(Translation)

WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Independent Accountant's Report

March 27, 2017

To Mr. Hiroshi Inagaki
Director of Information Systems Management Office
Government Information Systems Planning Division
Administrative Management Bureau
Ministry of Internal Affairs and Communications

KPMG AZSA LLC
Partner
Certified Public Accountant
Hiromi Iwashita

Scope of the examination

We have examined the assertion by the management of Ministry of Internal Affairs and Communications (the "management's assertion") that for its certification authority ("CA") services, as of January 31, 2017 through its the Government Public Key Infrastructure ("GPKI") Application Certification Authority2 (Root) and Application Certification Authority2 (Sub) (collectively referred to as the "SSL-CA services") in scope for SSL Baseline Requirements and Network Security Requirements, Ministry of Internal Affairs and Communications has:

1. disclosed its SSL certificate life cycle management business practices in its Application CA2(Root) CP/CPS, dated September 7, 2015 and Application CA2(Sub) CP/CPS, dated September 7, 2015, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on Ministry of Internal Affairs and Communications'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 and SSL certificates it manages is established and protected throughout their life cycles; and

(Translation)

-SSL subscriber information is properly authenticated (for the registration activities performed by Ministry of Internal Affairs and Communications)

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 and certificate 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 2.0.

Management's responsibility
Ministry of Internal Affairs and Communications's management is responsible for its assertion.

Independent Accountants' responsibility
Our responsibility is to express an opinion on management's assertion based on our examination. We conducted our examination in accordance with IT Committee Practice Guidelines No.2 established by the Japanese Institute of Certified Public Accountants, and accordingly, included:

(1) obtaining an understanding of Ministry of Internal Affairs and Communications's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Ministry of Internal Affairs and Communications's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) evaluating the suitability of the design of the controls; and
(3) performing such other procedures as we considered necessary in the circumstances.

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

(Translation)

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Ministry of Internal Affairs and Communications's controls, individually or in the aggregate.

The suitability of the design of the controls at Ministry of Internal Affairs and Communications 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 suitability of the design of the controls at individual subscriber and relying party locations.

Limitations in controls

Because of the nature and inherent limitations of controls, Ministry of Internal Affairs and Communications'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.

Opinion

In our opinion, as of January 31, 2017, the management's assertion is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v 2.0.

Emphasis

This report does not include any representation as to the quality of Ministry of Internal Affairs and Communications's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v 2.0, nor the suitability of any of Ministry of Internal Affairs and Communications's SSL-CA services for any customer's intended purpose.

Other matter

(Translation)

KPMG AZSA LLC and engagement partners have no interest in Ministry of Internal Affairs and Communications, which should be disclosed pursuant to the provisions of the Certified Public Accountants Law of Japan.

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