55 Second Street
San Francisco, CA 94105

Telephone 415 963 5100

Independent Accountants' Report

To the Management of
Symantec Corporation:

We have examined the assertions by the management of Symantec Corporation ("Symantec") and VeriSign Inc. ("VeriSign"), an independent service organization that provides data center hosting services to Symantec, that in providing its Symantec and VeriSign Certification Authority (CA) services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; and Dublin, Ireland during the period December 1, 2011 through November 30, 2012 -

- Symantec has disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Symantec Certificate Policy, Version 2.8.9, dated October 3,2012 ("STN CP") and Symantec Trust Network Certification Practice Statement, Version 3.8.10, dated October 3, 2012 ("STN CPS") for the Symantec and VeriSign Root CAs, Symantec and VeriSign Issuing CAs, and VeriSign Extended Validation Issuing CAs on Symantec's website
- Symantec has maintained effective controls to provide reasonable assurance that
  - Symantec's Certification Practice Statement is consistent with its Certificate Policy
  - Symantec provides its services in accordance with its Certificate Policy and Certification Practice Statement
- Symantec has maintained effective controls to provide reasonable assurance that
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - The Subscriber information is properly authenticated (for the registration activities performed by Symantec); and
  - Subordinate CA certificate requests are accurate, authenticated, and approved
- Symantec and VeriSign[1] have maintained effective 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

based on the AICPA/CICA Trust Services Criteria for Certification Authorities for the following Symantec and VeriSign CAs:

[1] Limited to only physical access to CA systems and data hosted within the VeriSign data center in New Castle, Delaware

Symantec and VeriSign Root CAs:	Symantec and VeriSign Issuing CAs:
• VeriSign Class 3 Public Primary CA (PCA) • VeriSign Class 2 PCA • VeriSign Class 1 PCA • VTN Class 3 PCA – Generation 2 (G2) • VeriSign Class 2 PCA – G2 • VeriSign Class 1 PCA – G2 • VTN Class 3 PCA – Generation 3 (G3) • VeriSign Class 2 PCA – G3 • VeriSign Class 1 PCA – G3 • VeriSign Class 3 Public Primary Certification Authority – G5 • VeriSign Class 3 Public Primary CA – Generation 4 (G4) • VeriSign Authorized Code Signing Root CA for Microsoft • VeriSign Universal Root Certification Authority • Symantec Class 1 Public Primary Certification Authority – G6 • Symantec Class 2 Public Primary Certification Authority – G6 • Symantec Class 1 Public Primary Certification Authority – G4 • Symantec Class 2 Public Primary Certification Authority – G4 **VeriSign Extended Validation Issuing CAs:** • VeriSign Class 3 Extended Validation SSL CA • VeriSign Class 3 Extended Validation SSL SGC CA • VeriSign Class 3 Extended Validation CA - T1 • VeriSign Class 3 Extended Validation SGC CA - T1 * Also a Root CA	• VeriSign International Server CA – Class 3 • VeriSign Class 3 Secure Server CA • VeriSign Open Financial Exchange (OFX) CA – Class 3 (G2) • VeriSign Class 3 Secure Intranet Server CA • VeriSign Class 3 WLAN Secure Server CA • VeriSign Class 3 Code Signing 2004 CA • VeriSign Class 3 Secure Server CA – G2 • VeriSign Class 3 Secure OFX CA –G3 • VeriSign Class 3 Secure Server 1024-bit CA – G2 • VeriSign Class 3 Code Signing 2009-2 CA • VeriSign Class 3 Code Signing 2009 CA • VeriSign Authorized Code Signing CA for Microsoft • VeriSign Time Stamping Authority CA • VeriSign Class 1 Individual Subscriber CA – G3 • VeriSign Class 2 MPKI Individual Subscriber CA – G2 • VeriSign Class 3 International Server 1024-bit CA – G2 • VeriSign Class 3 Code Signing 2010 CA • VeriSign Class 3 International Server CA – G3 • VeriSign Class 3 Secure Server CA – G3 • VeriSign Class 3 Organizational CA • VeriSign Time Stamping Authority CA – G2 • VeriSign Time Stamping Services CA • VeriSign Class 3 International Server CA – T1 • VeriSign Class 3 Secure Server CA – T1 • VeriSign Class 3 Extended Validation Code Signing CA • Symantec Class 3 Organizational CA – G2 • Symantec Class 3 Organizational CA – G3 • Symantec Class 1 Individual Subscriber CA – G4 • Symantec Class 2 Shared Intermediate Certificate Authority

The management of Symantec and VeriSign are responsible for their respective assertions. Our responsibility is to express an opinion on management assertions based on our examination.

