2024 “4•15”，为推动中国式现代化筑牢密码防线

今年国家密码管理局发布的“4·15”全民国家安全教育日密码安全宣传挂图的宣传语是：贯彻总体国家安全观，统筹高质量发展和高水平安全，增强密码安全意识，为推动中国式现代化筑牢密码防线。笔者特在活动日撰文解读今年的宣传语，希望能为密码同仁带来一些不一样的思考，为宣传“4·15”全民国家安全教育日做出一点点小小的努力。

一、何为中国式现代化？

中国式现代化是人口规模巨大的现代化，是全体人民共同富裕的现代化，是物质文明和精神文明相协调的现代化，是人与自然和谐共生的现代化，是走和平发展道路的现代化。

在推动中国式现代化总体任务中，战略保障是统筹推进“五位一体”总体布局的任务之一，主要内容有：目前，国际环境中的不确定因素增多，在推进社会主义现代化强国建设的过程中，要强化风险意识、底线思维，树立总体国家安全观，切实维护好国家主权、安全和发展利益。要统筹国内国际两个大局。

二、为何推动中国式现代化需要筑牢密码防线？

推动中国式现代化的总体任务之一就是安全保障，笔者重点解读与密码相关的三点：

1. 在国际环境不确定因素增多的形势下，强化风险意识和底线思维。

2022 年 2 月 24 日俄乌冲突发生后，西方 CA 吊销了已经签发给俄罗斯政府网站和银行网站的 SSL 证书，同时不再签发(断供)新证书，导致了几乎所有政府网站和银行网站无法正常 HTTPS 加密访问。SSL 证书这个密码产品变成了制裁工具，这给我国的网络安全敲了警钟。

我国必须强化密码应用的风险意识，必须有底线思维—如果这事发生在我国怎么办？因为我国的政府网站和银行网站也是像俄罗斯一样部署的是 RSA 密码算法 SSL 证书，并没有普及应用商用密码算法 SSL 证书。也就是说，我国还没有完成保障政府网站和银行网站安全的密码防线建设工作，仍然任重道远。

2. 树立总体国家安全观，包括网络安全观和数据安全观

网络安全是指通过采用必要的措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

数据安全是指通过采用必要的措施，确保数据处于有效保护和合法使用的状态，以及具备保障持续安全状态的能力。

这两个重要的安全观的核心安全是网络数据流通的传输安全，也就是 HTTPS 加密安全，用何种密码算法来实现 HTTPS 加密。传统的网络安全和数据安全观是“堡垒”观，保证数据在机房的安全。但是，在大数据时代，数据只有流通才有价值，而数据的流通传输过程的安全保护就需要 HTTPS 加密，这一点在我国并没有得到应有的高度重视，许多政务服务仍然是明文 HTTP 方式，并没有实现 HTTPS 加密，更没有实现商用密码算法 HTTPS 加密。商密 HTTPS 加密改造必须是密改和密评的第一重点工作。

3. 增强密码安全意识，统筹国内国际两个大局

“密码安全” 可以理解为“用密码来保障安全”，同时也可以理解为“加强密码自身安全”。“证书透明”就是一项加强 SSL 证书这个密码产品自身安全的技术，从 2013 年开始，所有全球信任的 RSA/ECC 算法 SSL 证书都支持证书透明来保障 SSL 证书自身安全可信，商密 SSL 证书也理应如此。

“统筹国内国际”可以在密码应用上解读为：既要推动商用密码的普及应用，同时也要考虑

到兼容国际密码体系，既要做到商密合规，也要做到全球信任。这就是需要统筹的两个大局，需要把这个大局观融入各种密码应用解决方案中。具体到SSL证书应用就是双SSL证书部署，自适应加密算法实现HTTPS加密。

三、密码企业可以为筑牢密码防线做些什么？

密码应用涉及到方方面面，已经渗透到每一个涉及到网络安全和数据安全的各种应用中，各种各样的密码应用都是在构筑密码防线。但是，要想筑牢密码防线，就得抓住防线的重点，才能称得上“筑牢”。这个防线的核心是数据流通的传输安全保障，就是HTTPS加密，这是所有网络安全和数据安全解决方案的核心安全，没有这个，其他解决方案都是空中楼阁，都无法形成牢固的防线。也正是由于这个太重要了，以至于SSL证书这个密码应用产品成为了制裁俄罗斯的工具，这是前车之鉴，我国必须未雨绸缪，提前防范未然。

《密码法》高瞻远瞩，2020年1月1日正式施行，比发生俄乌冲突导致密码产品(SSL证书)被吊销和被断供的密码安全事件还早两年，早就预见了这种密码应用安全事件的可能发生，所以才以国家大法形式要求我国关键信息基础设施必须采用商用密码进行保护。但是，如何保护？这个就需要解读《密码法》第二条，核心就是加密保护，这一点在国家安全观的网络安全观中有明确要求-保障网络数据的完整性、保密性、可用性，在数据安全观也有明确要求-确保数据处于有效保护的状态，这两个安全观都是要求“通过采用必要的措施”，本部分就讲清楚这个必要的措施是什么，这个必要的措施之一，也是核心措施，就是HTTPS加密，商密HTTPS加密。

