



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 for Symantec Corporation's ("Symantec") certification authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, and Verisign, Inc. ("Verisign"), an independent service organization that provides data center hosting services to Symantec, Symantec's disclosure of its SSL certificate life cycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Symantec website, the provision of such services in accordance with its disclosed practices, and the design of its controls over key and SSL certificate integrity, over the authenticity and confidentiality of SSL subscriber and relying party information, over continuity of key and SSL certificate life cycle management operations, and over development, maintenance, and operation of CA systems integrity, and over meeting the network and certificate system security requirements set forth by the CA/Browser Forum, throughout the period June 16, 2016 to November 30, 2016 for the GeoTrust CAs listed in Appendix A ("the GeoTrust Root and SSL Issuing CAs") in scope for SSL Baseline Requirements and Network Security Requirements.

These disclosures and controls are the responsibility of Symantec and Verisign's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0, based on our examination.

Symantec makes use of external registration authorities ("Affiliates") for specific subscriber registration activities as disclosed in the GeoTrust CPS. Our examination did not extend to the controls exercised by these external registration authorities.

We conducted our examination 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 SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Symantec's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) selectively testing transactions executed in accordance with disclosed SSL 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 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 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.



We noted the following matters that resulted in a modification of our opinion:

Impacted WebTrust for CAs Criteria	Matters Noted
<p>1</p>	<p>Principle 2, Criterion 2.2 requires that the CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following:</p> <ul style="list-style-type: none"> • As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA shall notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. • Also as of the Effective Date, the CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a SubjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name. (See SSL Baseline Requirements Section 9.2.6)
<p>2</p>	<p>It was noted that in accordance with the Baseline Requirements 9.2.6 and GeoTrust CPS section 1.4.1, Symantec performed a review of SSL certificates with internal names, expiring after October 1, 2016. Although Symantec identified and revoked the majority of such certificates as part of this activity, in limited circumstances certificates with internal names with pending TLD status were not identified and revoked in a timely manner. These certificates have since been revoked.</p> <p>This caused WebTrust for CAs – SSL Baseline with Network Security Principle 2, Criterion 2.2 to not be met.</p>
	<p>Principle 4, Criterion 4 requires that the CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; • Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: <ul style="list-style-type: none"> ○ Within one week of receiving a request from the CA/Browser Forum, ○ After any system or network changes that the CA determines are significant, and ○ At least once per quarter; • Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and



Impacted WebTrust for CAs Criteria	Matters Noted
<p>after infrastructure or application upgrades or modifications that the CA determines are significant;</p> <ul style="list-style-type: none">• Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test;• Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:<ul style="list-style-type: none">○ Remediate the Critical Vulnerability;○ If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following:<ul style="list-style-type: none">▪ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and▪ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or○ Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following:<ul style="list-style-type: none">▪ The CA disagrees with the NVD rating;▪ The identification is a false positive;▪ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or▪ Other similar reasons. <p>(See Network and Certificate Systems Security Requirements Section 4)</p>	<p>This caused WebTrust for CAs – SSL Baseline with Network Security Principle 4, Criterion 4 to not be met.</p>

	Impacted WebTrust for CAs Criteria	Matters Noted
3	<p>Principle 2, Criterion 2.1 requires that the CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following:</p> <ul style="list-style-type: none"> • Issuer Information (See SSL Baseline Requirements Section 9.1) • Subject Information (See SSL Baseline Requirements Section 9.2) • Certificate Policy Identification (See SSL Baseline Requirements Section 9.3) • Validity Period (See SSL Baseline Requirements Section 9.4) • Public Key (See SSL Baseline Requirements Section 9.5) • Certificate Serial Number (See SSL Baseline Requirements Section 9.6) • Additional Technical Requirements (See SSL Baseline Requirements Section 9.7) <ul style="list-style-type: none"> ○ Appendix A - Cryptographic Algorithm and Key Requirements ○ Appendix B - Certificate Extensions. <p>(See SSL Baseline Requirements Section 9)</p>	<p>It was noted Symantec disclosed an instance where a subscriber certificate was issued on 11/24/2016 from the RapidSSL SHA256 - G3 CA with a sequential serial number that did not meet the requirements listed in the GeoTrust CPS section 7.1 – Certificate Profile, which requires GeoTrust Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Per inquiry, this certificate was issued to meet a customer business requirement.</p> <p>This caused WebTrust for CAs – SSL Baseline with Network Security Principle 2, Criterion 2.1 to not be met for the RapidSSL SHA256 - G3.</p>

