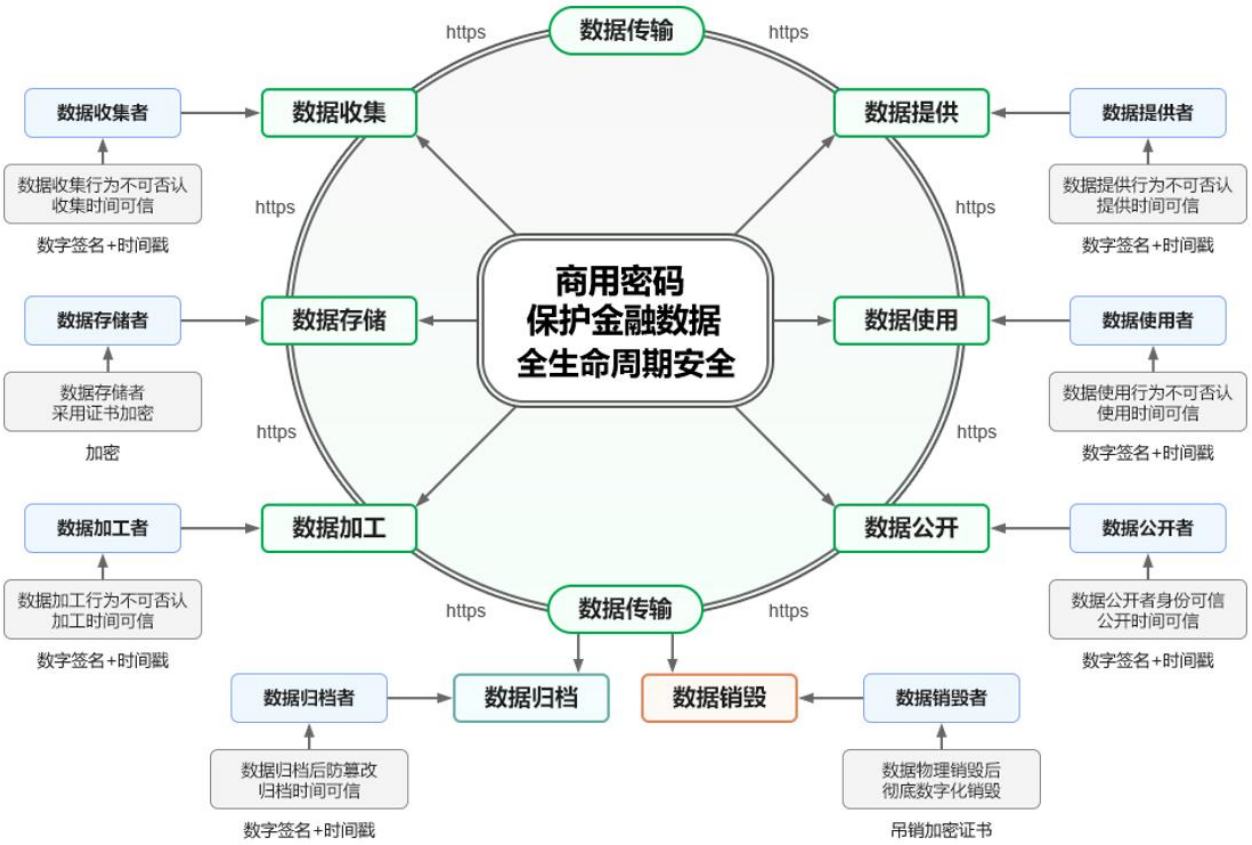
# 解读人行等七部委联合印发《行动方案》的商用密码保护要求

中国人民银行 、国家发展改革委、工业和信息化部、金融监管总局、中国证监会、国家数据局、国家外汇局等七部门于 2024 年 11 月 21 日联合印发了《推动数字金融高质量发展行动方案》(以下简称“行动方案”)，系统推进金融机构数字化转型，加强战略规划和组织管理，强化数字技术支撑能力，夯实数据治理与融合应用能力基础，建设数字金融服务生态，提升数字化经营管理能力。完善数字金融治理体系，强化数字金融风险防范，加强数据和网络安全防护，加强数字金融业务监管，提升金融监管数字化水平，健全金融消费者保护机制。

