Google wants to "Move together" or "Remove" other CAs ?

Google released the latest policies related to the Chromium Root Program on March 3, and released future plans in its "Moving Forward, Together" section, the most important of which is:

In a future policy update or CA/Browser Forum Ballot Proposal, we intend to introduce:

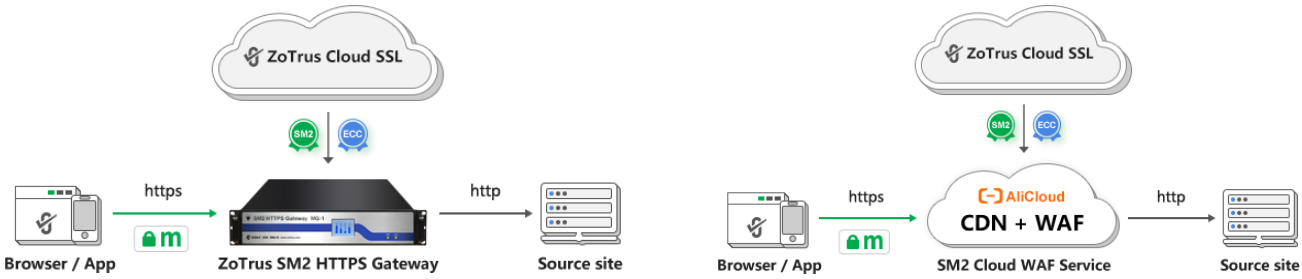
- ***a maximum validity period for subordinate CAs.*** *Much like how introducing a term limit for root CAs will allow the ecosystem to take advantage of continuous improvement efforts made by the Web PKI community, the same is true for subordinate CAs. Promoting agility in the ecosystem with shorter subordinate CA lifetimes will encourage more robust operational practices, reduce ecosystem reliance on specific subordinate CA certificates that might represent single points of failure, and discourage potentially harmful practices like key-pinning. Currently, our proposed maximum subordinate CA certificate validity is three (3) years.*
- ***a reduction of TLS server authentication subscriber certificate maximum validity from 398 days to 90 days.*** *Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on "broken" revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.*

The validity period of the SSL certificate has been reduced from the previous 10 years and 5 years to 3 years, 2 years, and then to 1 year (September 1, 2020), that is, within 3 years, the validity period will be reduced from 1 year to 3 months. Sectigo said in the webinar on March 7 that it is expected to be implemented within this year, which is definitely a blockbuster! Are global users ready to apply for SSL certificates that are only valid for 90 days? The answer is no!

The penetration rate of SSL certificates in Chinese websites is very low (less than 20%). On the one hand, it does not pay attention to the encryption and protection of confidential information on websites. On the other hand, it is very troublesome to apply for and install SSL certificates. Now, every 90 days, it is necessary to re-apply for a new certificate and reinstall the certificate. This is simply killing the web master! This change will definitely further discourage users' enthusiasm for deploying SSL certificates and may cause a large number of websites to no longer bother to apply for and install SSL certificates after the SSL certificate expires! How to do? CA industry, network security industry and cloud service providers must come up with countermeasures for this!

In fact, when Google released this policy plan, it has pointed out the direction for users, that is, to use the ACME client as soon as possible to realize automatic certificate management. Only in this way can tedious manual application, manual deployment and manual renewal of SSL certificates be avoided. However, the ACME service does not support the SM2 SSL certificate. Fortunately, ZoTrus Technology has launched the SM2 ACME service on January 6, including the SM2 ACME Client software - SM2cerBot and the SM2 ACME Service System, which can help users automatically apply for and deploy dual-algorithm dual-SSL certificates (ECC SSL certificate and SM2 SSL certificate). But unfortunately, since the original Nginx web server must be uninstalled while installing the SM2 ACME Client software, the modified Nginx system that supports the SM2 algorithm must be reinstalled, so that the web server can support the SM2 algorithm and the SM2 SSL certificate, but this is very harmful to the user's business system, so the author thinks that ACME is not the solution that the user needs, at least in China!

How to do? ZoTrus Technology has provided two feasible solutions: deploying SM2 HTTPS Gateway or enabling SM2 Cloud WAF Service to realize zero reconstruction of existing web servers, and automatically configure dual-algorithm and dual-SSL certificates, which is not afraid of Google or international standards requiring only 90 days period allowed. Within 90 days, the Gateway or Cloud service will automatically connect with the ZoTrus Cloud SSL system to automatically apply for a new SSL certificate and automatically deploy it. With the automatic deployment solution of zero reconstruction, even if the validity period of the certificate is shortened to 1 day in the future, it can be properly handled!



The author has emphasized the importance of automatic deployment of SSL certificates in several blog posts. Now it seems that this automatic deployment is no longer a solution that needs to be promoted, but a solution that must be implemented! This deserves great attention from all webmasters and cloud service providers, as well as all parties related to SSL certificates. All cloud service providers must provide automated certificate application and deployment services as soon as possible, and each website must decide which solution to use as soon as possible to solve this upcoming "revolution", because manually applying for certificates and deploying certificates every 90 days has become inoperable, the forgetting to renew the certificate events definitely happen, which will definitely affect the normal operation of the business system.

The above are all visible problems, but there is another problem that you may not see, that is, the impact of this plan on the CA business may be greater than the impact on end users. Just imagine, now the market share of supporting ACME automatic deployment of free 90-day SSL certificate is over 80%. If the paid SSL certificate must also be valid for 90 days, will there still be end users who are willing to spend money to buy a paid SSL certificate? If no one like to buy SSL certificate, how to make money for CA? isn't this going to kill CA? where is it to "moving forward, together"? Google really does tell stories! The 90-day free SSL certificates led by Google and Mozilla have occupied more than 60% of the global market share, and Google's plan this time to shorten the validity period of SSL certificates will further accelerate their market share. The prospect for CA operators is worrisome, and they must think carefully about which direction to go.

The author’s advice at many meetings is that the CA operators must change its mind and change the traditional concept of selling SSL certificates, because what end users need is https encryption, not SSL certificates! The only solution to the upcoming 90-day certificate validity period policy is to provide end users with an automatic certificate management solution to deploy SSL certificates, not to

sell SSL certificates! ZoTrus Technology began to explore this solution a year ago and has found the only feasible solution. Welcome to cooperate to deal with the "90-day Certificate Revolution".

Richard Wang

March 14, 2023
In Shenzhen, China