Deep thoughts on "Google no longer trusts Chunghwa Telecom CA"

Google announced in its official security blog on May 30 that Google Chrome version 139 no longer trusts the two root certificates (ePKI and HiPKI) of the Chunghwa Telecom CA and the root certificate of the Hungarian CA- Netlock for SSL certificates issued after July 31st. The author did not want to discuss such an unlucky thing publicly, but this matter did not attract enough attention, which is not a good thing, so the author decided to write an article to talk about this matter. All CAs must be prepared for a feasible disaster recovery response measure, rather than just believing that they will not have problems if they strictly abide by relevant standards. More importantly, all SSL certificate users should also carefully choose SSL certificate providers when purchasing SSL certificates, especially users such as governments and banks that run critical information infrastructure systems. This article will provide a decision-making guide for reference.

1. Many unstable factors in the SSL certificate supply chain

Google wrote in the announcement: "We recommend that affected website operators transition to a new publicly-trusted CA Owner as soon as reasonably possible. To avoid adverse website user impact, action must be completed before the existing certificate(s) expire if expiry is planned to take place after July 31, 2025. " For now, this is what users must and can only do. But when this happens, the biggest victims are SSL certificate users, which is very unfair to them, but also very helpless. In fact, SSL certificate users have better options to avoid such incidents of SSL certificate supply interruptions.

The author does not want to comment on the right and wrong of this matter. I just want to think about the fact that Chunghwa Telecom CA has issued more than 30K valid SSL certificates for Taiwan's government websites and bank websites. These users have to apply for new SSL certificates from other CAs and re-deploy SSL certificates on tens of thousands of servers. This has brought great pain to these users, and I feel like I have experienced it myself. I believe that all bank IT engineers still

remember the difficulties of working late into the night to redeploy DigiCert SSL certificates when Symantec SSL certificates were distrusted in 2017. That incident affected more than two million websites around the world. Almost all bank websites and many government websites around the world deployed Symantec SSL certificates, which are VeriSign brand SSL certificates that Symantec spent $1.28 billion to acquire. These security incidents that have occurred have caused me to think deeply about the security issues of the SSL certificate supply chain.

Don’t think this is a low-probability event and ignore it. Last November, Google decided to distrust Entrust CA including its subsidiary AffirmTrust, which was once the world’s second largest CA. This also forced nearly 600K users around the world, including many banks and government agencies, to re-apply for and re-install SSL certificates from other CAs that took over their users. The two cases of distrust were only six months apart, and no one knows which unlucky CA will be the next to be distrusted. Therefore, global CAs and all SSL certificate users should attach great importance to and think about the security issue of the SSL certificate supply chain.

The instability of SSL certificate supply is caused not only by technical factors, but also by geopolitics. After the Russia-Ukraine conflict three years ago, the SSL certificates of almost all Russian government and bank websites were revoked and cut off. This is of course a rare extreme security incident, but the result is also a problem with the SSL certificate supply chain.

SSL certificate is an important IT product, a cryptographic product, and a product that can be supplied by multiple suppliers. Since it is a product, there are supply chain security issues. As a very important and indispensable security product, the supply chain of SSL certificate has many uncertain factors. If the original supplier is unable to supply, it is difficult for users to immediately choose a new supplier to make up for it. Because once the SSL certificate is revoked, the website will immediately be inaccessible. Even if the original SSL certificate is not revoked, but it is cut off, you need to change supplier and apply for an SSL certificate from the new supplier. After obtaining the certificate, you need to redeploy it to the Web server. One website can still handle it, but what about one hundred or one thousand websites? These are issues that website administrators must consider, especially large organizations with many website systems, because all business systems require HTTPS encryption services that cannot be interrupted for a moment.

Some readers may say that you must choose a big brand. Symantec was the world's number one brand at that time (taking over VeriSign / GeoTrust / Thawte, etc.), but it was also "taken down in one fell swoop". Entrust was once the world's second largest CA, a CA that was only 4 years later than VeriSign, but it was also "taken down in one fell swoop". Choosing the number one brand may not be reliable, what should innocent users do? Is there a better choice? Even the world's number one CA cannot escape the fate of being distrusted by browsers. Should all CAs in the world be prepared for emergency disaster preparation?

