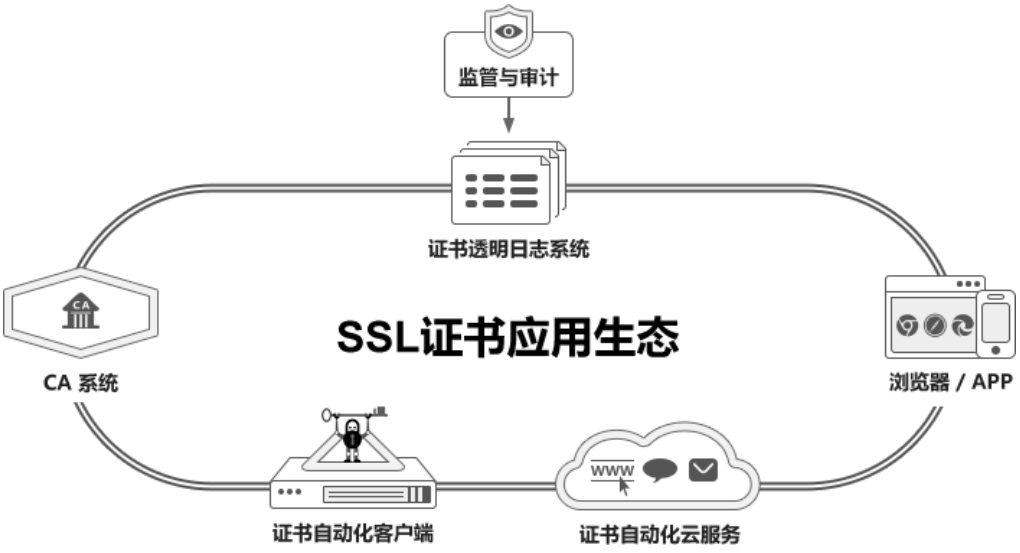
互联网的商业应用，得益于 Netscape 发明了 SSL 证书，因为互联网的最初设计是在内部使用的，所有通讯协议都是明文传输协议，包括最早的电子邮件是明文传输，后来的 Web 应

用是明文传输，DNS 信息也是明文传输，这些不安全的明文传输都需要用 SSL 证书来实现电子邮件 TLS 传输加密、Web 服务 HTTPS 加密和 DNS over HTTPS 加密，互联网也是在有了 SSL 证书实现信息传输加密后才有了商业应用，才有了今天的繁花似锦。

SSL 证书已经成为了所有互联网应用的核心加密产品，这是最成功的和用途最广的密码产品，任何一个网络应用都离不开这个密码产品，包括我们时刻也离不开的微信、支付宝、美团、网银服务和政务服务等等。为什么离不开 SSL 证书这个密码产品？因为保障各种互联网应用的安全，所有数据交换传输都必须加密，数据从云端流向到用户端需要通道加密。

SSL 证书已经不是一个简单的单个密码产品，而是一个全生态系统的支持和应用，做一个产品容易，做一个生态难。弃用一个产品容易，弃用一个生态很难！截止到 2023 年 12 月 12 日，全球已经记录在证书透明日志系统的 SSL 证书总数为 **114 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 **6.57 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，所以这个产品才成为了网络空间安全的“卡脖子”产品，成为了美国用于制裁俄罗斯的“武器”。

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 系统及网络安全标准、CA 审计标准、证书透明标准和自动化证书管理标准，从而有力保障 SSL 证书的可靠生产供给能力和快速应用部署能力，使得 SSL 证书能在全球范围内得到最广泛的应用。