本文仅解读其中与商用密码相关的内容：加强数据和网络安全防护。指导金融机构严格落实数据保护法律法规和标准规范，完善数据安全管理体系，强化数据安全的商用密码保护，建立健全全流程数据安全管理机制。重点解读如何加强数据安全的商用密码保护、如何加强网络安全的商用密码保护，明确说明应该如何采用商用密码来保护数据安全和网站安全。

## 一、 如何采用商用密码保护金融数据安全？

要讲清楚这个问题，必须先讲清楚什么是数据安全，依据《数据安全法》第三条对“数据处理”的定义，数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等 7 个环节。所以，要保护金融数据安全，就必须保护数据在这 7 个处理环节中的全程安全。当然，首选技术是商用密码技术，必须采用商用密码实现数据的传输安全(HTTPS 加密)、实现数据的完整性保护(数字签名+时间戳)、实现数据的机密性保护(加密)，有效保障每一个数据处理过程中的数据处于有效保护和合法利用中，使得数据从生产到销毁的全生命周期都处于持续安全状态。其中，最重要、最核心和最基础的数据保护就是数据在全生命周期中的流通传输都必须是通过商密 HTTPS 加密通道传输。




这就是《数据安全法》所定义的“数据安全”要求，“通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。这就是《行动方案》所要求的“严格落实数据保护法律法规和标准规范”-《数据安全法》的具体落实，并且是一个完整的“全流程数据安全管理机制”的商用密码保护。

目前我国金融数据的商用密码数字签名、验签、时间戳和加密等应用都是非常到位的，因为这方面的厂商非常多。唯一不足的是银行官网、网银系统和内部管理系统的商密 HTTPS 加密保护，现在仍然有许多银行官网没有启用 HTTPS 加密，仍然是明文 HTTP 不安全方式，只是网银系统启用 RSA 算法 HTTPS 加密，这是非常不安全和严重不合规的。

这里有一个非常错误的认识需要再次在本文强调一下：银行所有系统包括官网都必须实现全站 HTTPS 加密，而不是仅仅网银系统才实现 HTTPS 加密。因为如果官网页面没有实现 HTTPS 加密，则用户在通过官网访问网银系统时，极有可能访问了假冒的网银系统，这是由于官网页面是明文传输，则其页面中的链接到网银系统的网址就非常容易被非法篡改为假冒网银网址，从而导致了用户从正确银行官网链接到了假冒的网银系统。为了防范这种攻击，必须实现全站 HTTPS 加密，从官网入口开始到链接到各种银行业务系统都必须全部采用 HTTPS 加密。当然，银行系统必须严格依据相关的法律法规采用商用密码实现 HTTPS 加密。

还有一点也是必须指出的，那就是网银 APP 安全问题。现在，多家银行的网银系统已经

从浏览器的网页版切换到手机网银 APP，这个切换的确方便了用户使用移动网银服务，但是银行必须加强网银 APP 的 HTTPS 加密合规编程，严格验证 Web 服务器上部署的 SSL 证书和采用安全协议和加密套件实现 HTTPS 加密，并优先采用商密算法实现 HTTPS 加密。关于这一点，请同时参考文章：解读《关于加强银行业保险业移动互联网应用程序管理的通知》。

