Ernst & Young
22/F, CITIC Tower
1 Tim Mei Avenue
Central, Hong Kong

安永會計師事務所
香港中環添美道 1 號
中信大廈 22 樓

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

Report of Independent Accountants

To the Management of
China Internet Network Information Centre – Certification Authority Centre:

We have examined the assertion by the management of China Internet Network Information Centre – Certification Authority Centre (CNNIC-CA) that in providing its Certification Authority (CA) services known as CNNIC SSL Certification Service in Beijing, China for the Root CA: CNNIC Root, and the Subordinate Root CA: CNNIC SSL, CNNIC SHA 256 SSL and CNNIC DQ SSL, during the period from November 2, 2015 to February 29, 2016, CNNIC-CA has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
  - Certification Practice Statement, and
  - Certificate Policy

  and provided services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - CNNIC-CA's Certification Practice Statement was consistent with its Certificate Policy
  - CNNIC-CA provided its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages was established and protected through their life cycles;
  - the Subscriber information was properly authenticated (for the registration activities performed by CNNIC-CA); and
  - subordinate CA certificate requests were accurate, authenticated, and approved

- 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; and
  - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

for the Root CA: CNNIC Root, and the Subordinate Root CA: CNNIC SSL, CNNIC SHA 256 SSL and CNNIC DQ SSL, based on the Trust Services Principle and Criteria for Certification Authorities, Version 2.0.

CNNIC-CA'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 CNNIC-CA's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, 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 key and 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.

EY 安永
Building a better working world

The relative effectiveness and significance of specific controls at CNNIC-CA 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.

Because of the nature and inherent limitations of controls, CNNIC-CA'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.

In our opinion, for the period November 2, 2015 to February 29, 2016, CNNIC-CA management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the Trust Services Principle and Criteria for Certification Authorities, Version 2.0.

The WebTrust seal of assurance for certification authorities on CNNIC-CA's Web site 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.

This report does not include any representation as to the quality of CNNIC-CA's services beyond those covered by the Trust Services Principle and Criteria for Certification Authorities, Version 2.0, criteria or the suitability of any of CNNIC-CA's services for any customer's intended purpose.

Ernst & Young
April 5, 2016

Assertion by Management of China Internet Network Information Centre – Certification Authority Centre Regarding Its Disclosure of Its Business Practices and Its Controls Over Its Certification Authority Operations For the Period from November 2, 2015 through February 29, 2016

April 5, 2016

China Internet Network Information Centre – Certification Authority Centre (CNNIC-CA) operates a Certification Authority (CA) service known as CNNIC SSL Certificate Service in Beijing, China for the Root CA: CNNIC Root, and the Subordinate Root CA: CNNIC SSL, CNNIC SHA 256 SSL and CNNIC DQ SSL, and provides the following certification authority activities:

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation, and
- Certificate Status Information Processing

Management of CNNIC-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in CNNIC-CA's Certificate Practice Statement, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to CNNIC-CA's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of CNNIC-CA has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in CNNIC-CA Management's opinion, in providing its CA services known as CNNIC SSL Certificate Services in Beijing, China for the period November 2, 2015 to February 29, 2016 CNNIC has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
  - Certification Practice Statement, and
  - Certificate Policy

  and provided services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that
  - CNNIC-CA's Certification Practice Statement was consistent with its Certificate Policy
  - CNNIC-CA provided its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages was established and protected through their life cycles;
  - the Subscriber information was properly authenticated (for the registration activities performed by CNNIC-CA); and
  - subordinate CA certificate requests were accurate, authenticated, and approved

- 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; and
  - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

for the Root CA: CNNIC Root, and the Subordinate Root CA: CNNIC SSL, CNNIC SHA 256 SSL and CNNIC DQ SSL, in accordance with on the Trust Services Principle and Criteria for Certification Authorities, Version 2.0 including the following:

CA Business Practices Disclosure

CA Business Practices Management
- Certificate Policy Management
- Certification Practice Statement Management

Service Integrity

CA Key Life Cycle Management Controls
- CA Key Generation
- CA Key Storage, Backup and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- CA Key Escrow

Subscriber Key Life Cycle Management Controls
- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Life Cycle Management

Certificate Life Cycle Management Controls
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

中国互联网络信息中心
China Internet Network Information Center

Name: 

CNNIC CA