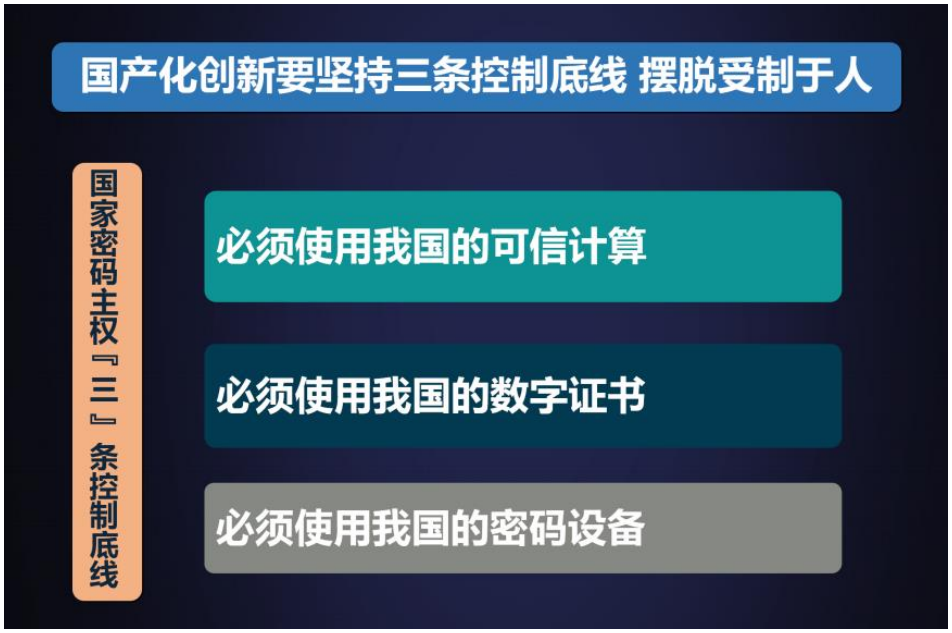
沈昌祥院士 | 国产化创新要坚持三条控制底线

笔者看到沈院士昨天在 2023 年中国网络和数据安全产业高峰论坛—商用密码创新应用分论坛的演讲的 PPT 很是兴奋，特撰文解读其中最重要的一页 PPT。沈昌祥院士是中央网信办专家咨询委员会顾问、国家集成电路产业发展咨询委员会委员、国家三网融合专家组成员，以《密码智能化跨越发展夯实网络强国、数字中国安全基石》为题目在论坛上进行了主题分享。



沈院士把“可信计算”、“国密证书”、“国密设备”列为国家密码主权的三条控制底线，高度非常高。第一个底线的基础实际上就是国密算法数字证书的应用，用国密证书作为设备证书来实现可信计算，所以笔者将重点解读第二条和第三条。

说起“**必须使用我国的数字证书**”，这里面还有一段我在 2018 年同沈院士的深度交流的深刻回忆。笔者在由中央网信办网络安全协调局、国家密码管理局指导，中国电子信息产业发展研究院主办的“**2018 网络空间可信峰会**”(2018 年 12 月 17 日-18 日)的由刘权博士主持的主论坛高端对话环节同**沈昌祥**院士(对话嘉宾第一位)、**袁文恭**研究员(第二位)、**荆继武**教授(第三位)、**刘建伟**教授(第四位)共同展开高端对话，就智能时代网络可信生态构建、密码技术发展方向、网络身份分级分类体系面临的主要问题，以及智能时代设备认证的新特点等议题做了精彩发言。

