KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

## Independent Accountant's 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, for the Symantec certification authority (CA) operations at Mountain View, California and New Castle, Delaware throughout the period June 16, 2016 to November 30, 2016 for Symantec's VeriSign Class 2 SSP Intermediate CA, VeriSign Class 3 SSP Intermediate CA, VeriSign Class 3 SSP Intermediate CA - G2, Symantec Class 1 SSP CA - G2, Symantec Class 2 SSP CA - G2, Symantec Class 3 SSP Intermediate CA - G3, Symantec Non Federal SSP Organization Signing CA, Symantec Healthcare CA, and the Symantec Non-Federal SSP – Customer Specific CAs[1] (collectively referred to as the "Non-Federal SSP CAs"):

- Symantec disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in its:
  - Symantec Trust Network Certificate Policy, Version 2.8.22, dated September 9, 2016 ("STN CP") – published on the Symantec website (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9),
  - Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013 ("Non-Federal SSP CPS") – published on the Symantec website, that was consistent with the STN CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9), and
  - Memorandum of Agreement dated June 15, 2016 between the Federal PKI Policy Authority and Symantec ("Symantec-MOA") (including all sections),

- Symantec provided its services in accordance with the disclosed practices including:
  - STN CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9),
  - Non-Federal SSP CPS that was consistent with the STN CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9), and
  - Symantec-MOA (including all sections)

- Symantec 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 integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Symantec); and

[1] The Symantec Non-Federal SSP – Customer Specific CAs include:

Under the VeriSign Class 2 SSP Intermediate CA: Fairfax County Government Basic CA

Under the VeriSign Class 3 SSP Intermediate CA - G2: APD MEAS Medium HW CA, Booz Allen Hamilton CA 02, Booz Allen Hamilton Device CA 02, CSC CA – 2, CSC Device CA - G2, Eid Passport LRA CA 1, Eid Passport LRA Content Signer CA 1, Eid PIV-I Test CA, Eid PIV-I Test Device CA, Millennium Challenge Corporation Medium HW CA - G2, Oregon Health Authority Medium Assurance CA, RAPIDGate PIV-I Agency CA, RAPIDGate PIV-I Device CA, RAPIDGate-Premier CA, RAPIDGate-Premier Device CA, Senate PIV-I CA G2, Senate PIV-I Device CA G2, State of Kansas Non Federal SSP CA G2

Under the Symantec Class 1 SSP CA - G2: NRC Rudimentary CA G2

Under the Symantec Class 2 SSP CA - G2: NRC Basic CA G2

Under the Symantec Class 3 SSP Intermediate CA - G3: CSRA FBCA C3 CA, CSRA FBCA C3 Device CA, Eid Passport LRA 2 CA, Eid Passport LRA CA 3, Eid Passport LRA Content Signer CA 3, Eid Passport LRA Device 2 CA, Senate PIV-I CA G4, Senate PIV-I Device CA G4, SureID Inc. CA1, SureID Inc. CA2, SureID Inc. Device CA1, SureID Inc. Device CA2

  - subordinate CA certificate requests are accurate, authenticated, and approved

- Symantec and Verisign[2] 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

for the Non-Federal SSP CAs based on the WebTrust Principles and Criteria for Certification Authorities v2.0.

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

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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Symantec makes use of external registration authorities for specific subscriber registration activities for the Symantec Non-Federal SSP – Customer Specific CAs and Symantec Healthcare CA as disclosed in the Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013. Our examination did not extend to the controls exercised by these external registration authorities.

We conducted our examination, which commenced on October 19, 2016 and ended on April 13, 2017, in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of Symantec's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations 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 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.

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, throughout the period June 16, 2016 to November 30, 2016, Symantec and Verisign management's assertions, as referred to above, are fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities v2.0.

This report does not include any representation as to the quality of Symantec's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of Symantec's services for any customer's intended purpose.

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

Symantec's use of the WebTrust for Certification Authorities 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

Santa Clara, California
April 13, 2017

**Assertion by Management as to**
**Its Disclosure of its Business Practices and its Controls**
**Over Certification Authority Operations**
**During the Period from June 16, 2016 through November 30, 2016**

April 13, 2017

Symantec Corporation ("Symantec") provides the following certification authority services through the VeriSign Class 2 SSP Intermediate CA, VeriSign Class 3 SSP Intermediate CA, VeriSign Class 3 SSP Intermediate CA - G2, Symantec Class 1 SSP CA - G2, Symantec Class 2 SSP CA - G2, Symantec Class 3 SSP Intermediate CA - G3, Symantec Non Federal SSP Organization Signing CA, Symantec Healthcare CA, and the Symantec Non-Federal SSP – Customer Specific CAs[1] (collectively referred to as the "Non-Federal SSP CAs"):

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

Symantec also makes use of external registration authorities for specific subscriber registration activities for the Symantec Non-Federal SSP – Customer Specific CAs and Symantec Healthcare CA as disclosed in the Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013.

