密码是信创的根基

今天，新修订的《商用密码管理条例》正式施行，这是 2020 年 1 月 1 日正式施行的《密码法》的落地应用的细化管理条例，这就使得信创产业的密码应用有法可依，有条例可执行，是一个值得重笔写一篇文章的大事，特撰文写写密码与信创的关系，希望能帮助信创产业界加深对密码的深度认识，并在产品规划和产品提升上多多增加密码的应用，以提升信创产品的内生安全能力和提升产品核心竞争力，让我国的信创产品能更上一层楼，为保障我国数字安全做出更大的贡献。

我国自 2016 年提出安全可控体系并升级为信息技术应用创新(简称“信创”)以来，国家大力推进从 IT 底层的基础硬件到基础软件再到应用软件三个层级的国产化替代，基本实现了包括基础软硬件到上层应用软件的全产业链的安全可控，涵盖了 IT 基础设施、基础软件、应用软件、信息安全四个领域。

信创产业作为新基建的重要组成和发展依托，对国民经济发展的基础支撑、创新驱动和融合牵引作用日益凸显，也将成为产业创新、拉动经济发展、释放动能的重要抓手之一。未来围绕“新基建”的国产软硬件全面规模化应用进程将逐步加快，信创产业面临加速发展的黄金机遇期。同时，在政府顶层设计中，各级政府发文推进互联网与政务服务深度融合，通过云架构，实现政府服务效能的提升，建成省市县多级连动、协同的“互联网+政务”体系。

那么，商用密码与信创产业是什么关系？还是让我们先看看目前正在广泛应用的信息技术与密码是什么关系。先从操作系统开始，目前使用最多的操作系统是 Windows，Windows 是一个深度集成了密码的系统，一个从底层就集成了 PKI 技术的系统，有自己的根证书信任列表，有操作系统核心代码包括启动软件的数字签名验证，有各种驱动软件的内核签名认证，有各种软件代码的运行的数字签名验证，没有可信数字签名的代码是不允许运行的。操作系统配套的三大应用软件：浏览器(微软 Edge 浏览器、谷歌浏览器)、邮件客户端(Outlook)和 PDF 阅读器(Adobe Reader)都深度集成了密码技术，依赖 Windows 根证书信任列表或自己的信任列表来实现 Web 传输的 https 加密、电子邮件数字签名和加密、PDF 文件数字签名和加密，这些安全机制都是采用 RSA 密码体系的数字签名和加密来保障操作系统的安全，保障各个应用软件实现的数据传输安全和数据共享使用安全，密码同操作系统和应用软件是作为不可分割的一个整体来为用户提供各种网络服务和数据服务。

再说一下网络基础设施的密码应用，互联网及万物互联的最广泛的连接协议是 HTTP 协议，这个协议奠定了今天繁荣的所有互联网应用，而保障这个传输协议安全的是采用密码技术的 SSL 证书，使得 HTTP 明文不安全传输变成了密文安全传输，目前全球已经签发了 97 亿多张 SSL 证书来保障全球互联网安全。这是一个基于 RSA 密码体系的保障体系，不仅所有 Web 服务器支持这个 RSA 密码体系产品实现 HTTPS 加密，而且所有客户端(浏览器和移动 APP)也都支持，CDN 内容分发网络都支持，WAF 防护也都支持，各种数据加密也都支持，各种身份认证也都支持，各种网上应用包括电子合同签署等都支持。可以说，每一个网络基础设施和网络应用都离不开密码的应用—数字签名、加密和时间戳，包括所有电子政务应用、电子商务应用、移动支付、人工智能、工业互联网等等，这些都是离不开密码的深度应用。但是，请注意：这些深度融合的密码应用是融合 RSA 密码体系，而不是国产密码体系。

大家从上面的简单介绍应该能看出：目前的信息技术应用的方方面面都离不开密码。也就是说，我国的信息技术应用创新产品当然也离不开密码，实际上有许多信创产品也正在应用密码来保障其安全，只不过仍然是沿用 RSA 密码体系，而不是采用我国的商用密码体系，密码要落地应用，落实《密码法》和《商用密码管理条例》的全面应用就应该从信创产品开始，所有信创产品都应该深度融合商用密码和采用商用密码来保障其安全。

