(Translation)

Assertion by Management
as to its Disclosure of its Business Practices and its
Controls Over its Certification Authority Operations as of March 30, 2017

May 10, 2017

Mr. Masaru Sakamoto
Senior Manager
Product Management Department
Technology Division
Cybertrust Japan Co., Ltd.

Cybertrust Japan Co., Ltd. (“Cybertrust”) operates Certification Authorities (“CA”) through the SecureSign RootCA11 in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL-CA services.

The management of Cybertrust is responsible for establishing controls over its SSL-CA operations, including its network and certificate security system controls, its SSL-CA business practices disclosure on its website, key lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.
There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, controls placed into operation can only provide reasonable assurance with respect to Cybertrust’s CA operations.

Cybertrust management has assessed its disclosures of its business practices and controls over its SSL-CA services. Based on that assessment, in Cybertrust management’s opinion, in providing its SSL-CA services, as of March 30, 2017, Cybertrust has:

1. disclosed its business practices in its JCSI Root CA Certification Practice Statement Version 1.1, dated March 30, 2017, including its commitment to provide SSL-CA services in conformity with the CA/Browser Forum Requirement on Cybertrust’s website, and provided such services in accordance with its disclosed practices

2. suitably designed, and placed into operation, controls to provide reasonable assurance that:
   - the integrity of keys it manages is established and protected throughout their life cycles

(Translation)

3. suitably designed, and placed into operation, controls to provide reasonable assurance that:
   - logical and physical access to CA systems and data is restricted to authorized individuals;
   - the continuity of key management operations is maintained; and
   - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

4. suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v 2.2.

(The above represents a translation, for convenience only, of the original assertion issued in the Japanese language.)