国产 CPU+国产 OS+免费国密浏览器：信创电脑的“最后一块拼图”终于补齐

2026 年 6 月 17 日

今天，零信浏览器正式发布基于国产 CPU-龙芯 3A6000 处理器、适配银河麒麟国产操作系统的信创版本。这款浏览器不仅永久免费，更是率先同时支持国密算法和国密混合后量子密码（PQC），兼容 RSA/ECC 及国际混合 PQC。这一版本的推出的背后，是政务数据安全和关键信息基础设施保护的重大突破。

一、国密改造“堵点”：浏览器端短板正在拖政务安全的“后腿”

近年来，信创产业高速发展，国产 CPU 和国产操作系统已在政府部门实现规模化普及应用。从中央到地方，龙芯、飞腾、鲲鹏等国产芯片与麒麟、统信操作系统的组合，已经成为政务办公的主流配置。然而，硬件和操作系统替代到位了，**“浏览器”这个最后的上网入口反而成了国密改造全链路中的最大堵点。**

目前，大量信创电脑仍默认配置不支持国密算法的普通浏览器，或预装仅提供 90 天试用版、后续需要付费才能继续使用的国密浏览器。这些普通浏览器无法正确识别国内 CA 机构签发的国密 SSL 证书，当用户访问部署了国密 SSL 证书的网站时，浏览器便会直接报错、提示“使用了不受支持的协议”。

现实中有多少单位面临这一问题？据行业调研数据显示，超过 90%的政企用户在信创迁移初期遇到过浏览器兼容问题障碍，这就是国密改造中典型配置双算法 SSL 证书的被动适用办法。为什么会出现这种尴尬局面？因为 Web 服务器端已经花大力气完成了国密改造，网站已经部署了国密 SSL 证书、支持国密 SM2 算法，但用户上网工具端却没有真正支持国密算法的浏览器可供免费使用。服务器端的国密投入变成了“单边工程”：**服务器已经能说“国密话”，**

浏览器却听不懂国密语言，国密 HTTPS 加密通道根本无法建立。

这种“服务器端准备好了，浏览器端不支持”的局面，导致国密改造徒有其表，政务数据在公网和内网的传输安全依然存在重大隐患。大量单位不得不沿用普通浏览器处理关键业务，这些浏览器不支持国密算法、无法适配国产软硬件生态、无法正确识别国内 CA 机构颁发的国密 SSL 证书。看似技术细节的短板，恰恰成为我国信息安全体系中最易被攻击的薄弱点，本以为不是事的事成为了障碍普及国密的大事。

二、普及国密 HTTPS 加密应用，亟需免费国密浏览器

回顾全球互联网的安全发展史，RSA 密码体系之所以能够在全球范围内普及应用，**完全免费的浏览器是第一功臣**。

Netscape 是第一家产品化的浏览器厂商，但其浏览器是收费的，虽然收费模式只是昙花一现。而微软则是全球第一个率先推出完全免费浏览器的大厂，IE 浏览器为全球数十亿用户提供了最基础的加密上网工具。谷歌将 Chromium 浏览器内核全面开源，为全球绝大多数主流浏览器提供了技术底座。谷歌浏览器、微软 Edge 浏览器、苹果 Safari、Mozilla Firefox 这四大完全免费的浏览器，让普通用户和企业用户在不支付任何费用的情况下，就能使用 HTTPS 加密来保护上网数据传输安全。正是免费浏览器铺平了道路，才使得基于 RSA 密码体系的 SSL 证书的商业化得以蓬勃发展，CA 机构卖证书赚钱的前提，是用户浏览器能用且免费。免费浏览器是信息产业生态支持 RSA 密码体系的基础工具软件，意义重大。

同理，我国要想普及国密 SSL 证书和国密 HTTPS 加密应用，首先必须有完全免费的浏览器支持国密算法。这个使命当然不能靠那些从未原生支持国密算法的国外四大浏览器来完成，必须由国产浏览器来承担。

这就是零信技术研发零信浏览器的初衷，承诺永久免费支持国产密码算法的根本原因。市

场上现有的其他国密浏览器都采取了收费模式，导致大量信创用户只能在试用期结束后要么放弃国密使用、要么承担额外采购成本。而零信浏览器从诞生之初就坚持完全免费、干净无广告的路线，让每一个用户，无论是使用 Windows 电脑还是信创电脑，无论个人和单位，也不论身处哪个政府部门、不管预算是否充裕，都能零成本获得一个支持国密 HTTPS 加密的上网工具。**只有让国密浏览器像当年的 IE 浏览器和现在的 Chrome 一样真正免费、人人可用，国密 HTTPS 加密才能真正实现从“示范工程”到“全民普及”的跨越。**

三、政务数据面临“先收集后解密”威胁，国密与 PQC 混合加密势在必行

量子计算的飞速发展，正在对当前所有基于传统密码算法的加密体系构成根本性威胁，RSA、ECC 乃至国密 SM2 算法在未来量子算力面前都将面临被破解的风险。

更大的安全隐患在于：攻击者现在已经大量收集 HTTPS 加密传输的政务数据并长期保存，待量子计算机可用时再集中批量解密，这就是业界公认的**“先收集后解密”**安全威胁。政务外网、内网中的海量敏感信息，涉密公文、人事数据、财政信息、关键基础设施运行数据等，如果今天仅靠传统密码 HTTPS 加密传输，未来可能在量子计算机面前变得毫无秘密可言。