For the VeriSign International Server CA – Class 3, VeriSign Class 3 Secure Server CA, VeriSign Class 3 Secure Server CA – G2, VeriSign Class 3 Secure Server 1024-bit CA G2, VeriSign Class 3 International Server CA – G3, and VeriSign Class 3 Secure Server CA – G3, Symantec makes use of external registration authorities for specific subscriber registration activities as disclosed in the STN CPS. Our examination did not extend to the controls exercised by the external registration authorities.

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 Symantec's key and certificate life cycle management business practices

- Obtaining an understanding of 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 Symantec'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.

The relative effectiveness and significance of specific controls at Symantec and VeriSign 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, Symantec's and VeriSign'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.

In our opinion, for the period December 1, 2011 through November 30, 2012, Symantec and VeriSign management assertions, as set forth in the first paragraph, are fairly stated, in all material respects, based on the AICPA/CICA Trust Services Criteria for Certification Authorities.

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

The WebTrust seal of assurance for Certification Authorities on Symantec's website 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.

KPMG LLP

Certified Public Accountants

San Francisco, CA

May 6, 2013

Assertion by Management of Symantec Corporation
Regarding Its Disclosure of Its Business Practices and Its Controls
Over Its Certification Authority Operations
During the Period December 1, 2011 through November 30, 2012

May 6, 2013

Symantec Corporation operates various certification authorities (CAs) which provide a range of CA services. The Symantec and VeriSign Root CAs, Symantec and VeriSign Issuing CAs, and VeriSign Extended Validation Issuing CAs include the following:

Symantec and VeriSign Root CAs:

- VeriSign Class 3 Public Primary CA (PCA)
- VeriSign Class 2 PCA
- VeriSign Class 1 PCA
- VTN Class 3 PCA – Generation 2 (G2)
- VeriSign Class 2 PCA – G2
- VeriSign Class 1 PCA – G2
- VTN Class 3 PCA – Generation 3 (G3)
- VeriSign Class 2 PCA – G3
- VeriSign Class 1 PCA – G3
- VeriSign Class 3 Public Primary Certification Authority – G5
- VeriSign Class 3 Public Primary CA – Generation 4 (G4)
- VeriSign Authorized Code Signing Root CA for Microsoft
- VeriSign Universal Root Certification Authority
- Symantec Class 1 Public Primary Certification Authority – G6
- Symantec Class 2 Public Primary Certification Authority – G6
- Symantec Class 1 Public Primary Certification Authority – G4
- Symantec Class 2 Public Primary Certification Authority – G4

VeriSign Extended Validation Issuing CAs:

- VeriSign Class 3 Extended Validation SSL CA
- VeriSign Class 3 Extended Validation SSL SGC CA
- VeriSign Class 3 Extended Validation CA - T1
- VeriSign Class 3 Extended Validation SGC CA - T1

* Also a Root CA

Symantec and VeriSign Issuing CAs:

- VeriSign International Server CA – Class 3
- VeriSign Class 3 Secure Server CA
- VeriSign Open Financial Exchange (OFX) CA – Class 3 (G2)
- VeriSign Class 3 Secure Intranet Server CA
- VeriSign Class 3 WLAN Secure Server CA
- VeriSign Class 3 Code Signing 2004 CA
- VeriSign Class 3 Secure Server CA – G2
- VeriSign Class 3 Secure OFX CA –G3
- VeriSign Class 3 Secure Server 1024-bit CA – G2
- VeriSign Class 3 Code Signing 2009-2 CA
- VeriSign Class 3 Code Signing 2009 CA
- VeriSign Authorized Code Signing CA for Microsoft
- VeriSign Time Stamping Authority CA
- VeriSign Class 1 Individual Subscriber CA – G3
- VeriSign Class 2 MPKI Individual Subscriber CA – G2
- VeriSign Class 3 International Server 1024-bit CA – G2
- VeriSign Class 3 Code Signing 2010 CA
- VeriSign Class 3 International Server CA – G3
- VeriSign Class 3 Secure Server CA – G3
- VeriSign Class 3 Organizational CA
- VeriSign Time Stamping Authority CA – G2
- VeriSign Time Stamping Services CA
- VeriSign Class 3 International Server CA – T1
- VeriSign Class 3 Secure Server CA – T1
- VeriSign Class 3 Extended Validation Code Signing CA
- Symantec Class 3 Organizational CA – G2
- Symantec Class 3 Organizational CA – G3
- Symantec Class 1 Individual Subscriber CA – G4
- Symantec Class 2 Shared Intermediate Certificate Authority

