信创产业的下一个风口是商用密码的原生集成和应用

现在是年会黄金期，各个单位都在开年会，总结过去的 2023 年和展望 2024 年工作。笔者特撰文为密码产业做一个简单的 2023 年总结和着重探讨 2024 年的展望，供各相关产业的管理高层决策参考。大家看到标题就应该大致了解了笔者的观点，“风口”实际上都被喊烂了，但是笔者认为这个名词通俗易懂并且深入人心，所以还是决定用这个名词。本文分四个部分来讲述。

一、 信创产业的现状分析

“信创”（全称“信息技术应用创新”）是基于国产芯片和操作系统的电脑、服务器、网络设备、存储设备、数据库、中间件等信息系统基础设施的信息技术创新。信创产业非常庞大，涉及基础硬件（芯片、服务器等）、基础软件（操作系统、数据库、中间件等）、应用软件（OA、ERP、办公软件等）、信息安全（边界安全产品、终端安全产品等）4 个部分，其中芯片、操作系统和数据库是更为重要的产业链环节。

我国国产基础软硬件从“无”到“有”，并正在向“好用”演变。信创产业作为“新基建”的重要内容，已经成为拉动经济发展的重要抓手之一。回顾 2023 年，信创产业已历经政策炒作期，现已进入建设落地期和上升期。展望 2024 年，有关机构预测信创产业规模将达到 2258 亿元。

从全球信息产业发展历程来看，目前我国的信创产业就相当于 80-90 年代个人电脑和互联网兴起的时代，当然由于起点不一样，比哪个时代的性能是无法同日而语了。但笔者为何要这样对比呢？因为我们现在处于从无到有的阶段，就像当时刚刚出现电脑一样的阶段，下一个阶段就是要步入“好用”的阶段。而如何用好已有的信创产品和如何升级现有信创产品，则仍然需要借鉴全球信息产业发展历程来谋划这个发展战略，走对方向才是关键。

先看一个信创业界专家的忧虑，这个专家所在公司是一家头部操作系统厂商，他的大意是：虽然我们做了自己的操作系统，但是各种硬件板卡的驱动还是 RSA 密码体系的数字签名，还是受制于人而无法回避。这在我这个密码专家看来，就真的不是什么事了，绝对不是什么受制于人的事情！我国是硬件板卡生产大国，完全可以建立一套硬件板卡必须使用商用密码体系建立驱动程序数字签名机制，而为了让厂家的板卡能兼容 Windows 操作系统可以设计为像目前的 HTTPS 加密解决方案一样的双算法双证书数字签名方式。这就是一个技术标准和制定政策的简单问题，根本不是什么卡脖子的难题！

笔者举这个例子的用意是想说明：信创产业必须同密码产业紧密结合和深度融合，信创产业的专家和工程技术人员必须了解密码技术及其应用。至于如何融合，将在下面两部分详细描述。

二、 密码产业的现状分析

随着《密码法》实施进入第 4 个年头以及《商用密码管理条例》新版发布施行，我国的密码产业也进入了快车道，有关机构预测 2024 年的密码产业规模将过千亿元。但是，这个规模仍然停留在传统的老四样上：密码芯片、密码板卡、密码整机和密码系统，目前的密码硬件占比 75%、密码服务占比 19%、密码系统占比 6%。当然，还必须包括 CA 产业，USB Key 证书市场和相关身份认证系统估计占密码产业的四分之一规模。

《密码法》第二条定义了密码的用途是加密保护和安全认证，而目前的密码产业基本上都集成在安全认证产业，更大的加密保护产业并没有得到高度重视和充足发展，因为这个产业涉及到数字证书的应用生态建设问题。如 HTTPS 加密，涉及到浏览器、Web 服务器、SSL 证书等相关产业的发展。邮件加密，涉及到邮件客户端和邮件证书等相关产业的发展，这是一个需要全生态产品都支持商用密码的生态建设工程，这些生态工程都需要信创产品和系统的原生支持才能完成。

