

31 March, 2016

Report of Independent Accountants

To the Management of WoSign CA Limited:

We have examined the assertion by the management of WoSign CA Limited (“WoSign”) that in providing its SSL Certification Authority (“CA”) services at Shenzhen, China, during the period 1 January, 2015 through 31 December, 2015, WoSign has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly collected, authenticated (for the registration activities performed by WoSign) and verified;
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
- Maintained effective controls to provide reasonable assurance that:
 - Logical and physical access to CA systems and data was restricted to authorized individuals;
 - The continuity of key and certificate management operations was maintained;
 - CA system development, maintenance and operations were properly authorized and performed to maintain CA systems’ integrity; and
 - Met the Network and Certificate system Security Requirements set forth by the CA/Browser Forum

for the Root CA: “**Certification Authority of WoSign**”, “**CA 沃通根证书**”, “**CA WoSign ECC Root**” and “**Certification Authority of WoSign G2**”, based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0](#).

WoSign’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of WoSign’s key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems’ integrity; (2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, WoSign’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on

our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

The relative effectiveness and significance of specific controls at WoSign and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

In our opinion, for the period 1 January, 2015 through 31 December, 2015, WoSign management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0](#).

Emphasis of Matters

Without modifying our conclusion, we draw attention to below matters:

1. Duplication in certificate serial number for a total of three hundred and ninety-two (392) SSL subscriber certificates issued by WoSign during the period from 9 April 2015 to 14 April 2015 was reported. We understand that remediation action was taken by WoSign to revoke those certificates in a timely manner. Incident investigation with root cause analysis was conducted and relevant result was documented in relevant incident report. Follow up action was also conducted to prevent the recurrence of the incident.
2. Principle 2, Criterion 2.1 of the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0](#) requires that, with respect to the validity period of SSL subscriber certificates, the CA maintains controls to provide reasonable assurance that the validity period of SSL certificates issued meet with the SHA-1 validity period requirement as set out in CA/Browser Forum Baseline Requirements Version 1.3.3 - Section 7.1.3.

During the course of our examination, we noted that a total of one thousand one hundred and thirty-two (1,132) SSL subscriber certificates utilizing the SHA - 1 algorithm were issued by WoSign, during the period from 16 January 2015 to 5 March 2015, which did not meet with the SHA-1 validity period requirement as set out in CA/Browser Forum Baseline Requirements Version 1.3.3 - Section 7.1.3. We understand that WoSign has established procedures and implemented controls to ensure that the aforementioned SSL subscriber certificates would be revoked on or before 31 December 2016.

Our conclusion is not modified in respect of the above matters.

This report does not include any representation as to the quality of WoSign's certificate services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0](#), nor the suitability of any of WoSign's services for any customer's intended purpose.



Ernst & Young
62/F One Island East
18 Westlands Road
Island East
Hong Kong

安永會計師事務所
香港港島東華蘭路 18 號
港島東中心 62 樓

Tel 電話: +852 2846 9888
Fax 傳真: +852 2868 4432
ey.com

WoSign's use of the WebTrust for Certification Authorities – Baseline Requirements Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Yours faithfully,

A handwritten signature in black ink that reads 'Ernst & Young' in a cursive, stylized font.



WoSign CA Limited

502#, Block A, Technology Building 2, No. 1057, Nanhai Blvd.

Nanshan District, Shenzhen 518067, China

Tel: +86-755-8600 8688

Fax: +86-755-3397 5112

**Assertion of Management of WoSign CA Limited Regarding
its Disclosure of its Certificate Practices and its Controls Over
its SSL Certificate Authority Services
During the Period 1 January, 2015 through 31 December, 2015**

31 March, 2016

The management of WoSign CA Limited (“WoSign”) has assessed the disclosure of its certificate practices and its controls over its SSL Certification Authority (“CA”) services located at Shenzhen, China for the period 1 January, 2015 to 31 December, 2015. Based on that assessment, in WoSign Management’s opinion, in providing its SSL – CA services at Shenzhen, China, during the period 1 January, 2015 through 31 December, 2015, WoSign has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly collected, authenticated (for the registration activities performed by WoSign) and verified;
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles;
- Maintained effective controls to provide reasonable assurance that:
 - Logical and physical access to CA systems and data was restricted to authorized individuals;
 - The continuity of key and certificate management operations was maintained;
 - CA system development, maintenance and operations were properly authorized and performed to maintain CA systems integrity; and
 - Met the Network and Certificate system Security Requirements set forth by the CA/Browser Forum



WoSign CA Limited

502#, Block A, Technology Building 2, No. 1057, Nantai Blvd.

Nanshan District, Shenzhen 518067, China

Tel: +86-755-8600 8688

Fax: +86-755-3397 5112

for the Root CA: “**Certification Authority of WoSign**”, “CA 沃通根证书”, “**CA WoSign ECC Root**” and “**Certification Authority of WoSign G2**”, in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0](#).

Yours faithfully,

For and on behalf of
WOSIGN CA LIMITED

.....
Authorized Signature(s)

Mr. Richard Wang
Chief Executive Officer
WoSign CA Limited

