A Final Statement of the WoSign Incidents

(Sept. 23rd, 2016)

WoSign received an email from Mozilla for 3 incidents on August 24th 2016. Over a month, there has been many emails asking for clarification and WoSign has released two reports (Preliminary Report and Final Report) with detailed information of those incidents and some others that have been requested as indicated in the Mozilla wiki page.

WoSign recognizes its mistakes but also thinks the issues have been clarified. WoSign is willing to accept any fair and reasonable sanctions, in case this happen, but the sanctions must ensure the current subscribers' benefit.

And WoSign would like to share some more information for consideration.

1. WoSign continues to improve and progress.

Pursuant to the problem has been found in 2015, WoSign issued **101,485** SSL certificates, of those, only 33 certificates had serious problem, so this is the **0.03%** of the total issued certificates; and there were 1,647 mis-issued certificates totally, accounting for **1.623%**.

In 2016, from Jan 1st to July 4th, WoSign issued **94,073** SSL certificates with no serious problems, with only 12 mis-issued certificates, which is the **0.013%** of the total issuance at that time.

From July 5th all certificates after have been submitted to the CT log servers, about **43,000** certificates, and there´s no problem with those certificates, the error rate is **0.000%**.

So, the mis-issued certificate rate is from **1.623%** to **0.013%** to the current **0.000%**, therefore you can see that WoSign has been constantly refined, tuned and improved their systems.

2. Why were there so many incidents with such a high error rate in 2015?

WoSign considers there were two reasons:

(1) Rapid growth in subscribers: In January 1st 2015, WoSign opened to worldwide users for a 3-year period with 100 multi-domain support free SSL certificate, at the moment no any other CA provide so big benefit, and was greatly welcomed by customers around the world. The daily orders surged in just 3 months' time covering more than 180 countries and regions. Issuing few certificates per day is quite different from issuing thousands certificates per day, it is thousands of times growth including some malicious attacks order, so the system security and reliability is a great challenge. One of the incidents is caused by a large number of concurrent requests to database.

(2) Not enough research to international standards: Due to foreign companies to China's technology blockade, WoSign decided to research and develop all systems by ourselves in 2009, including BUY system (Online certificate store), CMS (Certificate Management System, internal work flow), PKI/CA (Certificate issuing system), CRL/OCSP (Certificate revocation query system) and TSA (time stamp system). So many complex systems that must comply with all relevant international standards, this was a big challenge for the R&D team, and due to time to market reason, we have not thoroughly studied all the criteria, resulting in a problem of the system does not meet some international standards and have some bugs.

3. Why, after July 5th 2016 that submit all certificates to CT Log server, there is no longer one mistake?

There are two reasons:

(1) System has been emerging issues in 2015 and ongoing timely repair and improvement, in addition to 2016 SHA-1 to SHA-2 transition period there have been a small problem, but essentially no any other problems, all systems have proved stable and reliable. Currently CRL/OCSP queries have up to 200 billion times monthly.

(2) WoSign believes that the Certificate Transparency is a very good solution for self-discipline that force employees to attach great importance to product quality control, and for external oversight mechanism that let the third party supervise the CA's activity.
WoSign is the first CA that volunteer to post all issued SSL Certificates to Google CT log server initiatively. Our aim is to let the worldwide users trust WoSign SSL certificates, and hope to drive the global CAs to be open and transparent publishing all issued certificates to CT log server, making worldwide users, browser vendors and related stakeholder to take an overall supervision, this will benefit the global Internet security.

4. With regard to the issue related to the use of China encryption algorithm SM2 to issue SSL certificate

WoSign agrees that this is a violation of the BRs (only three US NIST P-256, P-384, or P-521 curves can be used for elliptic curve keys in certs), but being a Chinese licensed CA, we must abide by local laws and regulations, we must actively cooperate with domestic browsers to test the SSL certificate using SM2 algorithm issued by a global trusted root in the real Internet, not intranet.
WoSign, as a member of CAB Forum, will spare no effort to continue to promote China encryption algorithm SM2 to become the international standard allowed algorithm.

Finally, through over a year and 9 months a high amount of certificates has been issued, our systems have become more secure and reliable, our customer service team and validation teams have been more mature, we have the ability and determination to provide better products and better service for users worldwide, it is our commitment to global users.

Thanks.

WoSign CA Limited