## 二、 如何采用商用密码保护金融网络安全？

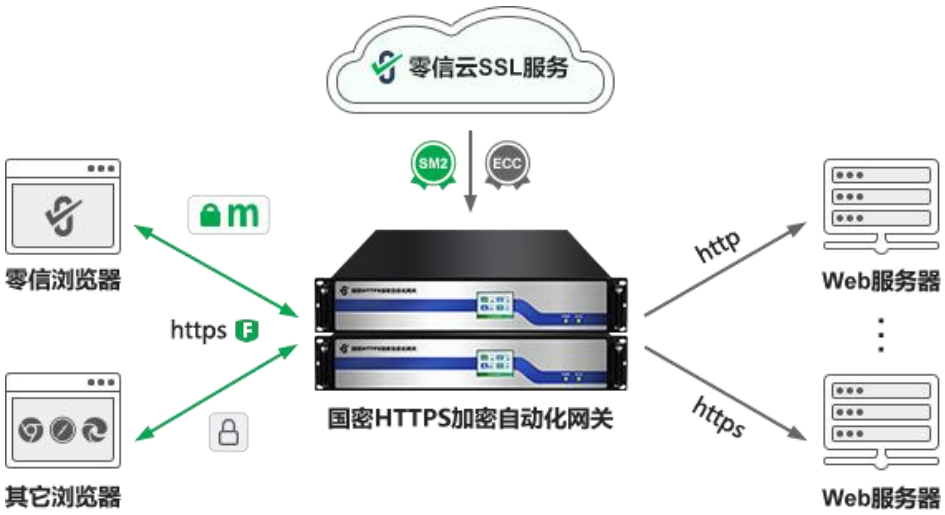
要讲清楚这个问题，必须先讲清楚什么是网络安全，依据《网络安全法》第二十一条明确指出：网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，必须采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，采取数据分类、重要数据备份和加密等措施，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

这里包含了两点要求：一是必须采用防止网络攻击和网络侵入的安全防护技术措施，二是重要数据必须加密，这就是要求银行网站和网银系统必须实现 HTTPS 加密和 WAF 防护。而依据《密码法》要求，就是必须实现商密 HTTPS 加密和 WAF 防护，从而有效地防止金融网络数据泄露、被窃取和被篡改。这就是《行动方案》所要求的采用商用密码加强网络安全防护。

目前 WAF 防护在银行官网和网银系统并没有得到普及应用，即使已经购置了 WAF 防护设备的银行，由于市场上的大部分 WAF 设备和云 WAF 服务都不支持商密算法实现 HTTPS 加密，这就导致了金融机构无法落实《行动方案》所要求采用商用密码加强网络安全防护。金融网络安全除了必须采用传统的网络安全防护设备外，金融机构还必须高度重视 Web 应用防火墙(WAF)的部署应用，并且必须采用支持商密 HTTPS 加密的 WAF 防护。

## 三、 零信技术提供哪些商用密码产品来保护金融数据安全和金融网络安全？

零信技术定位为基于商用密码技术的零信任安全提供商，能为金融数据安全和金融网络安全提供全系列商密产品和相关解决方案，包括商密 HTTPS 加密自动化解决方案、商密邮件加密自动化解决方案、商密文档数字签名和加密自动化解决方案、商密应用软件数字签名自动化解决方案，这些都是基于零信云密码基础设施提供的端云一体的密码应用自动化解决方案。其中核心产品是零信国密 HTTPS 加密自动化网关和零信浏览器，为保障金融网站和网银系统的数据安全和网络安全提供商密 HTTPS 加密自动化管理解决方案。




这是一个原 Web 服务器零改造实现商密 HTTPS 加密的解决方案，用户无需向 CA 机构申请商密 SSL 证书，无需在网银 Web 服务器上安装 SSL 证书，无需安装商密算法支持模块来改造 Web 服务器支持商用密码，也无需在 Web 服务器上安装 ACME 客户端软件，只需在原 Web 服务器前面部署零信国密 HTTPS 加密自动化网关即可，最多为 255 个网站自动化实现商密 HTTPS 加密和 WAF 防护，满足银行官网和网银系统的 HTTPS 加密数据传输安全，同时满足网站安全 WAF 防护要求。