欧美各国已要求在 2030 年前完成后量子密码迁移，全球互联网流量中已有 68%流量实现了国际混合 PQC 加密。我国密码技术团队基于国际抗量子密码算法已经普及使用但国产抗量子算法还未出台之现状，提出了睿智的应对之道：**国密算法与后量子密码算法（PQC）的混合密钥封装 HTTPS 加密**。混合加密并非用 PQC 替代国密，而是在同一通信链路中同时使用国密算法和 PQC 算法进行双重加密，让数据同时获得国密合规保护和抗量子攻击能力。这种“双栈保护”既满足《密码法》和密评的合规要求，又能确保关基数据在量子计算时代依然安全。SM2MLKEM768 就是这样的典型混合方案，它成功获得了国际互联网号码分配机构 IANA 分配的正式编号 4590，标志着国密+PQC 混合 HTTPS 加密正式进入国际标准化轨道。

但在互联网应用中，仅靠服务器端部署混合加密远远不够。**如果浏览器端不支持国密混合 PQC 算法，这条加密链路仍然是“断头路”！**服务器发出的 PQC 加密数据到达浏览器时，如果浏览器无法解析，加密就会自动降级回传统密码算法，服务端的量子安全防护形同虚设。因此，国产操作系统的浏览器端对国密混合 PQC 的原生支持，是实现全链路量子安全防护的最后一环。

四、零信浏览器信创版：为国密合规与量子安全提供“端到端”解决方案

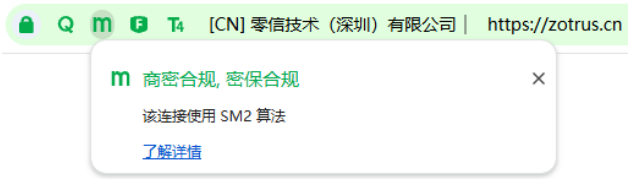
零信浏览器此前的版本仅支持 Windows 操作系统，无法为信创环境用户提供国密混合 PQC 高安全的 HTTPS 加密服务。此次发布的信创版本，支持最大市场份额的龙芯+麒麟的信创组合，具有三大里程碑式的意义：

首先，真正打通了纯国产全链路。龙芯 3A6000 是龙芯中科最新一代桌面处理器，性能已达到国际主流水平；银河麒麟是信创操作系统领域的“枭雄”，覆盖政务办公的超七成终端。零信浏览器完成对双主流平台的深度适配，意味着用户从按下开机键那一刻起，**国产 CPU、国产 OS、国产密码算法、国产浏览器**四位一体，不再有任何“卡脖子”的间隙。这不仅是技术适配的成果，更是信创生态从“可用”迈向“**好用**”的重要标志。

第二，率先实现了国密算法与国密混合 PQC 双支持在信创环境的支持。零信浏览器不仅原生支持 SM2/SM3/SM4 国密算法，还率先支持了国密算法与后量子密码的混合算法（SM2MLKEM768）HTTPS 加密。零信浏览器内部构建了九级算法自适应优先级，从纯国产 PQC 算法、纯国际 PQC 算法，到国密混合双 PQC 和国际混合双 PQC 算法、再到传统 SM2、ECC 和 RSA 算法，能够根据服务器端支持的算法类型自动选择最优的加密方案。同时，零信浏览器创新地在地址栏增加显示“**m**”标识（国密合规）和“**Q**”标识（量子安全），让用户一目了然自己的数据正在受何种级别的加密保护。

第三，形成了浏览器+网关的端到端全链路国密合规与量子安全闭环。零信浏览器与零信国密 HTTPS 加密自动化网关互为配套，自动化网关实现服务端双算法 SSL 证书的自动化申请和部署，浏览器实现客户端对国密和 PQC 的原生支持。从用户访问网站的那一刻起，HTTPS 加密便在浏览器和网关之间以国密混合 PQC 的最优算法建立，数据传输全链路同时满足国密合规和量子安全要求。这意味着，无论用户是访问公网政务网站，还是登录内网办公系统，每一次点击、每一次表单提交都受到国密和 PQC 双重保护，“先收集后解密”的威胁被真正阻断。

信创电脑的硬件和操作系统已经铺进了政府部门的每一间办公室，但国密改造的“最后一公里”过去一直被浏览器这个看似不起眼的小工具所困。零信浏览器信创版本的发布，补齐了这最后一块拼图。



零信浏览器信创版是一款真正免费的国密浏览器，不设试用期、不设授权限制，全功能对每一位用户开放。它同时支持国密算法、国密混合 PQC 和国际算法，兼容 RSA/ECC，适配龙芯 3A6000+麒麟的全链路国产环境，与零信国密 HTTPS 加密自动化网关配合，从客户端到服务端构建起国密合规与量子安全双重保障的 Web 安全防护体系。

我们相信，零信浏览器信创版本的发布，将真正推动国密 HTTPS 加密应用的全面普及，守护政务数据及所有关基数据的每一次端到端传输在今天、明天，乃至量子时代的持续安全。

欢迎免费 下载 使用零信浏览器信创版本，目前仅适配龙芯+麒麟版本，更多国产 CPU 和国产操作系统的版本后续陆续发布。

王高华

2026 年 6 月 22 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 275 篇(共 81 万 7 千多字)和英文 119 篇(16 万 6 千多单词)。