Code signing Cloud service will become the first choice for signing code

January 6, 2026

Code signing is a relatively "old" technology, a cryptographic application that was popular even before HTTPS encryption. Back in the 1990s, when malicious plugins were rampant in Internet Explorer, Microsoft mandated that all browser plugins (.cab) must be digitally signed to curb malicious activity; plugins without digital signatures were not allowed to be installed. This solution remains in place today, Windows blocks code without a digital signature by default. This article explains the development history of code signing certificates, helping readers understand why the ultimate solution for code signing is cloud signing service.

1. Three stages of code signing development

The earliest code signing certificates were software certificates (.pfx). Internet Explorer supported online generation of private keys and CSR files. After the CA issued the certificate, it could be automatically installed on Windows. Users could export it as a .pfx (.p12) certificate file for widespread use, which was very convenient. This was the first stage, when code signing certificates began to be used to prove the trusted identity of software.

With the widespread adoption of code signing certificates, malware also began to use digital signatures. In 2007, the CA/Browser Forum developed the EV code signing certificate standard, a solution for identifying software with higher trust levels through stricter validation, referencing EV SSL certificates. This allowed EV-signed software to gain trust more quickly in SmartScreen. This was the second phase, further strengthening the identity validation of software developers.

Because all software requires code signing, but obtaining an EV code signing certificate has certain barriers, a large number of code signing certificates have been stolen, as software certificates are easily compromised. Therefore, to ensure the security of private keys for code signing certificates, international standards require that, starting June 1, 2016, EV code signing certificate private keys

must be stored on hardware devices with FIPS 140-2 or higher, Common Criteria EAL 4 or higher, or equivalent certification levels. This is a key watershed moment in code signing certificate security standards, marking a new mandatory hardware level for software supply chain security protection. Seven years later (June 1, 2023), this requirement applies to ordinary code signing certificates, mandating that all private key generation, storage, and signing operations for code signing certificates must be performed on certified hardware devices, ensuring that the private key can never leave the hardware device, thus greatly reducing the risk of private key theft. This is the third stage, where there are no more software certificates, only hardware certificates, whether ordinary or EV code signing certificates.

It can be seen that the three stages of code signing development are a process of moving from soft certificates to hard certificates. This not only continuously raises the requirements for trusted identities, but also continuously strengthens the protection of trusted identities, thoroughly upgrading the security foundation of the global software supply chain and fundamentally solving the systemic trust crisis caused by private key leakage.

2. Code signing faces two challenges

Code signing requires a code signing certificate. To protect the private key of this certificate, it must be generated, stored, and used through rigorously certified hardware cryptographic devices. This necessitates that the Certificate Authority (CA) generate the private key and import the certificate into a compliant USB Key after the certificate issued, then deliver the USB Key to the end user from the US or Europe. This process typically takes 10-15 days, which is the first hurdle users encounter: waiting! And it's not just waiting; there are also shipping costs as high as $50!

The second challenge is the ever-shortening validity period of code signing certificates. Currently, it is valid for 3 years, but on March 1, 2026, it will be shortened to one year and 3 months (15 months). This means that from March 2026 onwards, users can only purchase one-year certificates, and they will have to pay for the USB key shipped from the United States every year. They will also have to wait every year to receive the hardware UKey certificate before they can sign the code. What if there are bugs in the software and an update is urgently needed? This is the second challenge that users

encounter: not only do they have to wait, but they have to wait every year!

This trend of continuously shortening the validity period of code signing certificates can also be seen in SSL certificates: the validity period will be shortened to 47 days on March 15, 2029. It is foreseeable that the validity period of code signing certificates will also continue to shorten and will not remain in the one-year period. This is because traditional cryptographic algorithms RSA/ECC/SM2 cannot resist quantum computing attacks, making the code signing mechanism to guarantee the trusted identity of software code no longer effective. The current solution is to continuously shorten the certificate validity period to shorten the attack window, while actively promoting the implementation of digital signatures using post-quantum cryptographic algorithms.

3. ZoTrus perfectly solves two challenges

ZoTrus Technology is also a user of code signing certificates because ZT Browser releases versions regularly, requiring a large amount of code to be digitally signed. Therefore, ZoTrus deeply understands the pain points software developers face regarding code signing. Application security is one of ZoTrus Technology's five planned zero trust + cryptographic technology solutions. After completing the most important website security solution, ZoTrus Technology invested its R&D resources to perfectly solve the two challenges faced by code signing.

The first challenge is waiting for the US CA to ship the USB Key. ZoTrus Technology's solution is to get the US CA to recognize and use USB Keys made in China, eliminating the need for users to wait for shipping. ZoTrus Technology only needs to ship a USB Key with the certificate pre-loaded to the user the first time; thereafter, no more shipping of the USB Key hardware is required, and users can directly use the original USB Key to renew the certificate.

The second challenge is the ever-shortening validity period of certificates. ZoTrus Technology's solution is to provide code signing cloud service. Users don't need to worry about the future validity of their code signing certificates; they only need to purchase the code signing service as needed, and the certificate can be used to sign software code immediately upon issuance. ZoTrus Technology uses

FIPS 140-2 Level 3 certified cryptographic module (HSM) to generate code signing certificate keys and protect signing keys, ensuring security and compliance, and has received strong support and technical cooperation from two top CAs.

This is the application security solution launched by ZoTrus Technology. Users can choose either method to protect their private key security. Both methods do not require waiting for international express delivery and can provide users with fast code signing services, greatly reducing the cost of using code signing.

ZoTrus Code Signing Cloud Service follows the Cloud Signing API standards released by Cloud Signature Consortium. This not only strongly ensures the quality of the cloud signing service but, more importantly, provides users with development capabilities an API interface based on international standards, making it convenient for users to integrate code signing automation service into their code automation management system.

4. Cloud signing services are poised to become the preferred choice for code signing.

Using ZoTrus code signing cloud service eliminates the need to wait for an oversea CA to deliver a USB key certificate. After completing identity validation and certificate issuance, users can immediately use the service to sign software codes. Whether the user purchases a IV, OV, or EV edition, there's no need for tedious hardware UKey management. This not only solves the security issue of signing keys but also addresses the problem of users not being able to obtain certificates immediately. More importantly, it completely frees users from the cumbersome management of hardware UKeys, allowing them to fully enjoy the convenience of cloud services for on-demand digital signing of software code.

ZoTrus code signing cloud service also has two unique technical advantages: First, it does not charge based on the number of signed files, but still charges a fixed annual fee like traditional UKey certificates; second, it does not require uploading the software code to be signed, but adopts advanced signing and code separation technology, only submitting the code HASH value to the cloud signing service system, which not only makes signing fast, but also ensures the security of user code.

Furthermore, in order to address the security threats posed by quantum technology to code signing, ZoTrus Technology has been closely following relevant international standards and will upgrade its cloud signing service to support hybrid PQC algorithm code signing for free as soon as possible. This is a unique advantage that traditional hardware UKey certificates cannot provide.

In conclusion, code signing cloud service will undoubtedly become the preferred choice for code signing, just as users currently prefer other cloud services — they are not only faster but also more cost-effective. ZoTrus Technology plans to provide cloud-based code signing services for China developed operating systems in its next step. ZoTrus look forward to close cooperation with China operating system manufacturers to jointly safeguard the fundamental and kernel security of operating systems using the SM2 algorithm code signing certificates and cloud code signing services. Of course, this also provides global code signing users with more options and better code signing cloud services.

Richard Wang

January 7, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 108 articles in English (more than 148K words)
and 249 articles in Chinese (more than 737K characters in total).