国产操作系统代码签名保障：标准化进程与生态共建

2026 年 1 月 13 日

在一次行业交流会中，某国产操作系统厂商的技术负责人坦言：“我们虽然建立了自主的操作系统，但硬件驱动的数字签名仍普遍采用 RSA 密码体系，这在技术上仍存在依赖和受制于人。”笔者当时的回应是：这真的不是什么事了，绝对不是什么受制于人的事情！我国不仅是硬件制造大国，更是密码技术应用大国，完全有能力构建自主可控的商密代码签名体系。通过推进“双算法双签名”技术方案—驱动程序同时携带 RSA 和 SM2 双算法签名，我国可以在兼容现有生态的同时，逐步实现技术自主。但这不仅是技术问题，更是标准制定与生态协同的系统工程。

当前，国产操作系统在党政、金融、交通等关键领域加速推广，其安全机制的完善迫在眉睫。为构建可信可控的操作系统环境，必须建立覆盖开发、分发、运行全流程的代码签名保障体系。本文将结合我国代码签名应用现状，探讨国产操作系统代码签名的发展路径与实施建议。

一、Windows 代码签名保障机制值得借鉴

Windows 通过三级签名机制构建了完整的软件信任链：

(1) **应用层强制数字签名**

未签名软件默认禁止运行，用户需手动确认风险，有效拦截恶意代码。并且国际标准要求不允许有代码签名软证书，都必须是 USB Key 硬证书，这是为了保障代码签名证书本身的安全。

(2) **驱动双重签名认证**

硬件驱动软件须先由开发者使用 EV 代码签名证书签名，通过微软硬件认证后，再由微软 Windows 硬件认证证书重新签名，才能实现无缝安装和同步更新分发，这就形成了双重信任保障。

(3) **系统内核启动验证**

系统核心文件均须由微软内核证书签名，启动过程中逐级验证签名，确保系统安全启用和软件完整性。

该机制从应用、驱动到内核实现全链路可信验证，为国产系统代码签名应用提供了成熟的安全架构参考。

二、国产操作系统代码签名支持与标准化进程

目前主流国产操作系统已在代码签名方面取得阶段性进展，同时相关标准体系正在逐步完善：

(1) 系统支持现状

- **麒麟操作系统**

  已支持 SM2 算法代码签名，并在政务等场景中试点驱动签名要求，但不是强制要求，硬件生态的 RSA 签名依赖仍然存在。

- **统信 UOS**

  建立应用签名审核机制，支持 SM2 算法代码签名证书，并在自研生态中推进签名验证，但在跨平台驱动兼容方面仍需加强，也还没有实施强制要求。

- **鸿蒙系统**

  从架构层面集成可信执行环境，在物联网与移动终端中推行 SM2 算法代码签名，正逐步向 PC 级生态扩展。目前也不是强制要求。

(2) 标准体系建设进展

我国已初步形成覆盖密码算法、证书管理、系统安全的多层标准框架：

- **基础密码标准**

  《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》为商密算法应用提供合规依据。

- **行业应用规范**

  金融、政务等领域在系统安全要求中逐步明确商密算法签名支持，形成行业级推动力。

- **专项标准在途**

  针对操作系统代码签名的专项国家标准已在起草中，预计将明确签名格式、验签流程、证书管理、代码签名证书签发等技术要求。

当前挑战在于：尚未形成如 Windows WHQL 认证那样的强制性生态签名规范，双算法兼

容机制缺乏统一标准；不同国产系统间的签名互认体系尚未建立。这是一个生态建设问题，我国应该参考国际体系。首先是必须有 CA 机构依据相关的密码行业标准签发 SM2 算法代码签名证书，其次是操作系统厂商必须信任这些 CA 机构签发代码签名证书的根证书，可以采用直接信任国家根的方式简化根证书信任体系，只需预置信任国家根即可。操作系统厂商必须实施强制要求所有应用软件包括硬件驱动程序都必须有可信数字签名和时间戳签名，只有这样，软件开发商和硬件厂商才会去申请商密代码签名证书实现代码签名。