还是先从国产操作系统开始，国产操作系统应该像 Windows 一样也是一个深度集成了密码的系统，一个从底层就集成了 PKI 技术的系统，有自己的商密根证书信任列表，有操作系统核心代码包括启动软件的商用密码数字签名验证，有各种驱动软件的内核商用密码数字签名认证，有各种软件代码的运行的商用密码数字签名验证，没有可信的商用密码数字签名的代码是不允

许运行的。国产操作系统配套的三大应用软件：浏览器、邮件客户端和文档阅读器也都必须深度集成了商用密码技术，依赖国产操作系统的根证书信任列表或自己的信任列表来实现 Web 传输的商密 https 加密、电子邮件商密数字签名和加密、PDF/OFD 文件商密数字签名和加密，这些安全机制必须采用商用密码体系的数字签名和加密来保障国产操作系统的安全，保障各个应用软件实现的数据传输安全和数据共享使用安全，商用密码同国产操作系统和国产应用软件必须作为不可分割的一个整体来为用户提供各种网络服务和数据服务。

再说一下网络基础设施的商用密码应用，互联网及万物互联的最广泛的连接协议是 HTTP 协议，这个协议奠定了今天繁荣的所有互联网应用，我国必须采用商密 SSL 证书来保障这个传输协议的安全，使得 HTTP 明文不安全传输变成了密文安全传输。不仅所有国产 Web 服务器都必须支持商密 SSL 证书实现 HTTPS 加密，而且所有客户端(浏览器和移动 APP)也都必须支持商密算法和商密 SSL 证书，CDN 内容分发网络也必须支持商密 SSL 证书，WAF 防护也必须支持商密 SSL 证书，各种数据加密也必须支持商用密码，各种身份认证也必须支持商用密码，各种网上应用包括电子合同签署等都必须支持商用密码。可以说，每一个网络基础设施和网络应用都必须采用密用密码实现数字签名、加密和时间戳，包括所有电子政务应用、电子商务应用、移动支付、人工智能、工业互联网等等，这些都必须采用商用密码，深度应用商用密码来保障其安全，而不是继续沿用已经深度融合的 RSA 密码体系。

笔者非常高兴看到广东省人民政府官网于 6 月 26 发布了《广东省人民政府关于进一步深化数字政府改革建设的实施意见》，意见明确指出：将数字技术广泛应用于政府管理服务，统筹推进技术融合、业务融合、数据融合，优化业务流程，创新协同方式，推动“一网统管”“一网通办”“一网协同”相互促进、融合发展，不断提升政府数字化履职效能。并且加快推进数字政府密码应用，研究制定密码应用支撑能力清单，探索建立政务信息化项目密码应用服务目录。这是非常值得推广的做法，有了应用清单和服务目录，大家就可以按照这个清单来自查和检查是否做到了政务信息系统的商密合规。

笔者参考 RSA 密码保障体系在此列出政务信息项目商用密码支撑能力清单，供有关部门研究和制定清单和目录时参考，具体如下：

(1) 政务信息化建设采购的国产操作系统必须深度融合商用密码应用，不仅必须要求各种政务应用软件必须有商密数字签名和时间戳，以保障政务办公系统安全；而且必须配套提供支持商密 SSL 证书实现 https 加密的国产浏览器，以保障政务 Web 应用安全；必须配套提供支持商密加密的电子邮件客户端软件，以保障政务邮件安全；必须配套提供支持商密数字签名和加密的 PDF/OFD 阅读器，以保障政务文档安全。

(2) 所有政务网站无论是公网网站还是内网 Web 应用系统，都必须采用商密 SSL 证书实现

https 加密，以保障 Web 流量安全，保障政务数据在传输过程的安全，保护机密政务数据安全。对于公众服务网站，由于需要兼容所有浏览器，必须同时部署国密 SSL 证书和国际 SSL 证书，实现自适应算法的 https 加密。

(3) 所有政务网站采用的 CDN 和 WAF 服务(包括 WAF 设备)都必须支持商密 SSL 证书，优先采用商密算法实现 https 加密内容分发和安全防护。

(4) 所有政务系统数据包括政务文档都必须采用商密数字证书来实现加密、数字签名和时间戳。

(5) 所有政务系统访问身份认证都必须采用电子政务许可 CA 签发的 USB Key 商密证书实现身份认证和数字签名。

(6) 其他各种内部政务管理应用，都必须采用商用密码来实现信息加密和安全认证。

王高华

2023 年 7 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。