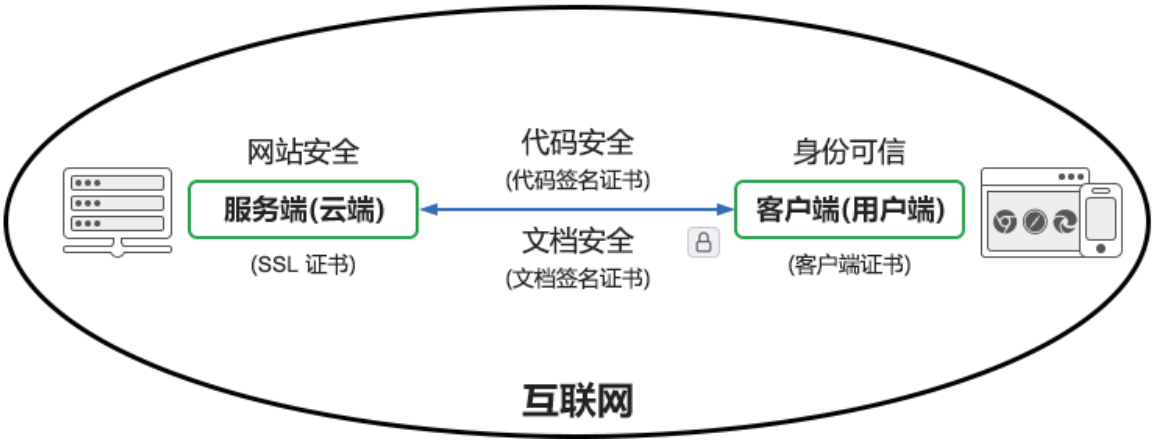
目前的大部分密码产品，如密码芯片、密码硬件(如网关)的出现都在为了解决现有基于 RSA 密码体系的系统不支持商用密码而设计，如果信创 CPU 和操作系统能原生支持商用密码算法，则就不再需要额外的密码芯片和外部网关来解决问题，不仅能大大提升信创产品安全性能，而且大大降低用户的密码实施成本和大大提升密码算力。而现在的两套技术体系各自为政，不仅使得密码应用非常复杂而且效率很低，大大浪费了社会资源和增加了密码应用成本。有一个非常成功的案例值得借鉴，那就是 Intel CPU 早在 2008 年内置了支持 AES 算法加解密功能，大大提升 CPU 的密码能力，这使得 ECC 算法在 SSL 证书部署上得到了普及应用。最新的 Intel QAT 技术不仅支持几乎所有 RSA/ECC 密码算法，也已经支持 SM2/SM3/SM4 商用密码算法，这些非常值得信创 CPU 学习和借鉴。

三、 信创产业和密码产业的深度融合，实现完整的信息技术应用创新

上面已经举例说明了 Intel CPU 对密码算法支持的成功案例，本部分深入探讨信创产业如何同密码产业紧密结合和深度融合。还是先让我们看看全球信息技术产业是如何同 RSA 密码

体系紧密结合和深度融合的。

电脑和内置操作系统用于用户端的办公和上网，服务器和内置的操作系统用于服务端(云端)的 Web 服务器应用，而为了保障机密信息从用户端浏览器到 Web 服务器之间的传输安全，需要用 SSL 证书来实现 HTTPS 加密。为了保证用户端的身份可信，这就需要客户端证书来实现数学签名来证明其可信身份。为了保障电子邮件的安全可信，这就需要电子邮件证书来实现电子邮件加密和数字签名。为了保证各种应用代码的安全可信，就需要代码签名证书来保证代码身份可信，上面讲到的各种硬件板卡的数字签名就需要代码签名证书来实现，Windows 操作系统就是强制要求各种软件驱动都必须有通过微软认证的数字签名才允许自动识别支持。为了保证各种文档安全可信，就需要文档签名证书来数字签名文档和文档加密证书来加密文档。目前全球互联网和各种信息系统的安全保障，都是在使用 RSA 密码体系来签发各种数字证书来实现数字签名和加密，都是由于用户端电脑和服务端服务器内生支持 RSA 密码体系而使得 RSA 密码应用非常容易实现而得到了普及应用。



同样，为了保障我国互联网和各种信息系统的安全，在已经实现了 CPU 芯片、电脑、操作系统、服务器的全部国产化后，信创产业的下一个重点就是把各种产品和系统中内置的 RSA 密码体系换成商用密码体系，全面采用商用密码来保障系统安全和身份可信。包括但不限于：

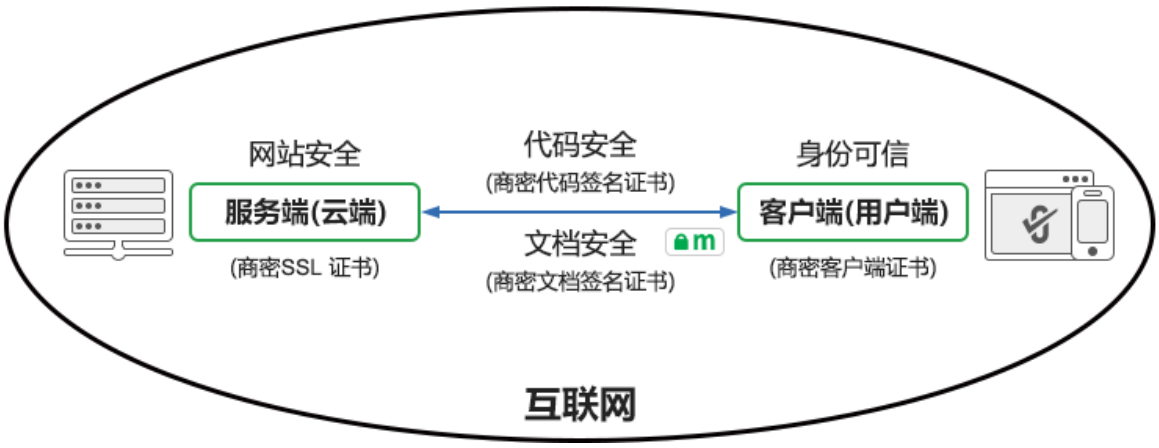
(1) 用商密 SSL 证书来实现 HTTPS 加密，这就要求信创操作系统的 Web 服务器支持商密算法和商密 SSL 证书，要求信创电脑操作系统必须默认免费配置支持商密算法和商密 SSL 证书的商密浏览器。