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, throughout the period June 16, 2016 to November 30, 2016, in all material respects:

- Symantec disclosed its SSL certificate life cycle management business practices in its GeoTrust Certification Practice Statement, Version 1.1.19 dated, September 9, 2016 (“GeoTrust CPS”) including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Symantec website, and provided such services in accordance with its disclosed practices
- Symantec maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
 - SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)
- Symantec and Verisign¹ 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
- Symantec maintained effective 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 v2.0.

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



Page 5

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 – SSL Baseline with Network Security v2.0, nor the suitability of any of Symantec's services for any customer's intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, CA
February 28, 2017

APPENDIX A –GeoTrust Root and SSL Issuing CAs

<p>GeoTrust Root CAs:</p> <ul style="list-style-type: none"> • GeoTrust Global CA • GeoTrust Primary Certification Authority • GeoTrust Primary Certification Authority - G2 • GeoTrust Primary Certification Authority - G3 • GeoTrust Primary Certification Authority - G4 • GeoTrust Universal CA • GeoTrust Universal CA 2 • GeoTrust Global CA 2 	<p>GeoTrust SSL Issuing CAs:</p> <ul style="list-style-type: none"> • GeoTrust Extended Validation SSL CA • GeoTrust Extended Validation SSL CA - G2 • GeoTrust EV SSL CA - G4 • GeoTrust Extended Validation SHA256 SSL CA • GeoTrust EV SSL CA - G5 • GeoTrust ECC EV SSL CA • GeoTrust SSL CA • GeoTrust DV SSL CA • RapidSSL CA • GeoTrust SSL CA - G2 • RapidSSL Enterprise CA • GeoTrust DV SSL CA - G2 • RapidSSL CA - G2 • GeoTrust SHA256 SSL CA • GeoTrust DSA SSL CA • GeoTrust SSL CA - G3 • RapidSSL Enterprise DSA SSL CA • RapidSSL SHA256 CA • GeoTrust DV SSL SHA256 CA • RapidSSL SHA256 CA - G2 • GeoTrust DV SSL CA - G3 • GeoTrust DV SSL CA - G4 • RapidSSL SHA256 CA - G3 • GeoTrust SSL CA - G4 • GeoTrust DV SSL SHA256 CA - G2 • RapidSSL SHA256 CA - G4 • GeoTrust Secure Site Starter DV SSL CA - G1 • Secure Site Starter DV SSL CA - G2 • Secure Site Starter DV SSL CA - G3 • Volusion, Inc. DV SSL CA • Volusion, Inc. DV SSL CA - G2 • Volusion, Inc. DV SSL CA - G3 • Intermediate Certificate DV SSL CA • Intermediate Certificate DV SSL CA - G2 • Intermediate Certificate DV SSL CA - G3 • STRATO SSL • STRATO SSL - G2 • STRATO SSL - G3 • Hostpoint DV SSL CA – G1 • Hostpoint DV SSL CA – G2 • Trust Provider B.V. DV SSL CA - G1 • Trust Provider B.V. DV SSL CA - G2 • AlwaysOnSSL CA - G1 • AlwaysOnSSL CA - G2 • TrustAsia Technologies, Inc. DV SSL CA - G1 • TrustAsia Technologies, Inc. DV SSL CA - G2 • STRATO SSL - G4 • STRATO SSL - G5 • Volusion, Inc. DV SSL CA - G4 • Volusion, Inc. DV SSL CA - G5 • DKHS Device CA • DKHS Device CA-G2
--	---



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

February 28, 2017

Symantec Corporation ("Symantec") provides its GeoTrust SSL Certification Authority (CA) services through the GeoTrust CAs listed in Appendix A ("the GeoTrust Root and SSL Issuing CAs") in scope for SSL Baseline Requirements and Network Security Requirements.