2. SSL certificate automation management can greatly reduce the impact of unstable SSL certificate supply

In order to ensure the security of HTTPS encryption, the international standard has released a timetable on May 16 to gradually shorten the validity period of SSL certificates, which will be shortened to 200 days on March 15 next year, 100 days on March 15, 2027, and 47 days on March 15, 2029. In other words, from now on, users need to consider one more thing when purchasing SSL certificates: choose a supplier that can provide SSL certificate automatic management solutions, because manual application and deployment of SSL certificates will soon become impossible.

Currently, more than 80% of the global SSL certificates have been managed automatically, and major cloud service providers and CAs have provided SSL certificate automatic management services (ACME). Imagine that if users of Chunghwa Telecom CA have implemented SSL certificate automatic management, they only need to modify the service URL of the ACME service provider on the server to continue to enjoy the SSL certificate automatic service. These users will be least affected, and this is the benefit of implementing SSL certificate automatic management.

In other words, SSL certificate automatic management can greatly reduce the impact of unstable SSL certificate supply. If an SSL certificate provider is unable to supply or deliberately stops supplying, users who manually apply for and deploy SSL certificates will suffer the most, while users who have already achieved SSL certificate automatic management will be much more relaxed and less affected. This is also one of the reasons Google emphasized when it proposed to promote the automation of 90-

day validity SSL certificates in March 2023: to improve agility and enhance resilience.

As an SSL certificate user, don't just care about the brand of the certificate, because choosing a big brand may also cause supply interruption. What users should care about is whether the SSL certificate provider can provide SSL certificate automatic management solutions and step up the implementation of SSL certificate automatic management. This can not only greatly reduce the burden of SSL certificate management, but more importantly, it can greatly reduce the difficulty of redeploying a new certificate if the SSL certificate deployed on your website is helplessly interrupted, because no one can guarantee when the SSL certificate they are using will be interrupted. The supply chain of SSL certificates is very fragile! Actively embracing SSL certificate automation is a wise choice, and it has become a necessary technical route.

3. Only by realizing automatic management of SSL certificates and multi-channel issuance can we truly solve the problem of unstable SSL certificate supply chain.

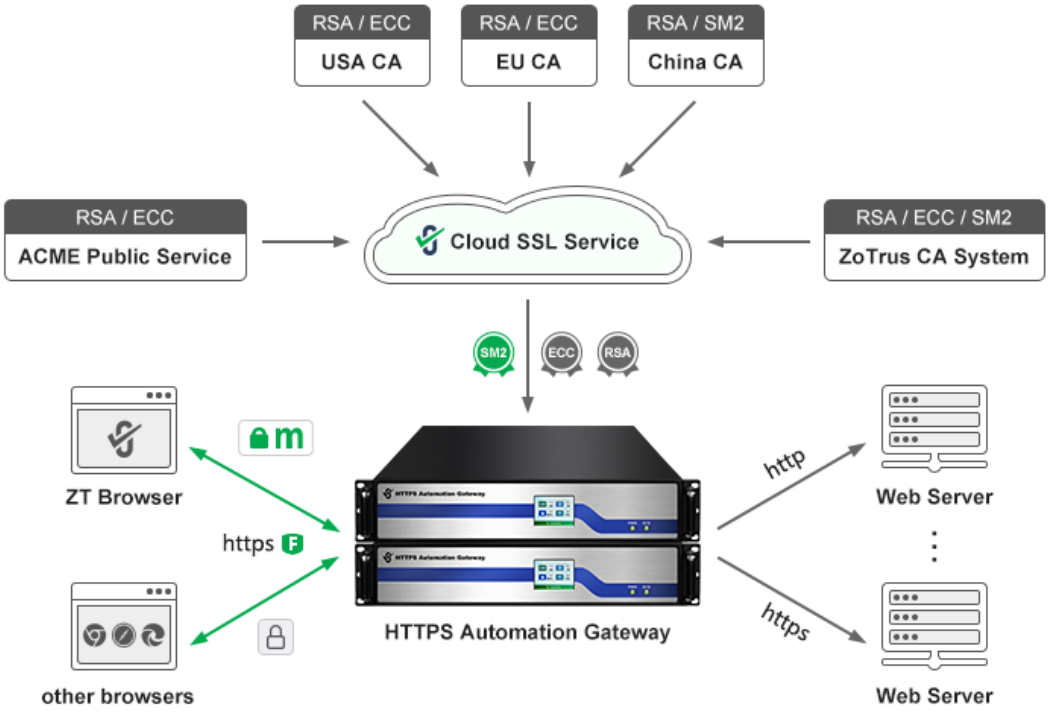
Automatic management of SSL certificates is very important and is the only way to go. When the SSL certificate provider is out of supply, users only need to switch to other SSL certificate providers that can provide automatic management of SSL certificates, but they need to manually modify the ACME service URL and other parameters of each website, restart the ACME service and restart the Web server. This is still a big challenge for government platforms, cloud platforms and large organizations that have hundreds or thousands of websites to manage, and it may cause a short interruption to the running business. What to do?