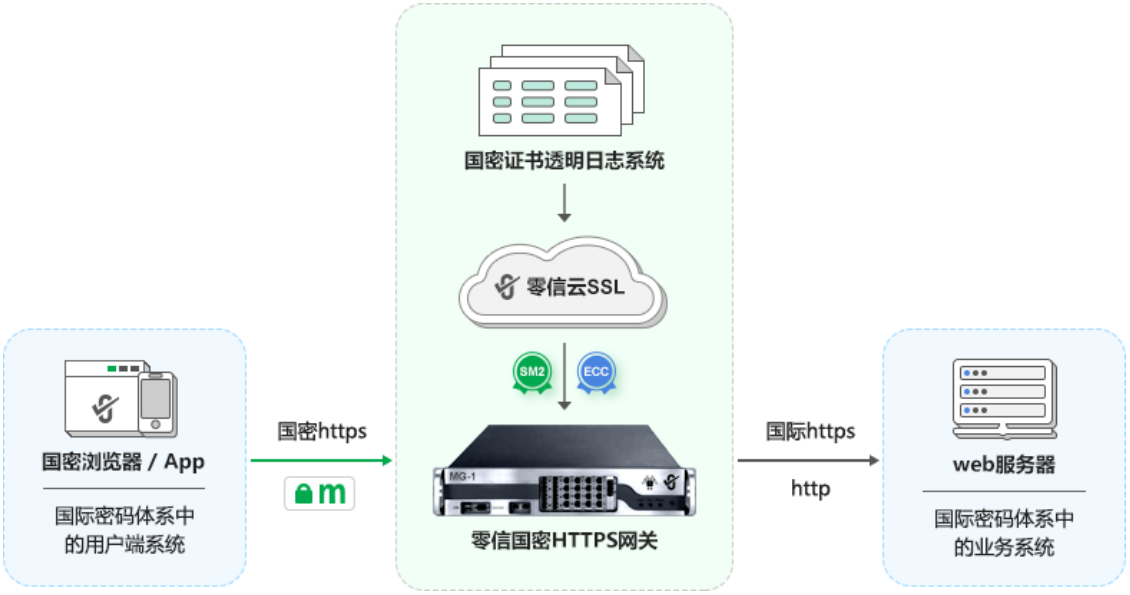
在会议午餐期间，笔者有幸同沈院士有了深度交流的机会，沈院士很关心我国的数字证书应用情况，我给他汇报了我国网站 https 加密用的 SSL 证书全部都是使用的 RSA 算法 SSL 证书，并且基本上全部都是国外 CA 签发的，他很是震惊，当场就说这怎么行呢？必须使用我国国产密码算法的 SSL 证书！并且还说我会在各种场合呼吁这件事情。这就是为何我今天看到沈院士的演讲 PPT 时很是兴奋的原因，沈院士德高望重，一言九鼎，的确是在践行他说的话和兑现他的承诺，而不是说说就算了！这让我很是感动。

就是在这个会议上，笔者做了《**商用密码网络可信生态问题与对策**》主题演讲，首次在我国提出了“**中国网络空间可信生态建设框架**”构想，参照国际上的基于 RSA 密码体系的网络可信生态，建设我国基于国产密码体系的网络空间可信生态，这个生态涉及到国产客户端软件支持国密算法和国密算法数字证书、CA 机构签发国密算法数字证书、国密证书标准体系和审计体系、各种应用系统的全面支持国密数字证书加密和数字签名。并且首次提出了实现网站 https 加密的 SSL 证书部署的“双轨制”(同时部署国密 SSL 证书和国际 SSL 证书)，并逐渐在时机成熟后自然过渡到“单轨制”(仅需部署国密 SSL 证书)。

在大会上提出构想容易，真正实施起来很难。要想普及国密 https 加密，首先需要浏览器支持国密算法和国密 SSL 证书，并且必须支持证书透明安全机制；再就是 Web 服务器必须支持国密算法和国密 SSL 证书；CA 系统能签发支持证书透明的国密算法 SSL 证书；还有 CDN/WAF 必须支持国密算法和国密 SSL 证书；还有，常用的移动 APP 也必须支持国密算法和国密 SSL 证书实现国密算法 https 加密。整个互联网应用生态产品都是基于 RSA 密码体系建立的，要改造生态中的所有产品都支持国密算法和国密 SSL 证书谈何容易！国密改造，太难了，所以我国的密改工作推进速度非常缓慢，不仅难改造，而且正在使用 RSA 算法的业务系统根本就不能停下来给你去改造！

