Independent Accountants' Report

To the Board of Directors of
Visa, Inc.:

We have examined the <u>assertion</u> by the management of Visa, Inc. ("Visa") that in providing its Visa PKI Certification Authority (CA) services in Foster City, CA and Highland Ranch, CO during the period September 1, 2010 through August 31, 2011, Visa, Inc. has—

- Disclosed its key and certificate life cycle management business and information privacy practices in its <u>Visa PKI Certificate Policy</u> on the Visa 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 Visa) 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 <u>WebTrust for Certification Authorities Criteria</u> for the Visa eCommerce Root CA, eCommerce Issuing CA, eVisa Sub-CA, USA CA, CEMEA CA, and Canada CA, (collectively referred to as the "Visa eCommerce CAs")

Visa 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:

- Obtaining an understanding of Visa's key and certificate life cycle management business and information privacy practices

- Obtaining an understanding of Visa's controls over:
    - Key and certificate integrity;
    - The authenticity and privacy of subscriber and relying party information;
    - The continuity of key and certificate life cycle management operations; and
    - Development, maintenance and operations of CA systems

- Selectively testing transactions executed in accordance with Visa's disclosed key and certificate life cycle management business and information privacy practices

- Testing and evaluating the operating effectiveness of the controls

- 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 September 1, 2010 through August 31, 2011, Visa management's assertion, as set forth above, 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) the degree of compliance with the policies or procedures may alter the validity of such conclusions.

The relative effectiveness and significance of specific controls at Visa 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.

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

KPMG LLP

November 2, 2011

**Assertion of Management as to
its Disclosure of its Business Practices and its Controls
over its Certification Authority Operations
during the period from September 1, 2010 through August 31, 2011**

November 2, 2011

Visa, Inc. ("Visa") provides the following certification authority (CA) services through the Visa eCommerce Root CA, eCommerce Issuing CA, eVisa Sub-CA, USA CA, CEMEA CA, and Canada CA, (collectively referred to as the "Visa eCommerce CAs"):

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate status information processing
- Integrated circuit card life cycle management.

Management of Visa is responsible for establishing and maintaining effective controls over its Visa eCommerce CA operations, including CA business practices disclosure in its Visa Public Key Infrastructure Certificate Policy on the Visa 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 controls can provide only reasonable assurance with respect to the Visa CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its Visa CA operations. Based on that assessment, in Visa Management's opinion, in providing its Visa CA services in Foster City, CA and Highland Ranch, CO during the period September 1, 2010 through August 31, 2011, Visa, Inc. has —

- Disclosed its key and certificate life cycle management business and information privacy practices in its Visa Public Key Infrastructure Certificate Policy on the Visa 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 Visa, Inc.) 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
- CA-Provided Subscriber Key Management Services

Certificate Life Cycle Management Controls
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Status Information Processing
- Integrated Circuit Card Life Cycle Management

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

Michael Stefanich,

Senior Business Leader, Global Information Security – Applied Cryptography