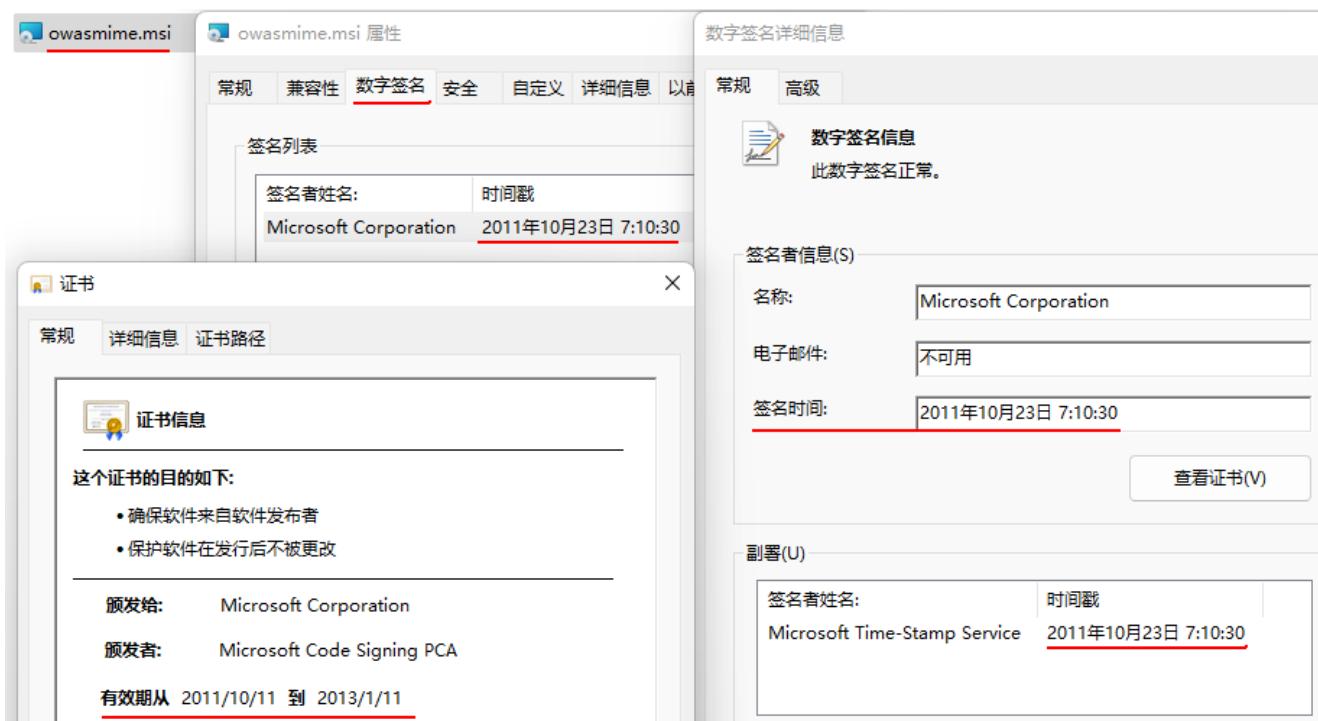


为何代码签名必须有时间戳？

2026 年 1 月 6 日

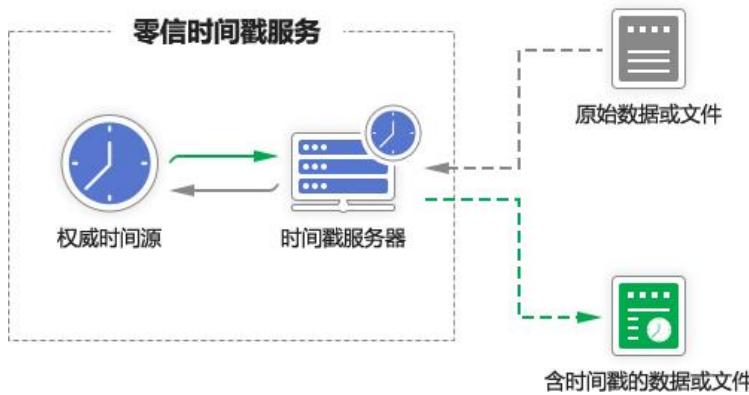
为了保障 Windows 系统安全，微软采用的是安全策略就是零信任原则，不信任没有数字签名的软件，所有软件都必须有数字签名。本文讲一讲为何代码签名必须要有时间戳，大家先看一下一个“古老”软件-IE 浏览器 S/MIME 邮件加密插件的数字签名截图：



此软件的签名时间为 2011 年 10 月 23 日，代码签名证书已于 2013 年 1 月 11 日过期，但是其数字签名在十几年后的今天仍然有效，仍然可以运行安装并显示签名者信息，这就是时间戳的作用。如果没有时间戳，虽然软件有数字签名，但是一旦用于数字签名代码的代码签名证书过期，则数字签名就无效了。目前代码签名证书最多是 3 年有效期，今年 3 月 1 日起为一年有效期，而一个软件的生命周期一般长于一年的，特别是一些工具软件或者设备驱动程序，就像上面的软件到今天都 14 年多了。

时间戳也是一种数字签名，必须有一个提供时间戳签名服务的系统，称之为“时间戳系统”或“时间戳服务器”，当然也必须有一张时间戳签名证书。其工作原理示意图如下图所示，用

户使用代码签名工具对待签名文件生成摘要数据，并把此数据提交给时间戳服务器请求签名，时间戳服务器对摘要数据和一个来自权威时间源的一个日期/时间记录进行签名，生成时间戳签名数据返回给签名工具，签名工具把此时间戳数据写入到待签名的文件中即完成时间戳签名。



零信代码签名云服务全自动为每次签名都附署了全球信任的时间戳签名，确保了每次签名的代码在代码签名证书过期后其数字签名仍然有效，保障了软件的全生命周期安全可信。

王高华

2026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 250 篇(共 73 万 7 千多字)和英文 109 篇(14 万 7 千多单词)。

