重磅关基规定，重任重责重罚，轻改方案是首选

国家密码管理局于 2025 年 6 月 27 日发布了由国家密码管理局、国家网信办和公安部联合发布的《关键信息基础设施商用密码使用管理规定》(以下简称《规定》)，此《规定》自 2025 年 8 月 1 日起施行。这是关基运营者的重任和重责，如果不能按时保质保量完成，那一定是会受到重罚的。怎么办？本文支高招，四个重重一个轻改方案就能轻松搞定！

一、《规定》涉及到哪些单位？

根据《关键信息基础设施安全保护条例》第二条的定义，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

根据这个定义，所有政府官网、政务服务系统、公共服务系统、网银系统、支付系统(包括微信支付和支付宝)、主流电商系统等运营单位都是本《规定》涵盖范围，也可以理解为这是要求全国所有大型公共服务系统都必须使用商用密码来保护其系统数据安全，范围之广，责任之大，所以大家都解读为重磅规定。

二、《规定》的核心内容有哪些？

第一条就列出了 7 个法律法规作为制定本《规定》的法律依据，这里就不再重复了，但需要重复一下《规定》的核心内容，主要有三条：

(1) **第五条**明确运营者总体责任。落实关键信息基础设施商用密码使用“三同步一评估”原则，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

(2) **第九条**明确商用密码技术、产品、服务使用要求。规定关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

(3) **第十条**明确数据安全保护、个人信息保护要求。强调关键信息基础设施应当使用商用密码对其存储、使用、传输的核心数据、重要数据和个人信息进行保护。

解读《规定》之前还是请读者再先看看在此之前各个部委最近一年来还发布了哪些相关的文件规定：

(1) **2024 年 5 月 22 日**，网信办官网发布了由网信办、中央编办、工信部和公安部联合发布的《互联网政务应用安全管理规定》，2024 年 7 月 1 日起施行。此规定明确要求政府官网和政务服务网站系统都必须实现商用密码算法 HTTPS 加密安全连接，包括列入关键信息基础设施的网站系统。

(2) **2024 年 7 月 19 日**，国家密码管理局发布了《商用密码随机抽查事项清单（2024 年版）》，自发布之日起施行。这是要执法检查商用密码应用情况，采用抽查的方案巧妙地解决了执法人力不足的难题，不仅能体现被检查对象的公平性，而且能达到法律具备足够威慑力的效果。

(3) **2024 年 11 月 21 日**，人行、发改委、工信部、金管局、证监会、国家数据局、国家外汇局等七部门联合印发了《推动数字金融高质量发展行动方案》，系统推进金融机构数字化转型，强化数字金融风险防范，加强数据和网络安全防护，强化数据安全的商用密码保护。

(4) **2025 年 5 月 28 日**，国务院发布《政务数据共享条例》，2025 年 8 月 1 日起施行。要求政府部门应当采取技术措施(商用密码)和其他必要措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用。

(5) **2025 年 6 月 27 日**，国家密码管理局发布了本《规定》，也是 2025 年 8 月 1 日起施行。

这一连串的重磅规定文件的发布意味着什么呢？有一点是可以肯定的，那就是不断加码要求全面普及应用商用密码来保障我国关键信息基础设施安全。怎样才能快速实现普及应用？这就是本文要讲的重点。鉴于此《规定》涉及到了所有重要行业领域，本文重点解读政府和金融两个领域。同时，依据《密码法》对密码用途的定义—加密保护和安全认证，这涉及到的应用范围也很广，本文仅讨论加密保护一个用途，这一项的应用也有很多，本文仅讨论最核心、最重要、用途最广的应用—保障数据传输安全的 HTTPS 加密，这也是笔者的强项，拥有 21 年的从业经验。所以，本文重点解读如何使用商用密码保护第十条所指的“存储、使用、传输的核心数据、重要数据和个人信息”，保障关基数据的传输安全和使用安全，这个安全是其他所有商用密码保护的核心，也是我国在这方面最薄弱的密码应用环节，值得重点解读。

三、目前的商用密码 HTTPS 加密使用现状是什么样的？还存在哪些严重问题？

也许正是因为目前的使用现状很不乐观，所以，国家有关部门才连续出台重磅文件，包括本《规定》。那么，目前我国关键信息基础设施网站系统的商密 HTTPS 加密情况到底如下，看看如下统计数据便知。

