How long should the SM2 SSL certificate validity period?

Some users reported that after the ZT Browser was upgraded to version 114, the original 97 version normally displayed the SM2 encryption **m** icon for Bank of China online banking website was displayed as "Not secure". This article talks about this issue, this issue has nothing to do with the 114 version. This is a technical issue about how long the validity period of the SM2 SSL certificate should be. The author thinks that it is necessary to talk about the history and future of this issue, so as to not only answer users' questions, but also inspire discussions on the validity period of SM2 SSL certificates in the formulation of the SM2 SSL certificate GM/T standard, which will help the industry to reach a consensus.

As shown in the left picture below, this is the UI displayed by ZT Browser before the upgrade, and the right picture is the UI displayed after upgrading to the Chromium 114, from the green address bar to "Not secure". In fact, this has nothing to do with the Chromium version upgrade, but it is the reason we have changed with the UI display rules. This change from the normal display to the "Not secure" display is due to the fact that this SM2 SSL certificate is valid for 3 years and expires on July 12, 2025, and this version upgrade of ZT Browser has revised the verification of the validity period of the SM2 SSL certificate. According to the rules, the validity period of the SM2 SSL certificate was changed from allowing more than 1 year period to less than 13 months following the international standard. In this way, everyone will see the "ERR_CERT_VALIDITY_TOO_LONG" security warning in the new version of ZT Browser. This is Chromium's default "Not secure" rule, but the original version 97 has made special treatment when dealing with SM2 SSL certificates, and the upgraded version 114 no longer retains this special treatment.

So, why does the international standard determine the validity period of SSL certificates as no more than 13 months? Why did Google start pushing to shorten the certificate validity period to 90 days? This is the focus of this article.

When the author started reselling GeoTrust SSL certificates in 2004, SSL certificates could be issued with a validity period of 10 years. Later, I don't remember when it started that it changed to validity period of 5 years, and then it was:

- From April 1, 2015, only 3 years (39 months) SSL certificates period can be issued.
- From March 1, 2018, only 2 years (27 months) SSL certificates period can be issued.
- From September 1, 2020, only 1 year (13 months) SSL certificates period can be issued.

On March 3, 2023, Google announced that it will promote to shorten the validity period of SSL certificates to 90 days. The author expects that the official effective time will be some day in the second half of 2024. As you can see, it took 3 years to change from 3 years periods to 2 years periods, 2 and a half years to change from 2 years periods to 1 year period, and it is estimated to take 4 years to change from 1 year period to three months (90 days). After 90 days, it will definitely continue to be shortened to 96 hours (4 days) on a certain day (short-term certificate).

Why are international standards constantly shortening the validity period of SSL certificates? This is related to the use scenarios of SSL certificates and the continuous improvement of global computing power. The public key of the SSL certificate is publicly visible. Anyone or organization may use its powerful computing power to try to crack the encryption algorithm of the SSL certificate and deduce the private key of the certificate, so as to achieve the purpose of deciphering HTTPS encrypted traffic. The shorter the validity period, the shorter the time for the attacker to brute force cracking, and the more secure the certificate key. For this reason, although users hope to get certificates with a long validity period to simplify the management of SSL certificates, in order to ensure the security of certificate keys, CA/Browser Forum are still pushing to shorten the validity period of SSL certificates, because the global computing power is growing, especially cloud computing and quantum computing are developing very rapidly.

Continuously shortening the validity period of SSL certificates has two main benefits:

(1) Achieve technology upgrades faster - a longer life cycle means it takes longer to effectively drive

technology upgrades.

A real example is the certificate signing algorithm upgrade from SHA1 to SHA2. If the certificates are valid for 5 or even 10 years, it may take years to replace all the old certificates unless a whole bunch of certificates are revoked, and users are forced to reissue. The SHA1 upgrade took 3 years, which creates various potential risks.

