科普：云签服务的核心技术是 HASH 签

2026 年 1 月 9 日

数字签名，对很多人来说既熟悉又陌生。大家都知道它在保障电子文件真实性、完整性方面至关重要，但你是否想过，当你在使用各种电子合同云签服务时，你的合同文件究竟经历了什么？今天，我们就来深入探讨一个关键问题：为什么说 **“HASH 签”** 是现代云签服务的核心技术，而不仅仅是一个基础步骤。

一、 数字签名的本质：签名 HASH

首先，我们需要理解一个基础概念。数字签名并非直接对一个大文件本身进行复杂的数学运算，那样效率极低。实际上，它采用的是“指代”的方式：

(1) **生成“数字指纹”（HASH）**：通过哈希算法（如 SHA256/SM3），将任意长度的文件内容，计算成一个固定长度（如 32 字节）、唯一对应的字符串，这就是 HASH 值。文件哪怕只改动一个标点，HASH 值都会彻底改变。它可以看作是这个文件的高度浓缩且不可伪造的“指纹”。

(2) **对“指纹”进行数字签名**：数字签名就是使用签名者的私钥，对这个 HASH 值进行密码运算，生成一段独特的签名数据。

(3) **验签**：验证者用签名者的公钥解密签名数据，得到 HASH 值 A，同时自己计算文件的 HASH 值 B。如果 A=B，就证明文件自签名后未被篡改，且签名者身份真实。

所以，所有数字签名最终签的都是文件的 HASH 值，这是密码学的基石和常识。

二、 传统云签模式：便捷背后的隐忧 —“文件上传”之患

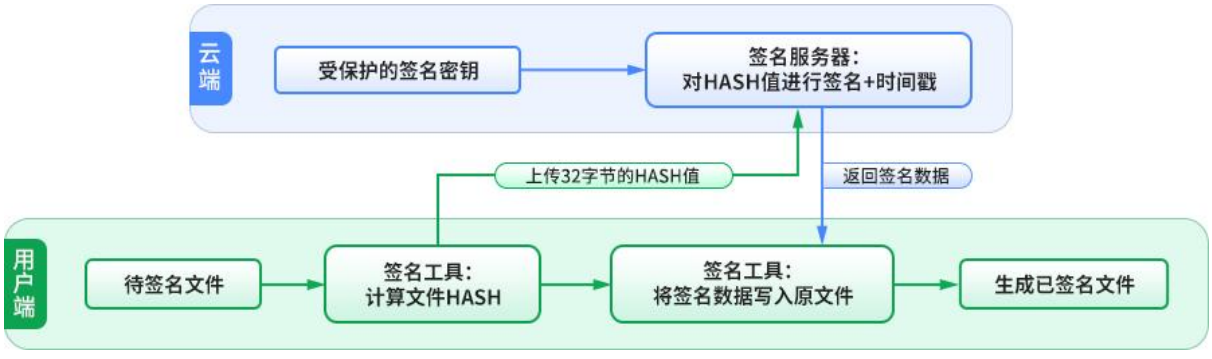
既然数字签名签的是 HASH 值，那为什么目前大家常用的电子合同签署服务都要求用户上传整个合同文件到签署平台呢？这主要是为了简化流程和降低客户端复杂度。服务商在云端统一完成“计算 HASH”和“签名 HASH”两步。当然，也不排除服务提供商不具备提供文件和签名的分离和合并技术。总之，这种“全包式”服务看似省心，却带来了不容忽视的安全与合规风

险：

- **数据泄露风险**：你的敏感合同、创意文档或核心代码，需要离开你的可控环境，进入第三方服务器。即使服务商信誉良好，但传输过程、服务器安全、内部管理都可能成为潜在漏洞。对于企业而言，这等于主动增加了商业机密和知识产权暴露的攻击面；对于个人来讲，这等于主动把自己的个人机密信息暴露给无关的第三方。
- **合规挑战**：越来越多的行业法规（如金融、医疗、政务）和数据保护法（如 GDPR）强调“数据最小化”和“隐私设计”，要求尽可能减少敏感数据的流动和非相关的第三方接触。无条件上传文件到云端的做法与此合规要求相悖，是违规行为。
- **效率瓶颈**：签署一份几百兆的设计图纸或 1G 大小的软件安装包？你需要等待漫长的上传时间，消耗大量带宽，用户体验在关键时刻大打折扣。某签名平台甚至不允许上传超过 100 兆的文件，导致用户无法使用其云签服务。

