The core technology of cloud signing service is HASH Signing

January 9, 2026

Digital signatures are both familiar and unfamiliar to many. Everyone knows they are crucial for ensuring the authenticity and integrity of electronic documents, but have you ever wondered what happens to your e-contract documents when you use various cloud-based electronic contract signing services? Today, we'll delve into a key question: why is **"HASH Signing"** considered the core technology of modern cloud-based signing services, rather than just a basic step?

1. The essence of digital signatures: Sign HASH

First, we need to understand a basic concept. Digital signatures don't involve performing complex mathematical operations directly on a large file itself, as that would be extremely inefficient. Instead, they use a method of "reference":

(1) Generating a "digital fingerprint" (HASH): Using a HASH algorithm (such as SHA256/SM3), the content of a file of any length is converted into a fixed-length (e.g., 32 bytes) unique string, which is the HASH value. Even changing just one punctuation mark in the file will completely change the HASH value. It can be seen as a highly condensed and unforgeable "fingerprint" of the file.

(2) Digitally signing the fingerprint: A digital signature is generated by using the signer's private key to perform cryptographic operations on the HASH value, resulting in a unique signature data.

(3) Verification: The verifier decrypts the signed data using the signer's public key to obtain HASH value A, and simultaneously calculates the file's HASH value B. If A = B, it proves that the file has not been tampered with since it was signed, and that the signer's identity is genuine.

Therefore, all digital signatures ultimately sign the file's HASH value, which is the cornerstone and common sense of cryptography.

2. Traditional Cloud Signing Model: Hidden Concerns Behind Convenience — The problems of "file upload"

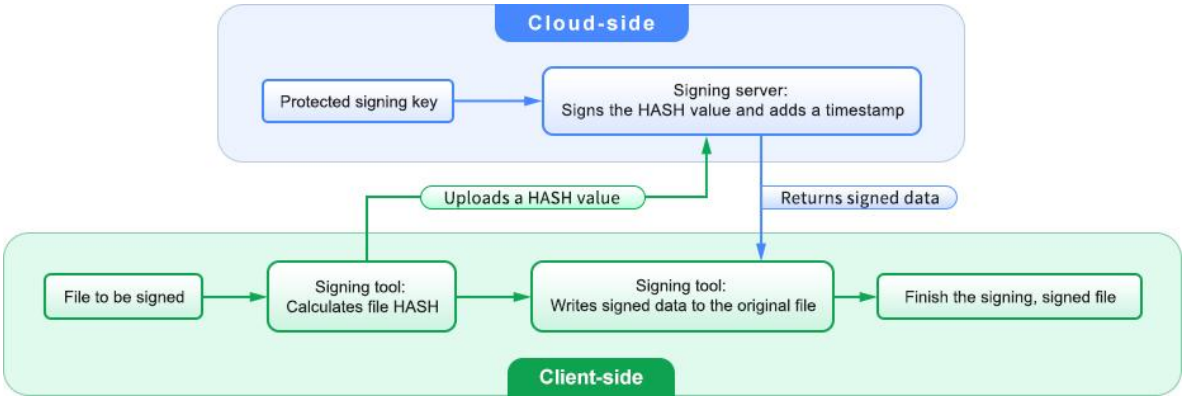
Since digital signatures are based on HASH values, why do most commonly used electronic contract signing services require users to upload the entire contract document to the signing platform? This is primarily to simplify the process and reduce client-side complexity. Service providers handle both the "HASH calculation" and "signature HASH" steps centrally in the cloud. Of course, it's possible that the service provider lacks the technology to separate and merge the document and signature. In short, while this "all-inclusive" service seems convenient, it introduces significant security and compliance risks.

- **Data breach risk**: Your sensitive contracts, creative documents, or core code need to leave your controlled environment and enter a third-party server. Even if the service provider is reputable, the transmission process, server security, and internal management can all become potential vulnerabilities. For businesses, this is equivalent to actively increasing the attack surface for exposing trade secrets and intellectual property; for individuals, it is equivalent to actively exposing their personal confidential information to unrelated third parties.
- **Compliance Challenges**: A growing number of industry regulations (such as those in finance, healthcare, and government) and data protection laws (such as GDPR) emphasize "data minimization" and "privacy design", requiring the reduction of the flow of sensitive data and contact with unrelated third parties as much as possible**.** Unconditionally uploading files to the cloud contradicts these compliance requirements and is a violation.
- **Efficiency bottleneck**: Signing a design drawing of several hundred megabytes or a software installation package of 1 gigabyte? You need to wait for a long upload time, consuming a lot of bandwidth, and the user experience is greatly reduced at critical moments. One signing platform even does not allow the upload of files larger than 100 megabytes, making it impossible for users to use its cloud signing service.