二、 中国网络空间安全需要、应该、必须用商密 SSL 证书来保障

我国的互联网应用已经发展到了一个相当高的水平，网络应用普及率也很高，可以毫不夸张地讲，人民群众的生活和工作已经是一刻也离不开互联网了。而 SSL 证书则是用于保障所有互联网应用的关键密码产品，是一个“卡脖子”产品，这就决定了我国网络空间安全不能完全依赖于国外 RSA 算法的密码产品，不能依赖于 RSA 算法 SSL 证书，因为已经有了前车之鉴，我们必须未雨绸缪，我国互联网需要采用商密算法的 SSL 证书，必须采用商密 SSL 证书来实现 Web 应用的 HTTPS 加密、实现 DNS 加密和邮件 TLS 传输加密。

当然，同 RSA 算法 SSL 证书普及应用一样，普及应用商密 SSL 证书也需要一个 SSL 证书应用生态，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，大家共同努力打造这个生态，就能实现商用密码 SSL 证书可靠供给和快速部署应用，从而彻底解决 SSL 证书的“卡脖子”难题。

三、 制定商密 SSL 证书密码行业标准是最关键的一步

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，这一点并不影响我国使用商密算法打造商密 SSL 证书应用生态。

我国已经制定了两个 SSL 证书相关的标准，一个是商密标准《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)》，我

国还缺的标准有：SSL 证书基线标准、CA 系统及网络安全标准、CA 审计标准、证书透明标准和自动化证书管理标准，前面 3 个标准已经在去年获得立项，正在紧锣密鼓的基于草案的不断完善中。而后两个由零信技术牵头的标准今天也已经获得立项，这就标志着我国对标国际标准的 SSL 证书相关的 5 个标准已经全部立项，全部进入制定阶段，期待这些标准能早日正式发布。

四、 制定商密 SSL 证书密码行业标准需要各利益相关方共同参与

SSL 证书急需的 5 个标准立项已经吸引了高校如北航网安学院、多家 CA 机构、云服务提供商如华为云、阿里云和腾讯云、安全厂商如 360、标准服务机构和金融认证机构等多个相关领域的单位参与，这非常有利于标准的快速落地应用。

由零信技术牵头的《证书透明规范》和《自动化证书管理规范》不仅仅是参考相应的国际标准制定，不仅仅是修改了密码算法，而是真正基于这两个标准草案成功研发了相应的产品，验证了这些国际标准改造成商密标准的可行性。其中《证书透明规范》涉及浏览器厂商、CA 机构、证书透明日志系统运营方、证书监督和审计方，而《自动化证书管理规范》则涉及到云服务提供商、云密码服务提供商、Web 服务器和操作系统提供商、安全网关厂商等，只有相关的大多数领先的厂商都共同参与进来，才能制定出真正符合各方利益的能真正落地实施的好标准。

零信技术牵头的两个标准虽然已经有了 17 家相关单位参与，但我们欢迎更多的相关厂家继续加入参与标准的制定和完善标准中来，共同努力打造一个适合我国商用密码应用环境的高质量商用密码标准。

五、 制定标准和建设符合标准的应用生态必须同步进行

零信技术在提出制定这两个标准之前就已经完成了符合标准的产品研发，有些产品已经成功稳定运行了将近两年，成功打造了基于这两个标准的应用生态和生态必配产品，包括：支持商密证书透明的零信国密证书透明日志系统、支持商密证书透明的浏览器-零信浏览器、能签发支持商密证书透明的商密 SSL 证书的 CA 系统-零信云 SSL 系统、支持自动化证书管理规范实现自动化申请和部署商密 SSL 证书和国际 SSL 证书的 ACME 客户端软件-零信国密 ACME 客户端 SM2cerBot、为 ACME 客户端提供证书申请和签发服务的国密 ACME 服务系统、对接国密 ACME 服务系统实现自动化 HTTPS 加密的零信国密 HTTPS 加密自动化网关和零信国密