(2) Shorter domain validation intervals - how long should information used to validate identities remain trusted? The longer the interval, the greater the risk. One Google specialist has said that under ideal circumstances, domain control should be revalidated every six hours.

If the validity period of the SSL certificate is changed from the current 1 year to 90 days, the traditional manual application and deployment of SSL certificates has become impossible, and automatic management of SSL certificates must be implemented to automatically apply for and deploy SSL certificates. Google's promotion of shortening the validity period of SSL certificates to 90 days is also intended to promote the automatic SSL certificate management. Google Chrome trusted root program policy page lists six benefits of implementing automatic certificate management:

(1) promote ecosystem agility,
(2) increase resiliency for CA owners and website administrators alike,
(3) help website owners address scale and complexity challenges related to certificate issuance,
(4) drive innovation through ongoing enhancements and support from an open community,
(5) ease the transition to quantum-resistant algorithms, and
(6) better position the Web PKI ecosystem to manage risk.

In fact, as early as 2015, Google initiated a Short-Lived Certificate (valid for 4 days) ballot in the CA/browser Forum and was rejected. However, the ballot to deprecate OCSP recently initiated by Google, Microsoft and Sectigo has been passed. One of them is that there can be no CRL and OCSP URL in Short-Lived Certificate. This is also one of the advantages of Short-Lived Certificate, including:

(1) The browser no longer needs to spend time querying the CRL/OCSP service provided by the CA, which may have a very slow access speed, then the browser can implement https encryption and display the padlock faster, display the website content faster, and provide a better user experience.
(2) The certificate expires within 4 days, which limits the use time after the attacker obtains the

private key of the certificate and is more conducive to protecting the security of the website.

(3) The CRL/OCSP query traffic of the global Internet is greatly reduced, which is one of the reasons why the international standard abandons the OCSP, not only for protecting user privacy.

The above mentioned so many benefits of shortening the validity period of SSL certificates. Of course, this is not good news for website administrators. Website administrators want to save time and trouble. Of course, they hope that the certificates they get will be valid as long as possible. But for website security, the shorter the validity period of the certificate, the safer it is, especially in the post-quantum era. This requires a balance point, you can also see this balance from the shortened timeline of the validity period of SSL certificates, it is a process of slowly and continuously shortening. What all webmasters should do is to make full preparations for the arrival of the 90-day validity period as soon as possible, which is why ZoTrus Technology has invested a lot of research and development efforts to develop the three solutions for SM2 HTTPS automation management, to make technical preparations before the 90 days validity period coming, and provide customers with three optional solutions, so that customers can be less trouble and less worry than current installing the certificate once a year. Only in this way can customers accept the ever-shortening certificate validity period, to achieve both convenience and security.

So, how long should the SM2 SSL certificate validity period? ZT Browser displayed a "Not secure" warning for the SM2 SSL certificate that is more than one year period, which is our answer. ZT Browser will refer to international standards and adopt the same processing method for SM2 SSL certificates that do not meet the requirements of international standards for the validity period of SSL certificate, so as to ensure the security of SM2 https encryption and the security of websites deployed with SM2 SSL certificates.

Finally, let’s talk about the validity period of the SSL certificate used in the intranet. As mentioned earlier, the continuous shortening of the validity period of the SSL certificate is a process of balancing key security and convenience. And considering that the intranet is isolated from the Internet, it is difficult to realize automatic certificate management. Therefore, the author believes that the SSL certificate used for intranet HTTPS encryption can appropriately relax the validity period of the certificate, because the intranet is not a public network, and the possibility of its public key certificate

encountering brute force is greatly reduced. Properly relaxing the certificate validity period can ensure that the key is relatively security, and it is convenient to deploy and use the intranet SSL certificate, so that the intranet originally transmitted in plain text can realize more secure https encryption of intranet traffic, thereby ensuring the security of intranet traffic.

Richard Wang

August 8, 20233
In Shenzhen, China