The management of Symantec is responsible for establishing and maintaining effective controls over its Symantec and Verisign CA operations, including its CA business practices disclosure, CA business practices management, CA environmental controls, CA key life cycle management controls, subscriber key life cycle management controls, certificate life cycle management controls, and subordinate CA certificate life cycle 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, even effective controls can only provide reasonable assurance with respect to Symantec and Verisign's certification authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Symantec management has assessed its disclosures of its certificate practices and controls over its Non-Federal SSP CA services. Based on that assessment, in Symantec management's opinion, in providing its

---

[1] The Symantec Non-Federal SSP – Customer Specific CAs include:

Under the VeriSign Class 2 SSP Intermediate CA: Fairfax County Government Basic CA

Under the VeriSign Class 3 SSP Intermediate CA - G2: APD MEAS Medium HW CA, Booz Allen Hamilton CA 02, Booz Allen Hamilton Device CA 02, CSC CA – 2, CSC Device CA - G2, Eid Passport LRA CA 1, Eid Passport LRA Content Signer CA 1, Eid PIV-I Test CA, Eid PIV-I Test Device CA, Millennium Challenge Corporation Medium HW CA - G2, Oregon Health Authority Medium Assurance CA, RAPIDGate PIV-I Agency CA, RAPIDGate PIV-I Device CA, RAPIDGate-Premier CA, RAPIDGate-Premier Device CA, Senate PIV-I CA G2, Senate PIV-I Device CA G2, State of Kansas Non Federal SSP CA G2

Under the Symantec Class 1 SSP CA - G2: NRC Rudimentary CA G2

Under the Symantec Class 2 SSP CA - G2: NRC Basic CA G2

Under the Symantec Class 3 SSP Intermediate CA - G3: CSRA FBCA C3 CA, CSRA FBCA C3 Device CA, Eid Passport LRA 2 CA, Eid Passport LRA CA 3, Eid Passport LRA Content Signer CA 3, Eid Passport LRA Device 2 CA, Senate PIV-I CA G4, Senate PIV-I Device CA G4, SureID Inc. CA1, SureID Inc. CA2, SureID Inc. Device CA1, SureID Inc. Device CA2

Non-Federal SSP CA services at Mountain View, California and New Castle, Delaware throughout the period June 16, 2016 to November 30, 2016:

- Symantec disclosed its business, key life cycle management, certificate life cycle management, and CA environment control practices in its:
  - Symantec Trust Network Certificate Policy, Version 2.8.22, dated September 9, 2016 ("STN CP") – published on the Symantec website (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9),
  - Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement version 1.24 – dated April 29, 2013 ("Non-Federal SSP CPS") – published on the Symantec website, that was consistent with the STN CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9), and
  - Memorandum of Agreement dated June 15, 2016 between the Federal PKI Policy Authority and Symantec ("Symantec-MOA") (including all sections)

- Symantec provided its services in accordance with the disclosed practices including:
  - STN CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9),
  - Non-Federal SSP CPS that was consistent with the STN CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9), and
  - Symantec-MOA (including all sections)

- Symantec 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 integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Symantec); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- Symantec 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 WebTrust Principles and Criteria for Certification Authorities v2.0, including the following:

**CA Business Practices Disclosure**

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

**CA Business Practices Management**

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

**CA Environmental Controls**

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security

- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

**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 Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

**Subordinate CA Certificate Life Cycle Management Controls**

- Subordinate CA Certificate Life Cycle Management

Symantec Corporation

Nicolas Popp
Senior Vice President, Information Protection

**Assertion by Management of Verisign, Inc.**
**Regarding its Controls**
**Over Symantec Certification Authority Operations Hosted in New Castle, Delaware**
**During the Period June 16, 2016 through November 30, 2016**

April 13, 2017

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 June 16, 2016 through November 30, 2016, Verisign has

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

based on the WebTrust Principles and Criteria for Certification Authorities v2.0 including the following:

**CA Environmental Controls**

- Physical and Environmental Security

Verisign, Inc.

Joseph David Pool
Senior Vice President of Architecture & Tech Services