Symantec's CA Business Practices Disclosures includes the following:

Certification Authorities	Corresponding CA Business Practices Disclosure
Symantec and VeriSign Root CAs, Symantec and VeriSign Issuing CAs, and VeriSign Extended Validation Issuing CAs	Symantec Certificate Policy, Version 2.8.9, dated October 3, 2012 ("STN CP") and Symantec Trust Network Certification Practice Statement, Version 3.8.10, dated October 3, 2012 ("STN CPS")

Symantec provides the following certification authority services through the Symantec and VeriSign CAs:

- Subscriber key management services
- Subscriber registration
- Certificate renewal *(except for the VeriSign Class 3 Code Signing 2004 CA, VeriSign Class 3 Code Signing 2009-2 CA, VeriSign Class 3 Code Signing 2009 CA, VeriSign Authorized Code Signing CA for Microsoft, and VeriSign Class 1 Individual Subscriber CA - G3 which support rekey but not renewal)*
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate status information processing (using an online repository)

Symantec makes use of external registration authorities for specific subscriber registration activities for the VeriSign International Server CA – Class 3, VeriSign Class 3 Secure Server CA, VeriSign Class 3 Secure Server CA – G2, VeriSign Class 3 Secure Server 1024-bit CA G2, VeriSign Class 3 International Server CA – G3, and VeriSign Class 3 Secure Server CA – G3 as disclosed in the STN CPS.

Management of Symantec is responsible for establishing and maintaining effective controls over its Symantec and VeriSign CA operations, including CA business practices disclosures in its STN CPS on Symantec's 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.

Controls have inherent limitations, 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 the Symantec and VeriSign CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its Symantec and VeriSign CA operations. Based on that assessment, to the best of our knowledge and belief, we confirm that in providing its Symantec and VeriSign CA services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; and Dublin, Ireland during the period December 1, 2011 through November 30, 2012, -

- Symantec has disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Symantec Certificate Policy, Version 2.8.9, dated October 3,2012 ("STN CP") and Symantec Trust Network Certification Practice Statement, Version 3.8.10, dated October 3, 2012 ("STN CPS") for the Symantec and VeriSign Root CAs, Symantec and VeriSign Issuing CAs, and VeriSign Extended Validation Issuing CAs on Symantec's website

- Symantec has maintained effective controls to provide reasonable assurance that
  - Symantec's Certification Practice Statement is consistent with its Certificate Policy
  - Symantec provides its services in accordance with its Certificate Policy and Certification Practice Statement
- Symantec has maintained effective controls to provide reasonable assurance that
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - The Subscriber information is properly authenticated (for the registration activities performed by Symantec); and
  - Subordinate CA certificate requests are accurate, authenticated, and approved
- Symantec has maintained effective 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

in accordance with the AICPA/CICA Trust Services Criteria for Certification Authorities including the following:

CA Business Practices Disclosure

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP/CPS Consistency

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

Subscriber Key Life Cycle Management Controls

- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

CA Environmental Controls

- 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
- Audit Logging

Symantec Corporation

Francis Rosch
Vice President, Engineering

Assertion by Management of VeriSign, Inc.
Regarding Its Controls
Over Symantec Certification Authority Operations Hosted in New Castle, Delaware
During the Period December 1, 2011 through November 30, 2012

May 6, 2013

VeriSign, Inc. an independent service organization (sub-service provider), provides data center hosting services to Symantec Corporation ("Symantec") for Symantec Certification Authorities (CAs) hosted in New Castle, Delaware.