HTTPS 加密自动化云服务，所有这些产品和服务验证了两个标准的可行性和先进性，并且已经开始为用户提供商密 HTTPS 加密自动化服务。

但是，这个应用生态的发展壮大当然不是一家企业能建设起来的，需要业界共同参与，包括所有商密浏览器都应该支持商密证书透明来保证商密 HTTPS 加密的安全，有更多的厂商或权威机构提供商密证书透明日志服务，各家 CA 签发的商密 SSL 证书都应该支持商密证书透明，各个云服务提供商都能为用户提供支持自动化证书管理的商密 HTTPS 加密服务，各种需要应用商密 SSL 证书的硬件网关产品都应该支持商密证书自动化管理来自动实现 HTTPS 加密，只有相关产业厂商都依据这些商密标准参与到这个生态建设中来，才能真正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 证书的应用大生态。

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 RFC 6962 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，所以我们必须尽快完成这些商密标准的制定，并同时在标准草案基础上研发基于这个标准草案的产品，让标准制定与生态建设同步进行。

六、 以商密标准推动商密应用，以商密应用完善商密标准

标准建设当然不是为了有标准而制定标准，当然是我们发现了商密 SSL 证书体系还缺少这些标准而制定这些标准。《证书透明规范》是为了保障 CA 机构签发的商密 SSL 证书的自身安全，能及时发现 CA 机构由于操作失误而错误签发商密 SSL 证书，或者由于 CA 系统被攻击而恶意签发用于网络攻击的商密 SSL 证书，这不是增加了 CA 的负担，而是提升了 CA 机构的

商密 SSL 证书签发能力和核心竞争力，提升了我国商密 SSL 证书的自身安全水平，目前每一张国际 SSL 证书都支持证书透明已经证明证书透明的支持并不是负担而是加分项！而所有商密浏览器支持商密证书透明，当然也是为了提升商密 HTTPS 加密的安全水平，保护商密浏览器用户的上网安全。

《自动化证书管理规范》则是为了实现商密 SSL 证书的自动化申请和自动化部署，为业界提供一个证书签发标准接口，将大大推动商密 SSL 证书的普及应用，大大降低各种业务系统商密改造的门槛，可以让原 Web 服务器零改造实现商密 HTTPS 加密。《证书透明规范》和《自动化证书管理规范》这两个商密标准的制定，将推动商密 HTTPS 加密的普及应用，让各种商密 SSL 证书的加密应用有准可依。

反过来，各种商密 SSL 证书的广泛应用会带动这些商密标准的不断完善，这就是为何标准批准制定后给与两年时间的期限提交报批稿，大家可以在这段时间内把依据这些标准草案的产品和生态做起来，来检验这个标准的成熟度，并根据实际应用需要不断完善这个标准草案，这样制定的标准才是一个高质量的商密标准。所以，我们欢迎各个提供遵循《证书透明规范》和《自动化证书管理规范》两个标准草案的产品的厂商在积极参与制定这两个标准的同时大胆提出自己的产品在应用中需要完善标准的需求，不仅能提升自己产品的核心竞争力，而且能带动标准的完善和提升，这是一个双赢的结果。实际上，在标准立项过程中，我们已经收到了华为提交的在《自动化证书管理规范》草案基础上增加扩展标识类型和扩展挑战类型的补充内容，以满足在电信设备中自动化部署 SSL 证书的应用需求。

总之，商密标准的建设与商密应用的推进必须同步进行，相互促进，这也是零信技术为何为两个牵头的商密标准在官网设立专栏介绍这两个标准的原因，方便业界基于标准草案研发相关产品，并在产品研发过程中对标准草案提出完善建议。我们同时免费提供了一个供标准参与单位使用的电子邮件列表服务，供大家像制定国际标准一样充分利用电子邮件组来讨论标准草案和完善标准草案，以期高效和高标准地完成两个商密标准的制定工作。

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。要打造这两个能力的关键是建立和发布相关的标准，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“卡脖子”难题，就一定能普及应用商密 SSL 证书来保障我国网络空间安全，保障我国国家安全稳定。

有诗为证：

喜获立项双标准，多年努力终开花。

标准建设促应用，普及应用结硕果。

王高华

2023 年 12 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。