(1) 国务院 84 个部门 79 个有独立官网，其中实现了 HTTPS 加密的有 62 个，占比 78%，有 17 个部门官网没有启用 HTTPS 加密，占比 22%。这些启用 HTTPS 加密的网站中只有 1 个公安部启用了商用密码 HTTPS 加密，占比仅 1.26%，也就是说，除了公安部官网外其他部委官网都是不符合《规定》的—未采用商用密码算法实现 HTTPS 加密。

(2) 31 个省市自治区政府官网中，只有 18 个省市自治区启用了 HTTPS 加密，占比 58%，比国务院各部委占比低。只有 4 个省(湖南、海南、江西、陕西)政府官网实现了商用密码 HTTPS 加密，占比仅 12.90%，比国务院各部委占比高。

(3) 20 大银行官网中，有 11 个银行启用了 HTTPS 加密，占比 55%，居然被各省和各部委数据还要低。而启用商用密码 HTTPS 加密的只有一个兴业银行，占比仅 5%，这也是不能接受的占比。我国最早在金融行业要求实施国密改造，但是在这个不差钱的行业居然这么低的比例，可见商用密码 HTTPS 加密改造是何等之难。

其他行业的数据就不再展示了，基本都是零商用密码 HTTPS 加密应用，这就是目前我国商用密码 HTTPS 加密保护的现状，一个作为密码人汗颜的现实，不是这些关基单位不作为，是密码人没有拿出好的解决方案给这些单位。笔者上周四收到某个县级市政务信息系统建设的招标文件，看了之后就直接拒绝了。因为这个项目的规划方案就有问题，所有招标文件采购的设备都是错的，我公司提供不了这些错误用途的密码设备。

《规定》第五条明确要求落实关键信息基础设施商用密码使用“三同步一评估”原则，同步规划、同步建设、同步运行商用密码保障系统。规划在先，只有规划对了，建设才是对的，后面的运行才能真正使用商用密码来保证关基系统安全。所以，笔者先重点讲一讲 HTTPS 加密的方案规划。

要想实现商密 HTTPS 加密，就得采购支持商密算法的网关、国密 SSL 证书和国密浏览器三样产品，这是目前所有密改项目规划方案，十年前就一直是这个方案，但是现在就不合适了，因为 SSL 证书有效期将缩短为 47 天，方案中的所有产品都已经不再能满足商用密码 HTTPS 加密的实际应用需求了。还是具体以上周四的招标项目来举例说明。

先看看这个招标文件对网关的要求，如下截图所示，首先是产品选型有问题，SSL VPN 网

关是用于远程接入内部网络的，用于实现互联网政府网站 HTTPS 加密就是错误的产品选型，正确的技术方案必须是采购 HTTPS 加密网关。更可笑的是要求支持 SM9 算法，HTTPS 加密仅涉及到 SM2/SM3/SM4 三个商用密码算法，为何需要支持毫不相干的 SM9 算法呢？这不符合密评对正确使用密码算法的要求，也不符合《规定》要求。

1.名称：IPsec/SSL VPN综合安全网关 2.功能参数：1、产品具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书； 2、支持256位SM2公钥密码算法，支持2048位和4096位RSA公钥密码算法，支持SM4和AES等对称密码算法，支持SM3、SHA256摘要算法； 3、支持创建SSL VPN服务并支持单双向SSL配置，同时支持国密和国际证书策略，并支持国密与国际SSL算法套件及协议； 4、具备SM9算法SSL连接建立功能，在50并发用户数时，SM9算法SSL平均吞吐量不低于800Mbps；

再看看这个招标文件对 SSL 证书的要求，如下截图所示，标配双算法 SSL 证书，各 11 张，要求能安装部署在服务器或网关上，这些要求看起来没有什么问题，除了数量有问题外，因为一个县级市不可能只有 11 个系统需要实现 HTTPS 加密。最重要的问题是技术方案有问题，这个项目现在才开始招标，估计实施就是明年，项目规划者是否知道 SSL 证书有效期明年 3 月 15 日就只有 200 天了，2027 年只有 100 天，2029 年只有 47 天，难道要求用户以后每个月都去向 CA 申请双 SSL 证书，每个月都去服务器和网关安装证书？这个规划是技术严重落后而不是稍微超前，正确的技术方案是要求双算法 SSL 证书必须支持自动化管理。

1.名称：国际算法SSL证书（第三方合规机构颁发） 2.功能参数：1、基于国际算法为网站提供身份鉴定并保证该网站拥有高强度加密安全； 4、可安装部署在服务器或网关，实现数据传输加密。	张	11
1.名称：国密算法SSL证书（第三方合规机构颁发） 2.功能参数：1、基于国密算法为网站提供身份鉴定并保证该网站拥有高强度加密安全；	张	11