Management of VeriSign is responsible for establishing and maintaining effective controls over its data center hosting services for Symantec CAs hosted in New Castle, Delaware including CA environmental controls (limited to physical and environmental security). 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 internal control can provide only reasonable assurance with respect to VeriSign's data center hosting services for Symantec CAs hosted in New Castle, Delaware. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its data center hosting services for Symantec CA operations. Based on that assessment, to the best of our knowledge and belief, we confirm that in providing its data center hosting services in New Castle, Delaware during the period December 1, 2011 through November 30, 2012, VeriSign has

- Maintained effective controls to provide reasonable assurance that
  - Physical access to Symantec CA systems and data is restricted to authorized individuals

in accordance with the AICPA/CICA Trust Services Criteria for Certification Authorities including the following:

CA Environmental Controls

- Physical and Environmental Security

VeriSign, Inc.

Mark Gathje
Senior Vice President

55 Second Street
San Francisco, CA 94105

Telephone 415 963 5100

Independent Accountants' Report

To the Management of
Symantec Corporation:

We have examined the assertion by the management of Symantec Corporation ("Symantec") that in providing its VeriSign Extended Validation (EV) Certification Authority (CA) services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, during the period December 1, 2011 through November 30, 2012, management of Symantec:

- Disclosed its VeriSign EV Certificate life cycle management practices and procedures on Symantec's website, in its Symantec Trust Network Certification Practice Statement, Version 3.8.10, dated October 3, 2012 ("STN CPS") including its commitment to provide VeriSign EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with its disclosed practices, and
- Maintained effective controls to provide reasonable assurance that:
  - EV Subscriber information was properly collected, authenticated (for the registration activities performed by Symantec) and verified, and
  - The integrity of keys and EV certificates it manages is established and protected throughout their life cycles

based on the WebTrust for Certification Authorities - Extended Validation Audit Criteria for the VeriSign Class 3 Public Primary Certification Authority, VeriSign Class 3 Public Primary Certification Authority – G5, VeriSign Universal Root Certification Authority, VeriSign Class 3 Extended Validation SSL CA, VeriSign Class 3 Extended Validation SSL SGC CA, VeriSign Class 3 Extended Validation CA – T1, and VeriSign Class 3 Extended Validation SSL SGC Certification Authority – T1 (collectively referred to as the "VeriSign EV-CAs").

Symantec's 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 (1) obtaining an understanding of Symantec's VeriSign EV certificate life cycle management practices and procedures, including its controls over issuance, renewal and revocation of Symantec's VeriSign EV certificates; (2) selectively testing transactions executed in accordance with Symantec's disclosed VeriSign EV certificate life cycle management 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 Symantec 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, Symantec'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.

In our opinion, for the period December 1, 2011 through November 30, 2012, Symantec management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the WebTrust for Certification Authorities - Extended Validation Audit Criteria.

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

Symantec’s use of the WebTrust for CAs EV Seal 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.

KPMG LLP

Certified Public Accountants

San Francisco, CA

May 6, 2013

Assertion by Management of Symantec Corporation
Regarding Its Disclosure of Its Business Practices and Its Controls
Over Its Certification Authority Operations
During the Period December 1, 2011 through November 30, 2012

May 6, 2013

Symantec Corporation ("Symantec") provides Extended Validation Certification Authority (EV-CA) services through its VeriSign Class 3 Public Primary Certification Authority, VeriSign Class 3 Public Primary Certification Authority – G5, VeriSign Universal Root Certification Authority, VeriSign Class 3 Extended Validation SSL CA, VeriSign Class 3 Extended Validation SSL SGC CA, VeriSign Class 3 Extended Validation CA – T1, and VeriSign Class 3 Extended Validation SSL SGC Certification Authority – T1 (collectively referred to as the "VeriSign EV-CAs").

Management has assessed the controls over its VeriSign EV-CA operations. Based on that assessment, to the best of our knowledge and belief, we confirm that in providing its VeriSign EV-CA services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan during the period December 1, 2011 through November 30, 2012, Symantec has:

- Disclosed its VeriSign EV Certificate life cycle management practices and procedures in its Symantec Trust Network Certification Practice Statement, Version 3.8.10, dated October 3, 2012 ("STN CPS") including its commitment to provide VeriSign EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with its disclosed practices, and
- Maintained effective controls to provide reasonable assurance that:
  - EV Subscriber information was properly collected, authenticated (for the registration activities performed by Symantec) and verified, and
  - The integrity of keys and EV certificates it manages is established and protected throughout their life cycles

in accordance with the AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria.

Symantec Corporation

Francis Rosch
Vice President, Engineering