要实现HTTPS加密，用户就需要向CA机构申请和购买SSL证书，手动部署SSL证书到Web服务器上、部署到CDN系统上、部署到WAF设备或云WAF系统上，才能实现HTTPS加密。而为了应对RSA算法的SSL证书可能被吊销和被断供，我国必须部署商密SSL证书，用商密算法实现HTTPS加密。同时，浏览器和APP也都必须支持商密算法才能使用SM2算法实现HTTPS加密，CDN网络、WAF设备或云WAF服务也必须支持SM2算法和SM2 SSL证书。这是一个全生态的商密算法支持，商密改造难就是难在整个生态都要改造。

零信技术深深理解这一难点，在深入研究了国际密码体系的发展历程和快速普及应用HTTPS加密的相关技术和发展经验后，历时三年研发，创新地提出了零改造自动化完成商密HTTPS加密改造的解决方案。这是一个端云一体的自动化实现商密HTTPS加密的解决方案，原Web服务器零改造，只需在前面部署零信国密HTTPS加密自动化网关，由网关自动对接零信云SSL服务系统，自动化为用户网站配置双算法SSL证书，实现自适应加密算法的HTTPS

加密，免费配套的零信浏览器优先采用商密算法实现 HTTPS 加密，兼容其他浏览器采用 RSA 算法实现 HTTPS 加密。

零新技术零改造解决方案的核心是自动化证书管理，目前全球 90%以上的国际算法 SSL 证书部署都实现了自动化管理，要想普及商密算法 SSL 证书应用，也只有自动化这一条道。只有自动化完成商密 HTTPS 加密改造，才能快速应用商密 SSL 证书来保障数据流通的传输安全，这是互联网安全的核心安全，其他安全措施都是以这个核心安全为基础之上的安全保障，只有实现了核心基础安全，再加上其他安全保障措施，才能算是实现了筑牢密码防线的战略目标。

零信技术商密 HTTPS 加密自动化解决方案实现了第二部分解读的三项任务：

1. 强化风险意识和底线思维

俄乌冲突让我们看到了金融制裁的后果，而更需要看到的是密码制裁的更严重的后果，因为密码制裁会严重影响老百姓的日常网络生活，我国老百姓已经一刻也离不开网络服务了。所以，我们在看到有前车之鉴后必须有风险意识和底线思维，必须及时果断采取行动，尽快实施商密 HTTPS 加密改造，并及时完成普及应用商用 HTTPS 加密，以规避将来可能出现的网络安全风险，真正实现筑牢密码防线的伟大目标。

2. 用商用密码来保障网络安全和数据安全

既然已经认识到 RSA 密码保障不了我国的网络安全和数据安全，那就要找出一条适合我国的 HTTPS 加密保障之路，这就是商密 HTTPS 加密自动化，而不是传统的申请 SSL 证书并改造 Web 服务器之路。目前唯一可行之道就是零改造快速完成普及应用商用密码来实现 HTTPS 加密，那就是零信技术提出的端云一体自动化实现商密 HTTPS 加密的创新解决方案，只有这个方案，才能快速普及应用商密 HTTPS 加密技术来保障我国网络安全和数据安全。

这是一个商密生态建设的大事，只有密码企业和网络安全企业都遵循《自动化证书管理规范》商密标准参与到这个商密证书自动化生态中来，才能实现筑牢密码防线的伟大目标。

3. 增强密码安全意识，商用密码优先，兼容国际密码

为了保障商密 SSL 证书的自身安全，商密 SSL 证书也必须支持证书透明，这是一个保障密码安全的重要技术措施，防止敌对势力利用商密 SSL 证书来实施网络攻击，加强密码安全，

保障国家网络安全。这也是商密生态建设的一部分，需要生态中的 CA 机构、浏览器厂商等都能遵循《证书透明规范》商密标准支持商密证书透明，只有这样才能真正保障 SSL 证书这个重要密码产品的自身安全可信。

同时，我国必须采取“商用密码优先、兼容国际密码”战略，无论何种密码技术都是为了保障网络安全和数据安全，我们必须有国内和国际大局观，平时可以同时采用国际密码和商用密码共同保障我国网络安全和数据安全，非常时期则能自动切换到商用密码，实现仅用商用密码也一样能保障我国网络安全和数据安全，也一样能不影响老百姓正常的网络生活，这才是真正的筑牢了密码防线。

密码人，让我们携手努力，增强密码安全意识，强化风险意识和底线思维，共同为早日实现“为推动中国式现代化筑牢密码防线”的伟大目标而奋斗！

王高华

2024 年 4 月 15 日于深圳