再看看这个招标文件对国密浏览器的要求，如下截图所示，首先是采购的数量是 200 套，一个县级市的政务系统难道只有 200 个工作人员使用。但这不是这个招标单位的问题，这是无奈之举，笔者还看到过只规划采购 1 套国密浏览器的标书。这是密码产业的问题，国密浏览器本应该是普及国密 HTTPS 加密的利器，全球 RSA 密码体系之所以迅速在全球范围普及应用，最大的功劳是四大浏览器对 RSA 密码体系的全面支持和完全免费使用。而我国也想普及商用密码体系的全面应用，但是本应为普及商用密码算法做贡献的国密浏览器却由于是必须品而成为了收费产品，严重阻碍了商用密码的普及应用，这是产业界短视的悲哀，也是普及商用密码的最大障碍。笔者在此强烈呼吁国家密码管理部门尽快取消国密浏览器的商用密码产品认证要求，只有这样才能让商用密码在完全免费的国密浏览器普及应用下得到快速发展，这是必须学习和借鉴的 RSA 密码体系的普及应用之道。

1.名称：国密浏览器 2.功能参数：1、产品具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书； 2、支持基于 SM2 算法的数字证书、数字证书撤销列表（CRL）； 3、同时支持 SSL 单向及双向链接； 4、支持基于 RSA 算法的数字证书、数字证书撤销列表（CRL）； 5、双算法支持，同时支持国密算法和国际通用算法；	套	200

请读者朋友们千万不要以为这是笔者是在发牢骚，笔者这是在展示我国商用密码 HTTPS 加密的应用现状，是在找出存在的问题。各位已经完成了密改和密评的单位可以对比一下自己的密改方案，是否也是上面那一套？但是，现在已经进入 SSL 证书自动化管理时代，全球 11 亿张 SSL 证书中超过 80%都已经实现了自动化管理，我国要想普及应用国密 SSL 证书来实现 HTTPS 加密保障互联网政务应用的安全，也得向国际密码界学习，与时俱进，积极拥抱 SSL 证书自动化管理，而不是还在用十年前的老三样方案，要按《规定》要求不断改进商用密码应用技术措施。

四、落实《规定》要求，真正正确使用商用密码 HTTPS 加密来保障关基系统安全

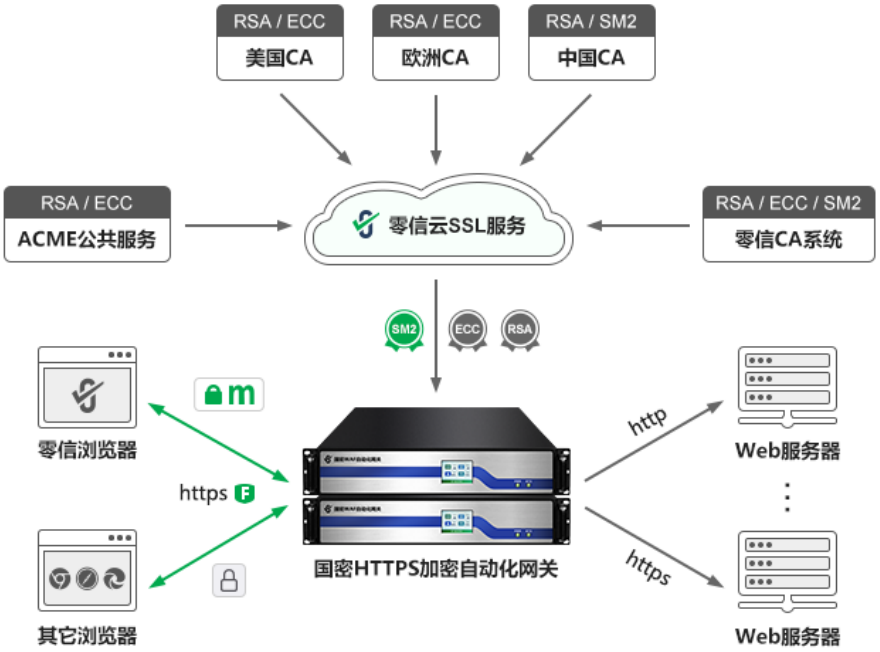
在讲明我国商用密码 HTTPS 加密应用的现状后，本部分就接着讲一讲如何解决问题，不能只是简单的转发《规定》，必须给关基运营者一个指导方案，以便轻松完成《规定》的重任重责，以免重罚，因为重罚不是目的。