(2) 用商密客户端证书来实现用户端的身份认证，这就要求信创电脑的操作系统支持商密算法和商密客户端证书来实现强身份认证。

(3) 用商密邮件证书来实现电子邮件加密和数字签名，这就要求商密办公电脑操作系统必须默认配置支持商密邮件证书实现电子邮件加密的电子邮件客户端软件。

(4) 用商密代码签名证书来实现代码签名，那就需要信创电脑和服务器的操作系统都支持商密算法来验证代码的商密数字签名，只允许有操作系统可信的数字签名的代码在操作系统中运行，包括各种硬件的驱动软件的数字签名，以保障信创操作系统的安全稳定。

(5) 用商密文档签名证书来保证文档的身份可信，用商密文档加密证书加密文档来保证机密文档的安全，这就是要求信创电脑和信创服务器都支持商密算法数字签名和能验证数字签名。



以上 5 个方面的商密应用都要求信创电脑操作系统和信创服务器操作系统都有自己的可信根证书系统和可信根认证计划，只信任已通过认证的 CA 根证书签发的各种商密数字证书实现的数字签名，从而实现商用密码来保障信创操作系统安全的目标，保证国产操作系统的稳健发展。

这个保证互联网安全和操作系统安全的机制就是借鉴了国际信息技术体系来完整实现我国信息技术应用创新的机制，但是我们还不能止步如此，做到了这一步也只是达到了国际体系的 2013 年密码应用水平。国际体系在 2013 年开启了密码应用新突破，那就是 ACME(自动化证书管理环境)。目前已经实现自动化为 Web 服务器配置 SSL 证书，自动化实现 HTTPS 加密，因为所有系统(万物互联)都需要 HTTPS 加密，而手动先 CA 申请 SSL 证书部署到各种系统中去已经无法满足普及 HTTPS 加密的应用需求。所以，需要自动化为 Web 服务器配置 SSL 证书，自动化实现 HTTPS 加密。

我国密码行业标准技术委员会已经下达了由零信技术牵头制定的商用密码领域行业标准-《自动化证书管理》，这意味着在我国已经正式开启自动化证书管理生态建设，将不仅仅实现商密 SSL 证书的自动化管理，同时将实现商密邮件证书、商密客户端证书、商密邮件证书、商密代码签名证书和商密文档证书的自动化管理，意味着我国有可能快速实现商密证书的全生态

应用的自动化，这当然也是信创产业的黄金机会，无需像国际密码体系应用那样经历了从“无”到“有”和从“有”到“自动化有”的两个阶段，而是可以从“无”到“自动化有”的直接飞跃，希望信创产业界都能认识到这个黄金机会，都能抓住这个风口快速普及应用商用密码来保证各种信创系统和信创产品的安全可信，实现商用密码的快速普及应用，让商用密码真正发挥巨大作用来保障我国互联网和信息系统安全。

四、 信创产业的稳健发展的关键就是商用密码的全生态应用

信创产业不仅是新基建产业，而且是关系到国家安全的关键产业。密码产业是保障信创产业稳健发展的关键产业，密码产业的发展更需要信创产业的深度融合，两者是密不可分的产业。商用密码在信创产业所有系统和产品的全生态应用和原生态支持，是信创产业升级发展的关键，也是下一个风口，信创产业、密码产业和风投机构的企业管理层必须能看到和理解这一个制高点，这是国际信息产业和国际密码产业的制高点，英特尔、微软、谷歌、亚马逊、Cloudflare 等国际巨头都在其 CPU、操作系统和云服务中深度融合密码来保障电脑、操作系统和云服务的安全，这非常值得我国信创产业界和密码产业界借鉴和学习。

我国信创产业在第一步实现了芯片和操作系统的从无到有后，只要及时把握时机和看清大方向，就可以实现密码应用从“无”到“自动化有”的跨越式飞跃，快速实现中国式信息技术应用创新，从而有力保障数据要素的全生命周期安全，实现做大做强数字经济的宏伟目标。

有诗为证：

信创产业要飞跃，密码融合是关键。

商密原生全支持，系统安全有保障。

王高华

2024 年 1 月 26 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。
从 2021 年 12 月 9 日开始，已累计发表中文 149 篇(共 39 万多字)和英文 58 篇(7 万多单词)。