In other words, automation alone is not enough to ensure the uninterrupted and reliable operation of the website system, especially for large organizations that have many website systems to manage, and they also need solutions that can automatically switch to other SSL certificate issuance channels. Only automatic certificate management will become semi-automatic due to the fragility of the SSL certificate supply chain. The globally accepted SSL certificate automatic management solutions are actually only semi-automatic. It is still possible to be interrupted that need the manual intervention due to the fragility of SSL certificate supply. The best solution is multi-channel certificate issuance plus

automatic channel switching plus automatic certificate management, which means that there are multiple SSL certificate suppliers that can automatically issue SSL certificates for user websites, and there is an automatic switching issuance channel system, which completely solves the problem of unstable SSL certificate supply chain.

For Chinese users, it is not only necessary to solve the problem of automatic management of dual-algorithm SSL certificates, but also to add multi-channel issuance and automatic switching of issuance channels, and to solve the problem that the Web server does not support the SM2 algorithm. In particular, what if the Web server does not allow the installation of ACME client software? These are the technical problems encountered by Chinese websites, especially government websites, bank websites, etc., which have many website systems that need to deploy SM2 SSL certificates and complete SM2 supported transformation. Is there a better solution?

ZoTrus Technology innovative solution is to separate the HTTPS encryption task originally undertaken by the Web server, and have the ZoTrus HTTPS Automation Gateway take on the automatic certificate management work. The original Web server does not need to be modified, and the dual-algorithm (ECC/SM2) SSL certificates for HTTPS encryption are managed by ZoTrus Gateway that it automatically connecting to the ZoTrus Cloud SSL Service System for automatic issuance and automatic deployment. The ZoTrus Cloud SSL Service System has been connected to several international CAs and China CAs, and it also connects with the international ACME public service system and the ZoTrus CA system, to automatically switch certificate issuance channels to provide dual-algorithm SSL certificates for user websites. Users do not need to manually apply for and deploy SSL certificates, nor do they need to worry about a certain SSL certificate provider being unable to issue SSL certificates or being out of supply, ensuring the uninterrupted and reliable operation of HTTPS encryption of user website systems.



4. The SSL certificate supply chain is stable, ensuring continuous Internet services.

SSL certificates, like all products, have supply chain security issues. In the current unstable international environment, this issue must be given high priority. Fortunately, SSL certificates are digital products, and there are already automatic management solutions for SSL certificates. With multi-channel issuance and multi-channel automatic switching, only by implementing these measures can we thoroughly resolve the instability issues in the SSL certificate supply chain. All SSL certificate users should correctly choose automatic SSL certificate providers to offer reliable automatic certificate management solutions for their business systems, thereby ensuring the uninterrupted secure operation of HTTPS encryption in business systems, maintaining continuous Internet services.

Richard Wang

July 7, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 95 articles in English (more than 129K words) and 218 articles in Chinese (more than 648K characters in total).