三、零信技术双算法双签名云服务方案

为助力国产系统在兼容现有代码签名生态的同时构建自主签名体系，零信技术计划在单国际算法代码签名云服务基础上推出“双算法双签名代码签名云服务”：

- **双签名自动化**

  软件开发者可使用零信代码签名云服务，一键实现软件代码的双签名和双时间戳，用户无需直接向 CA 申请代码签名证书。由零信云签名服务系统自动化对接相关 CA 实现证书申请和签发，RSA 算法代码签名证书由微软指定的国际 CA 签发，SM2 算法代码签名证书由国内 CA 签发。用户可选只实现 SM2 算法代码签名和时间戳。

- **智能验签适配**

  - Windows 系统自动识别并验证 RSA 签名，保障现有兼容性；
  - 国产操作系统优先验证 SM2 签名，实现自主可控。

- **灵活部署支持**

  支持纯 SM2 签名模式，满足完全国产化环境需求；提供 API 与自动化工具，降低开发适配成本。

该方案旨在通过技术手段弥合生态断层，大大减轻软件开发商和硬件厂商的代码签名负担，推动商密代码签名在渐进式升级中落地应用。

同时，零信代码签名云服务计划第一时间免费升级支持后量子密码（PQC）算法数字签名，可行的方案是传统密码算法和后量子密码算法双签名，不仅确保了老系统的兼容，而且确保了企业的软件供应链能够抵御未来的量子计算威胁，这是传统硬件证书签名难以灵活实现的巨大优势。

四、实施建议：标准、生态与政策协同

为系统推进国产操作系统代码签名体系建设，建议从以下方面着手：

1. **加快标准制定与迭代**

   推动《操作系统代码签名技术规范》等专项标准尽快出台，明确双算法签名格式、验签优先级、兼容性测试等要求，并建立标准动态更新机制。

2. **构建跨平台互认体系**

   建立国产系统间代码签名互认机制，推动“一次签名，多系统运行”。这个互认机制实现并不难，因为国内 CA 都有一个统一的国家根证书，只要操作系统厂商预置信任国家根证书，并能按照《操作系统代码签名技术规范》来验证代码签名即可。

3. **强化政策推动与合规要求**

   结合网络安全法、等保 2.0、关基保护条例等政策，在党政、金融、能源等重点领域率先推行强制代码签名要求，不仅能真正有效保障使用国产操作系统的系统安全，而且还能给代码签名产业形成示范效应。

4. **完善工具链与服务生态**

   鼓励第三方服务商提供低成本、自动化的双算法签名服务和签名工具，降低开发者使用门槛；推动 CA 机构、测试认证中心、安全厂商协同共建代码可信服务生态。

五、密码保障操作系统安全，抓紧代码可信生态建设

代码签名是密码的重要应用之一，代码签名是操作系统安全体系的基石，只有代码签名技术才能真正做到让攻击者“进不去、拿不到、改不了、瘫不成、赖不掉”的防护效果，代码签名应该成为构建自主可控信息技术生态的关键环节。当前，国产操作系统代码签名在技术实践、标准建设、生态协同等方面已具备一定基础，正处在从“试用”到“可用”再向“好用、强用”迈进的关键阶段。

我们应抓住国产化替代的历史窗口，从起步阶段就要构建以商密算法为核心、兼容现有生态、强制可信验证的代码签名体系。这需要技术突破、标准引领、政策推动与生态共建的多轮驱动。唯有如此，国产操作系统才能在安全可控的轨道上行稳致远，真正支撑起数字中国建设的宏伟蓝图。

王高华

2026 年 1 月 13 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 256 篇(共 75 万 1 千多字)和英文 114 篇(15 万 5 千多单词)。