三、 先进模式解密：端云协同与“HASH 签” — 安全与效率的平衡艺术

真正的技术创新，在于重新划分任务的执行边界。先进的云签服务采用了 “端云分离协同”架构，其核心就是 **“HASH 签”**模式。整个签名流程图可以清晰展示这一过程，如下图所示，本地签名工具计算待签名文件的 HASH 值，只提交 HASH 到云端签名服务器，完成 HASH 值数字签名加时间戳后返回已签名数据给签名工具，由签名工具把签名数据写入待签名文件中完成数字签名。



这一模式的核心优势在于：

(1) **数据不动，HASH 动**：文件的“本体”寸步不离用户本地环境，彻底杜绝了因传输和云端存储导致的内容泄露。云端服务器“看到”的只是一串无含义的、无法反推出原文件

的 HASH 字符串，切实保障了用户数据安全。

(2) **权责清晰，各司其职：**

- **用户端：**完全掌控原始文件，负责生成其“指纹”（HASH）。这是用户隐私和所有权的体现。
- **云端：**专注于提供高强度安全保障的签名运算，签名私钥生成、存储和密码运算都由通过认证的密码机(HSM)完成，同时提供时间戳签名服务和高效的签名管理。这是专业性和权威性的体现。

(3) **体验飞跃：**无论文件是 1KB 还是 1GB，需要上传的都只是同一个固定长度的 HASH 值（32 字节）。签名请求几乎是瞬间发出和完成，特别适合自动化流水线、大量和大型文件数字签名应用场景。

四、 行业实践：零信代码签名云服务

在要求极高的软件代码签名领域，“**HASH 签**”模式的价值尤为突出。零信代码签名云服务正是这一技术的典范应用。

- **真正的零接触：**开发者的源代码或编译后的程序，始终保存在内部构建服务器或开发机上。云签服务在签名过程中，对其内容无法触及，真正实现了“零信任”环境下的安全操作。
- **专业安全，化繁为简：**签名私钥存储和签名运算都是由通过 FIPS 140-2 Level 3 认证的云端密码机（HSM）完成，安全等级远超多数企业自建环境。用户从此无需担忧传统签名的硬件 UKEY 丢失、损坏或管理不当的风险。
- **无缝集成 DevOps：**在 CI/CD 流水线中，构建任务只需将生成的程序 HASH 值提交给云端签名服务，毫秒级获取签名数据后即可继续发布流程，极大加速了软件交付速度。
- **符合最高安全标准：**这种模式满足了对软件供应链安全日益严格的审查要求，确保从构建到签名的环节没有引入任何外部代码泄露风险。

五、 展望：为什么“HASH 签”是未来标配？

零信技术秉承零信任+密码技术的技术理念，不仅代码签名云服务不上传用户的代码，而且其文档签名云服务也是不上传用户的文档(电子合同)，都是采用“**HASH 签**”技术为用户提供可信可靠的云签服务。

“**HASH 签**”不仅仅是技术方案的优化，它更代表了一种服务理念的升级：云服务应该在不“看见”用户数据的前提下，为用户提供强大的计算能力。这就是零信任原则，并且与边缘计算、隐私计算等前沿理念一脉相承。

随着数字化转型进入深水区，数据已成为核心资产。无论是保护一份商业合同或个人合同，还是一行软件代码，其重要性都不言而喻。能够提供“**HASH 签**”模式的云签服务，通过精巧的端云协同设计，在不牺牲便捷性的前提下，为用户筑起了最高级别的数据安全防火墙，这才是真正值得信赖的云签服务。

总之，当您选择云签服务时，不妨问一句：“我的文件需要上传吗，还是只需要上传 HASH 值？” 这个问题的答案，将是衡量云签服务技术先进性和安全理念的关键标尺。选择“**HASH 签**”，就是选择将安全和控制的钥匙，紧紧握在自己手中。这不仅是技术的进步，更是数字时代对用户数据主权的基本尊重和核心保护。

王高华

2026 年 1 月 9 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 254 篇(共 74 万 5 千多字)和英文 68 篇(8 万 4 千多单词)。