3. Demystifying advanced model: client-to-cloud collaboration and "HASH Signing" — the art of balancing security and efficiency

True technological innovation lies in redefining the boundaries of task execution. Advanced cloud-

based signing services employ a "client-cloud separation and collaboration" architecture, the core of which is the **"HASH Signing"** model. The entire signature process can be clearly illustrated in the diagram below: the local signing tool calculates the HASH value of the file to be signed, submits only the HASH to the cloud signing server, completes the digital signature of the HASH value with a timestamp, and returns the signed data to the local signing tool. The signing tool then writes the signed data into the file to be signed, completing the digital signature.



The core advantage of this model lies in:

(1) **The data remains unchanged, but the HASH moves**: the file itself stays within the user's local environment, completely eliminating content leaks caused by transmission and cloud storage. The cloud server only sees a meaningless HASH string that cannot be used to deduce the original file, effectively ensuring user data security.

(2) **Clear division of responsibilities and duties**:

- **Client side**: complete control over the original file, responsible for generating its "fingerprint" (HASH). This reflects user privacy and ownership.
- **Cloud side**: Focused on providing high-security signature operations, with signing key generation, storage, and cryptographic operations all performed by certified HSM. It also provides timestamped signing service and efficient signature management. This reflects professionalism and authority.

(3) **Experience a leap forward**: Whether the file is 1KB or 1GB, only a fixed-length HASH value (32 bytes) needs to be uploaded. Signing requests are sent and completed almost instantly, making it particularly suitable for automatic pipelines and digital signature applications for large and bulk files.

4. Industry Practice: ZoTrus Code Signing Cloud Service

In the highly demanding field of software code signing, the "**HASH Signing**" model is particularly valuable. ZoTrus code signing cloud service is a prime example of this technology's application.

- **True zero-touch**: The developer's source code or compiled program is always stored on the internal build server or development machine. The cloud signing service cannot access its content during the signing process, truly achieving secure operation in a "zero trust" environment.
- **Professional and secure, simplified for all:** Both the storage of the signing key and the signing computation are performed by a cloud-based cryptographic machine (HSM) certified to FIPS 140-2 Level 3, with a security level far exceeding that of most enterprise-built environments. Users no longer need to worry about the risks of losing, damaging, or mismanaging the traditional hardware UKey signing.
- **Seamless integration with DevOps**: In the CI/CD pipeline, build tasks only need to submit the generated code HASH value to the cloud signing service. After obtaining the signed data in milliseconds, the release process can continue, greatly accelerating the software delivery speed.
- **Meets the highest security standards**: This model meets the increasingly stringent review requirements for software supply chain security, ensuring that no external code leakage risks are introduced from the build to the signing stage.

5. Outlook: Why is "HASH Signing" the standard for the future?

ZoTrus Technology adheres to the technical concept of zero trust + cryptography. Not only does its code signing cloud service not upload users' code, but its document signing cloud service also does not upload users' documents (e-contracts). Both use "**HASH Signing**" technology to provide users with a trustworthy and reliable cloud signing service.

"**HASH Signing**" is not merely an optimization of the technical solution; it represents an upgrade in service philosophy: cloud services should provide users with powerful computing capabilities without "seeing" their data. This is the zero trust principle, and it aligns with cutting-edge concepts such as

edge computing and privacy computing.

As digital transformation enters its more complex phase, data has become a core asset. Its importance is self-evident, whether protecting a commercial or personal contract, or even a line of software code. Cloud signing service that offers "**HASH Signing**" model, through a sophisticated client-to-cloud collaboration design, build the highest level of data security firewall for users without sacrificing convenience. This is a truly trustworthy cloud signing service.

In short, when you are choosing a cloud signing service, consider asking yourself: "Do I need to upload my file, or is it just HASH value?" The answer to this question will be a key benchmark for measuring the technological advancement and security philosophy of the cloud signing service. Choosing "**HASH Signing**" means choosing to firmly grasp the key to security and control in your own hands. This is not only a technological advancement but also a fundamental respect for and core protection of user data sovereignty in the digital age.

Richard Wang

January 9, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 114 articles in English (more than 155K words) and 254 articles in Chinese (more than 745K characters in total).