KISA
Korea Internet & Security Agency

IT Venture Tower, 135 Jungdae-ro,
Songpa-gu, Seoul, Korea, 138-950

Assertion by Management of Korea Internet & Security Agency ("KISA") Regarding its Disclosure of its Business Practices and its Controls over its Certification Authority Operations and its SSL Certification Authority during the period from 1 January 2016 through 31 December 2016

Korea Internet & Security Agency as a Certification Authority (CA) Known as KISA provides the following certification authority services through Root Certification Authority (KISA RootCA1 and KISA RootCA4) and provides SSL Certification Authority services through Root Certification Authority(KISA RootCA1 and RootCA4) ;

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation

KISA is responsible for the management assertion of the KISA operation. Management of KISA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure at http://rootca.or.kr/kor/down/cps16.pdf , service integrity (including key and certificate life cycle management), 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 KISA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

KISA has assessed the controls over its CA operations. Based on that assessment, in KISA Management's opinion, in providing its Certification Authority services (KISA RootCA1 and KISA RootCA4) at http://www.rootca.or.kr/ , during the period 1 January 2016 through 31 December 2016

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement, version 1.0, dated May 2016, as published on the website of KISA and provided its services in accordance with its disclosed practices.

- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - subordinate CA certificate requests were accurate, authenticated, and approved
  - 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 KISA, in accordance with the WebTrust for Certification Authorities version 2.0 including following;

CA Business Practice Disclosure
Certification Practice Statement

CA Business Practice 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

Certificate Life Cycle Management Controls
Certificate Renewal
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls
Subordinate CA Certificate Life Cycle Management

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

KISA also has assessed the controls over its CA-SSL operations. Based on that assessment, in KISA Management's opinion, in providing its SSL Certification Authority services (KISA RootCA1 and KISA RootCA4) at http://www.rootca.or.kr/

- disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines

- maintained effective controls to provide reasonable assurance that
  - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
  - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - 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.
  - CA's network and certification systems security were properly managed.

in accordance with the WebTrust Principle and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security version 2.0;

With the KISA RootCA1 and KISA RootCA4 hierarchy, KISA does not operate an OCSP responder to serve status of information on the subordinate CAs. The rationale for this decision is that the inception of Digital Signature Certificate Profile (KCAC.TS.CERTPROF), predates the effective date of the Baseline Requirements by three years. In the environment, status information is made available by means of Authority Revocation Lists which mean CRLs for subordinate CAs.

Director, Korea Certification Authority Center, JongHyun Baek
Korea Internet & Security Agency,
13 April, 2017

Deloitte.

Deloitte Anjin LLC
9Fl., One IFC,
10, Gukjegeumyung-ro,
Youngdeungpo-gu, Seoul
150-945, Korea

Tel: +82 (2) 6676 1000
Fax: +82 (2) 6674 2114
www.deloitteanjin.co.kr

Independent Practitioner Report

To the management of Korea Internet & Security Agency ("KISA");

We have examined KISA management's assertion that for its Certification Authority ("CA") services, as a Root CA ("KISA RootCA 1 and KISA RootCA 4"), in Korea during the period 1 January through 31 December 2016, KISA has:

- disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control practices in its certification practice statement, version 1.0, dated May 2016, as published on the website of KISA and provided its services in accordance with its disclosed practices.
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - subordinate CA certificate requests were accurate, authenticated, and approved
  - 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

based on the WebTrust Principle and Criteria for Certification Authorities version 2.0

And we also have examined the assertion by the management of KISA that in providing its Secure Socket Layer ("SSL") Certification Authority services, as a Root CA ("KISA RootCA 1 and KISA RootCA 4"), in Korea during the period 1 January 2016 through 31 December 2016, KISA also has

- disclosed its certificate practices and its commitment to provide SSL certificates in conformity with the applicable CA/Browser forum guidelines
- maintained effective controls to provide reasonable assurance that
  - the certificate policy and/or certificate practice statement are available on a 24x7 basis and updated annually;
  - the integrity of keys and certificates it manages was established and protected

throughout their life cycles;

- 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 systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity; and
- CA's network and certification systems security were properly managed.

based on the WebTrust Principle and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security version 2.0

The management of KISA 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 KISA's key and certificate life cycle management business practice and its controls over key and 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 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.

The relative effectiveness and significance of specific controls at KISA 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, KISA'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 period is subject to the risk that changes may alter the validity of such conclusions.

As stated by KISA in management assertion, KISA ("KISA RootCA 1 and KISA RootCA 4") does not provide revocation information via an online certificate status protocol (OCSP) service.

In our opinion, for the period 1 January 2016 through 31 December 2016, KISA management's assertion, as set forth above, is fairly stated, in all material respects, based on Webtrust Principle and Criteria for Certification Authorities version 2.0 and WebTrust Principle and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security version 2.0

This report does not include any representation as to the quality of KISA's services beyond those covered by the Webtrust Principle and Criteria for Certification Authorities version 2.0 and the WebTrust Principle and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security version 2.0 , nor the suitability of any services of KISA for any customer's intended purpose.

Deloitte Anjin LLC

Deloitte Anjin LLC
4 May 2017