这是我国首个同时自动化实现商密 HTTPS 加密和 WAF 防护的解决方案，一个网关搞定金融数据传输安全和网络安全的三大难题：

**(1) 搞定商密 HTTPS 加密改造难题**

原银行官网和网银系统零改造，自动化配置商密合规的商密 SSL 证书实现商密 HTTPS 加密，同时自动化配置全球信任的国际 SSL 证书实现兼容国际算法 HTTPS 加密，以自适应加密算法方式实现 HTTPS 加密保护。金融机构无需购买国密 SSL 证书和国际 SSL 证书，节省证书费用和人工部署证书的人力成本。

**(2) 搞定 WAF 防护难题**

金融机构不再需要单独采购 WAF 设备或云 WAF 服务，零信网关内置高性能 WAF 系统，并且是支持商密 HTTTPS 加密自动化的 WAF 防护，实现一个网关同时搞定商密 HTTPS 加密和商密算法支持的 WAF 防护自动化。而目前市场上的 WAF 设备都是需要用户自己去申请 SSL 证书并人工导入证书的方式，并且仅支持国际算法，不支持商密 HTTPS 加密，这在要求网银系统必须采用商密 HTTPS 加密保护的应用场景下，这样的 WAF 设备是无法

满足合规要求的。而零信国密 HTTPS 加密自动化网关已经集成了高性能 WAF 系统，实现商密 HTTPS 加密方式的 WAF 防护。

**(3) 搞定 IPv6 改造难题**

人行有关规定要求所有银行官网和网银系统都必须支持 IPv6，并且是在 IPv6 网络环境中支持商密 HTTPS 加密，零信国密 HTTPS 加密自动化网关让银行无需改造网银 Web 服务器支持 IPv6，原 Web 服务器仍然可以只支持 IPv4，由零信网关实现 IPv6 到 IPv4 的协议转换，银行只需在零信网关配置 IPv4 和 IPv6 双地址即可，并且这是同时支持商密 HTTPS 加密和 WAF 防护的 IPv6 访问。

**(4) 免费配套商密浏览器**

要实现商密 HTTPS 加密来保障银行数据安全和网络安全，支持商密算法的浏览器也是必不可少的软件。零信浏览器是一个基于先进的 Chromium 内核的、完全免费的、干净无广告的、支持商密算法和商密证书透明的全功能高性能通用浏览器，优先采用商密算法实现 HTTPS 加密，有力保障银行数据传输安全和保障网银系统网络安全。

## 四、 只有强化商用密码保护，才能真正保障金融数据安全和网络安全

人行等 7 部委联合发布的《行动方案》是为了全力做好数字金融大文章，加快建设金融强国，巩固和拓展我国数字经济优势。其中第五点的“完善数字金融治理体系”要求必须加强数据和网络安全保护，采用商用密码保护不仅是相关法律法规的要求，而且是保障银行数据传输安全和银行网络安全的唯一可靠技术手段，其核心应用就是商密 HTTPS 加密和 WAF 防护。

要实现商密 HTTPS 加密的关键不是传统的让银行去向 CA 申请和部署 SSL 证书，去改造现有的网银系统 Web 服务器支持商密算法，这不是一个优选方案。这个不合理的技术方案让银行承受了不可承受的商密改造压力和负担，从而导致经过了多年的商密改造的今天还没有普及应用商用密码来保障我国网银系统安全，还需要 7 部委继续不断的发文要求采用商用密码保护。

唯一可行的、能实现普及商用密码保护的技术方案是零信技术历时三年打造的商密 HTTPS 加密自动化管理解决方案，这个自动化解决方案是一个端云一体实现的原网银 Web 服务器零改造方案，让金融机构能轻松实现普及应用商用密码来保障金融数据传输安全和网络安全，从而轻松实现《行动方案》所提出的合规要求，从而真正普惠提升银行网络安全防护体系

建设水平。

王高华

2024 年 12 月 2 日于深圳

---

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 194 篇(共 55 万 6 千多字)和英文 81 篇(10 万 4 千多单词)。