4 年多以来，笔者不忘初心，一直在践行承诺，按照自己提出的构想一直在不断打造这个生态。虽然很难并经历了许多磨难，但是笔者很荣幸在 4 年后的现在基本上已经完成了这个生态所有产品的研发，已经具备了建设和实施这个生态的条件。笔者打造的第一个生态是国密证书透明生态，这是打造了一个国密 SSL 证书的可靠供给生态，包括国密证书透明日志系统、能签发支持国密证书透明的国密 SSL 证书的国密 CA 系统、国密浏览器，并牵头制定国密证书透明密码行业标准，联合各家 CA 和国产浏览器厂商尽快支持国密证书透明。有了国密 SSL 证书的可靠供给能力，接着打造了第二个生态—国密证书自动化管理生态，这是一个借鉴国际 SSL 证书快速部署的成功经验-ACME(自动化证书管理环境)而打造的能实现快速部署国密 SSL 证书的生态，包括国密 ACME 服务系统、国密 ACME 客户端、支持国密 ACME 的国密 HTTPS 网关、国密 WAF 网关和国密云 WAF 服务等生态产品，并牵头制定国密证书自动化管理密码行业标准。

第一个生态是国密 SSL 证书的可靠供给能力，第二个生态则是国密 SSL 证书的快速部署能力，二者缺一不可，因为光有供给能力而无法落地应用还是无法实现普及国密 HTTPS 加密。而要实现快速部署，最重要的核心产品是国密 HTTPS 网关，可不要小看这个网关，它是把很难实施改造的现有的基于 RSA 密码体系的业务系统包起来不动，干脆不改造你，在你的外面增加一个硬件网关来自动化实现国密 https 加密，你里面的业务系统根本就不用改造，这也是用户最喜欢的解决方案，不影响你现有的业务系统的正常运行，不动你的服务器。有了这个利器，那普及实现国密 https 加密就只剩下这个硬件网关的生产能力和国密 SSL 证书的可靠供给能力了，这些也都是小事一桩。剩余的事情就是改造用户端了，已经有了免费的国密浏览器--零信浏览器，就只剩下常用的移动 APP 的国密算法支持了，这些常用的 APP 都是大公司造，那绝对也不是个事！



也就是说，沈院士所讲的三条控制底线的第二条和第三条都已经具备了快速实施的能力，可以“使用我国的密码设备”—国密 HTTPS 网关实现“使用我国的数字证书”的 https 加密，现有 Web 服务器零改造，快速以国密 SSL 证书和国密设备来保障我国网站系统安全。

俄乌冲突已经发生一周年了，西方 CA 在发生后十天内就吊销了已经签发给俄罗斯政府和银行网站的 SSL 证书高达三千多张(禁用)，导致政府网站和银行网站无法访问。同时停止为俄罗斯政府和银行网站签发新的 SSL 证书(断供)，这让俄罗斯措手不及，赶紧临时设立自己的 RSA 算法根证书给政府网站和银行网站签发 SSL 证书，但是西方的浏览器不信任这个新的根证书，不但不信任而且还给拉黑了。通过这个已经真实发生的把密码作为制裁手段的恶性事件，我们应该不难理解沈院士所讲的“必须使用我国的数字证书”是三条控制底线之一了，这的确是三条“国家密码主权”控制底线的最重要的一条，没有这条底线，在目前的不确定的国际形势下，我国互联网也极有可能遭遇俄罗斯一样的数字证书被断供和被禁用的互联网安全危机。

所以，我国必须有密码底线思维，必须尽快普及使用我国自主密码算法的 SM2 SSL 证书实现 https 加密，以应对可能遭遇的密码应用安全危机。笔者非常感激沈院士把“必须使用我国的数字证书”提高到了一个国家密码主权的高度，也非常欣慰通过这 4 年多的努力已经可以在下次见到沈院士时有成果可以向他汇报了。现在万事俱备，只差大家行动起来快速部署采用国密 SSL 证书和国产密码设备实现 https 加密的普及应用了。

王高华

2023 年 2 月 25 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。