代码签名云服务一定会成为签名代码首选

2026 年 1 月 6 日

代码签名是一个比较“古老”的技术了，一个比 HTTPS 加密更早流行的密码应用。早在 IE 浏览器恶意插件横行的 90 年代，微软为了遏制恶意插件强制要求所有浏览器插件(.cab)都必须有数字签名，没有数字签名的插件不允许安装。这个解决方案的思路一直沿用到了现在，没有数字签名的代码 Windows 是默认阻止运行的。本文通过讲解代码签名证书的发展历程，让读者朋友理解为何代码签名的终极解决方案是云签名服务。

一、 代码签名三个发展阶段

最早的代码签名证书都是软证书(.pfx)，IE 浏览器支持在线生成私钥和 CSR 文件，CA 签发证书后支持自动化安装到 Windows 中，用户可以导出为.pfx(.p12)证书文件到处使用，非常方便。这是第一阶段，开始使用代码签名证书来证明软件的可信身份。

随着代码签名证书的普及应用，恶意软件也有了数字签名，CA/浏览器论坛于 2007 年制定了 EV 代码签名证书标准，这是参考 EV SSL 证书的更加严格身份认证的标识更高信任级别软件的解决方案，使得 EV 签名的软件在 SmartScreen 中获得更快的信任建立。这是第二个阶段，进一步加强软件开发者的身份认证。

正是由于所有软件都必须有代码签名，但申请 EV 代码签名证书有一定的门槛，这就导致了大量的代码签名证书被盗的发生，因为软证书容易被盗。所以，为了保障代码签名证书私钥安全，国际标准要求 2016 年 6 月 1 日起 EV 代码签名证书私钥必须存储在 FIPS 140-2 级以上、Common Criteria EAL 4 级以上或同等认证级别的硬件设备上，这是代码签名证书安全标准的一个关键分水岭，标志着行业对软件供应链安全保护提升到了一个新的强制硬件级别。而这个要求在 7 年后(2023 年 6 月 1 日)适用于普通代码签名证书，要所有代码签名证书的私钥生成、存储和签名操作必须在经过认证的硬件设备中进行，确保私钥永远无法以明文形式离开硬件设备，从而极大程度上杜绝私钥被盗的风险。这是第三个阶段，不再有软证书，都是硬证书，无论是普通代码签名证书还是 EV 代码签名证书。

可以看出：代码签名的三个发展阶段是从软证书到硬证书的发展过程，不仅在不断提升可信身份的要求，而且在不断提升可信身份的保护力度，彻底升级全球软件供应链的安全基石，

从根本上解决因私钥泄露导致的系统性信任危机。

二、 代码签名面临两大难题

实现代码签名就必须有代码签名证书，而为了保护代码签名证书的私钥安全，必须在通过严格认证的硬件密码设备生成、存储和使用私钥。这就要求 CA 在完成用户身份鉴证后，在合规的 USB Key 中生成私钥和导入证书，再从美国或欧洲快速 USB Key 硬件给用户，一般都需要 10-15 天时间，这是用户遇到的第一个难题：等！不仅仅是要等，还要支付高达 50 美元的运费！

第二个难题是不断缩短的代码签名证书有效期，现在是 3 年有效期，2026 年 3 月 1 日缩短为一年零 3 个月(15 个月)有效期，也就是说从 2026 年 3 月开始只能购买一年期证书，每年都要花钱从美国快递 USB Key，每年都要等收到硬件 UKey 证书才能签名代码，如果软件有 Bug，急需更新发布版本怎么办？这是用户遇到的第二个难题：不仅要等，而且每年都要等一次！

这个不断缩短代码签名证书有效期的步伐也可以从 SSL 证书中看到：2029 年 3 月 15 日将缩短为 47 天，可以预见的是代码签名证书有效期也一定会不断缩短的，不会停留在一年期中 ，这是因为传统密码算法 RSA/ECC/SM2 无法抵御量子计算攻击，使得代码签名机制来保障软件代码的可信身份不再有效，目前的解决方案是不断缩短证书有效期来缩短攻击窗口，同时积极推进后量子密码算法实现数字签名。

三、 零信技术完美解决两大难题

零信技术也是代码签名证书的用户，因为零信浏览器会定期发布版本，有大量的代码需要数字签名，所以我们深知软件开发商的代码签名痛处。应用安全是零信技术规划的五大零信任+密码技术解决方案之一，在完成了最重要的网站安全解决方案后，零信技术投入研发力量，完美解决了代码签名面临的两个难题。

第一个难题是必须等美国 CA 快递 USB Key，零信技术的解决方案是让美国 CA 认可使用中国制造的 USB Key，用户就不用等快递了。零信技术只需第一次快递灌好证书的 USB Key 给用户，以后就不再需要快递 UKey 硬件了，直接使用原 UKey 续期证书即可。

第二难题是不断缩短证书有效期，零信技术的解决方案是为用户提供代码签名云服务，用户不用担心将来代码签名证书有效期有多长，只需按需购买代码签名服务即可，证书签发即刻

可以用于签名软件代码。零信技术采用通过 FIPS 140-2 Level 3 认证的密码机(HSM)来生成代码签名证书密钥和保护签名密钥，安全合规，并得到了两家国际 CA 的大力支持和技术配合。

这就是零信技术上线的应用安全解决方案，用户可选任何一种方式来保护私钥安全，两种方式都是不用等国际快递，都能为用户快速提供代码签名服务，并大大降低代码签名的使用成本。

零信代码签名云服务遵循国际云签名联盟发布的云签 API 标准，不仅有力保障了云签服务质量，更重要的是为有开发能力的用户提供了基于国际标准的 API 接口，方便用户集成代码签名自动化服务到其代码自动化管理系统中。

四、 云签名服务必将成为代码签名首选

使用零信代码签名云服务无需等待国外 CA 快递 USB Key 证书，完成身份认证和证书签发，就可以马上使用代码签名云服务来签名各种软件代码，无论用户选购的是个人版、单位版还是单位 EV 版，都无需费力管理硬件 UKey。不仅解决了签名密钥的安全问题，而且解决了用户无法马上拿到证书的难题，更重要的是彻底把用户从繁琐的硬件 UKey 管理中解决出来，充分享受便捷的云服务来按需数字签名软件代码。

零信代码签名云服务还有两个独家技术优势：一是不按签名代码数量收费，仍然像传统 UKey 证书一样按年固定收费；二是不用上传待签名的软件代码，采用先进的签名和代码分离技术，只提交代码 HASH 值到云端签名服务系统，不仅签名快，而且确保了用户代码安全。

不仅如此，为了应对量子技术对代码签名的安全威胁，零信技术一直在紧跟相关国际标准，会在第一时间为云签用户免费升级支持混合 PQC 算法代码签名服务，这也是传统硬件 UKey 证书无法做到的特别优势。

综上所述，代码签名云服务一定会成为代码签名首选，就像现在用户首选其他云服务一样，不仅快还省钱。零信技术计划下一步提供国产操作系统的代码签名云服务，期待同国产操作系统厂商的紧密合作，共同努力，用国密 SM2 算法代码签名证书和代码签名云服务来保障国产操作系统的基础安全和内核安全。当然，这也为全球代码签名用户提供了更多的选择和更好的代码签名云服务。

王高华

2025 年 1 月 6 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 249 篇(共 73 万 7 千多字)和英文 108 篇(14 万 8 千多单词)。