

Report of Independent Certified Public Accountant

To the Management of
Ministry of Internal Affairs and Communications:

We have examined the [assertion](#) by the management of Ministry of Internal Affairs and Communications (MIC) that in providing its Certification Authority (Government Public Key Infrastructure (GPKI) Application CA) services at Tokyo, Japan during the period from Aug 1, 2008 through Jan 31, 2009, MIC has—

- Disclosed its key and certificate life cycle management business and information privacy practices in [GPKI Application Certification Authority Certificate Policy and Certification Practice Statement](#) on the GPKI website and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by MIC) and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
 - the continuity of key and certificate life cycle management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the AICPA/CICA [WebTrust for Certification Authorities Criteria](#).

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

MIC makes use of external registration authorities for specific subscriber registration activities as disclosed in MIC's business practice disclosures. Our examination did not extend to the controls of external registration authorities.

Our examination was conducted in accordance with IT Committee Report No.2 established by the Japanese Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of MIC's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the continuity of key and certificate life cycle management operations, over the authenticity and privacy of subscriber and relying party information and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy 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.

In our opinion, for the period Aug 1, 2008 through Jan 31, 2009, MIC management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities Criteria.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for Certification Authorities on GPKI'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.

The relative effectiveness and significance of specific controls at MIC 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 external registration authorities and individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.

This report does not include any representation as to the quality of MIC's services beyond those covered by the WebTrust for Certification Authorities Criteria, nor the suitability of any of MIC's services for any customer's intended purpose.

Deloitte Touche Tohmatsu

Tokyo, Japan

Mar 31, 2009

**Assertion of Management as to
its Disclosure of its Business Practices and its Controls Over
its Certification Authority Operations
during the period from Aug 1, 2008 through Jan 31, 2009**

Jan 31, 2009

Ministry of Internal Affairs and Communications (MIC) provides the following certification authority (CA) services through the GPKI Application CA (APCA):

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

APCA makes use of external registration authorities for specific subscriber registration activities as disclosed in APCA's business practice disclosures.

Management of MIC is responsible for establishing and maintaining effective controls over its Certification Authority operations, including CA business practices disclosure in its [GPKI Application CA CP/CPS](#) on the GPKI website, 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.

There are inherent limitations in any controls including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal control can provide only reasonable assurance with respect to MIC's Certification Authority operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in Ministry of Internal Affairs and Communications (MIC) Management's opinion, in providing its Certification Authority (CA) services at Tokyo, Japan during the period from Aug 1, 2008

through Jan 31, 2009, MIC has—

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by MIC) and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
 - The continuity of key and certificate life cycle management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the AICPA/CICA [WebTrust for Certification Authorities Criteria](#) including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation

CA Key Storage, Backup and Recovery

CA Public Key Distribution

CA Key Usage

CA Key Destruction

CA Key Archival

CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Status Information Processing

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
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
Event Journaling

Norio Hashiguchi
Director General, Administrative Management Bureau,
Ministry of Internal Affairs and Communications