要想普及应用商用密码实现 HTTPS 加密来保障我国互联网政务应用安全，就得向国际先进技术学习，实现 HTTPS 加密所需的网关、SSL 证书和浏览器都得支持 SSL 证书自动化管理，因为不可能要求关基运营者每个月都去人工申请和部署 SSL 证书，必须实现国密 SSL 证书和国际 SSL 证书的自动化申请和部署，必须为用户提供原 Web 服务器零改造零安装零停机的商密 HTTPS 加密自动化解决方案，并且是自适应密码算法，国密浏览器优先采用商用密码 SM2 算法实现 HTTPS 加密，兼容其他不支持商密算法的浏览器采用 RSA 算法实现 HTTPS 加密。

对于上述标书的网关采购，应该规划采购“国密 HTTPS 加密自动化网关”，而不是采购 SSL VPN 网关，除非的确是要求 VPN 远程接入用。标书应该要求网关支持双算法 SSL 证书的自动化部署，网关报价应该包含 5 年国密 SSL 证书和国际 SSL 证书的费用，SSL 证书无需单独采购。国密浏览器不应该列入需要采购的产品，因为市场上已经有了完全免费的、干净无广告的符合国密 HTTPS 加密应用要求的国密浏览器，无需再花钱采购，把宝贵的建设经费用在刀刃上。只有这样，才能真正轻松实现商密 HTTPS 加密来满足《规定》的要求，满足《互联网政务应用安全管理规定》、《抽查》等文件要求。

零信技术双算法 SSL 证书自动化管理解决方案远不止实现以上最低要求，零信技术的解决方案是一个“端云一体”的解决方案，一个重要的“端”也是网关，但是零信国密 HTTPS 加密自动化网关不是 SSL VPN 网关，是通过商密产品认证的专用于 HTTPS 加密自动化和 WAF 防护的网关。零信网关默认自动化配置国际 SSL 证书和国密 SSL 证书，双算法 SSL 证书都是最安全的“一站一密钥一证书”自动化申请和自动化部署，证书密钥不出网关硬件，保证了密钥安全。用户无需另外采购和申请双算法 SSL 证书，也无需在 Web 服务器或网关上人工手动安装 SSL

证书，包 5 年最多 255 个网站的双算法 SSL 证书费用，并且是硬件也包用 5 年，包用期间故障网关设备直接换新。



还有一个“端”就是国密浏览器—零信浏览器，这是一个完全免费的、干净无广告的、支持国密证书透明的国密浏览器，支持 Windows、麒麟和统信国产操作系统，即将发布的版本是基于谷歌浏览器内核 137 版本，这是目前市场上所有国密浏览器中的最新的内核版本。所有用户都可以在零信官网直接下载，不限数量的免费使用，根本不用在规划方案中列入采购国密浏览器这一项。

零信技术双算法 SSL 证书自动化管理解决方案的“云”就是零信云 SSL 服务系统，为零信国密 HTTPS 加密自动化网关提供双算法 SSL 证书的自动化签发服务，已经对接了多家国际 CA 和国密 CA，同时还对接了国际 ACME 公共服务系统和零信 CA 系统，实现了自动化切换双算法 SSL 证书供应链，确保了无论那家 CA 无法供货时都可以可靠地为用户网站自动化签发国际 SSL 证书和国密 SSL 证书，切实保障了网站 HTTPS 加密的不中断可靠运行。

也就是说，HTTPS 加密密改方案必须按照《规定》要求与时俱进改进技术方案，而不是传统的老三样(SSL VPN 网关、国密 SSL 证书和国密浏览器)，只需要采购一样—国密 HTTPS 加密自动化网关，有了这一样产品，就可以实现自动化配置国密 SSL 证书和国际 SSL 证书，自动化实现商密 HTTPS 加密和 WAF 防护。国密浏览器不用列入采购计划花钱购买，因为市场上已经有了完全免费的国密浏览器。这不仅能轻松满足《规定》的要求，而且能满足关基运营者轻松应对即将到来的 SSL 证书有效期缩短为 47 天的技术难题。

五、关基商密规定，不是负担，是保障业务系统持续可靠运行的催化剂

SSL 证书有效期即将缩短为 47 天，这给所有关基运营者带来了巨大的技术改造压力，而《规定》的出台正好让运营者可以名正言顺地做好合规规划，及时落实经费预算，一步到位实现双算法 SSL 证书的自动化管理，而不是采用 SSL 证书人工部署的老方案，只有这样才能真正实现用好用对密码产品来保障我国关键信息基础设施的安全，真正实现普及应用商用密码来保障业务系统的不间断的持续可靠运行。

王高华

2025 年 6 月 30 日于深圳