Symantec also makes use of external registration authorities ("Affiliates") for specific subscriber registration activities as disclosed in the GeoTrust CPS.

The management of Symantec is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key life cycle management controls, and SSL 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'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 GeoTrust SSL CA services. Based on that assessment, in Symantec management's opinion, in providing its SSL certification authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Cape Town, South Africa; Melbourne, Australia; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, throughout the period June 16, 2016 to November 30, 2016, Symantec has:

- disclosed its SSL certificate life cycle management business practices in its [GeoTrust Certification Practice Statement](#), Version 1.1.19 dated, September 9, 2016 ("GeoTrust CPS"), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Symantec website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
 - SSL subscriber information is properly authenticated (for the registration activities performed by 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
- maintained effective 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 v2.0 except for the matters noted below.

Impacted WebTrust for CAs Criteria	Matters Noted
<p>1</p> <p>Principle 2, Criterion 2.2 requires that the CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the SSL Baseline Requirements including the following:</p> <ul style="list-style-type: none"> • As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA shall notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. • Also as of the Effective Date, the CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a SubjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name. (See SSL Baseline Requirements Section 9.2.6) 	<p>It was noted that in accordance with the Baseline Requirements 9.2.6 and STN CPS section 3.2.2, Symantec performed a review of SSL certificates with internal names, expiring after October 1, 2016. Although Symantec identified and revoked the majority of such certificates as part of this activity, in limited circumstances certificates with internal names with pending TLD status were not identified and revoked in a timely manner. These certificates have since been revoked.</p> <p>Prior to the October 1, 2016 change in Baseline Requirements regarding internal names, Symantec conducted an analysis in which we examined every CN and SAN in certificates still valid at the time. Following this analysis, Symantec identified and revoked the still valid certificates including internal names. We subsequently identified an edge case where certificates with internal names where the TLD status was pending with ICANN had not been included in our effort prior to the October 1, 2016 change. Once we identified this case, we revoked these remaining certificates using internal names. We publicly disclosed this issue and remediation when it occurred.</p>
<p>2</p> <p>Principle 4, Criterion 4 requires that the CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; • Perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: <ul style="list-style-type: none"> ○ Within one week of receiving a request from the CA/Browser Forum, ○ After any system or network changes that the CA determines are significant, and ○ At least once per quarter; • Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and 	<p>It was noted that Symantec did not consistently maintain formal documentation of the basis for Symantec's determination that remediation was not required for critical vulnerabilities not requiring remediation, as required by WTBR criterion 4.4 and Symantec's Threat and Vulnerability Management Policy.</p> <p>Additionally, the following was noted pertaining to in-scope systems for one international production environment (where two in-scope CAs are hosted):</p> <ul style="list-style-type: none"> • vulnerability scans on internal IP addresses did not include all production systems in-scope • vulnerability scans on internal IP addresses were not consistently performed at least quarterly per the frequency requirements in the Network Security Requirements • a penetration test was not performed during the examination period.

Impacted WebTrust for CAs Criteria	Matters Noted
<p>after infrastructure or application upgrades or modifications that the CA determines are significant;</p> <ul style="list-style-type: none"> • Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; • Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: <ul style="list-style-type: none"> ○ Remediate the Critical Vulnerability; ○ If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: <ul style="list-style-type: none"> ▪ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ▪ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or ○ Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: <ul style="list-style-type: none"> ▪ The CA disagrees with the NVD rating; ▪ The identification is a false positive; ▪ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or ▪ Other similar reasons. <p>(See Network and Certificate Systems Security Requirements Section 4)</p>	<p>Symantec has updated its vulnerability management program to ensure that the disposition and associated analysis are consistently documented. In addition to the external vulnerability scans already performed, Symantec has expanded its quarterly scan process to include the internal production hosts in the international location referenced above and a penetration test has been scheduled to complete in March 2017.</p>

Impacted WebTrust for CAs Criteria	Matters Noted
<p>3 Principle 2, Criterion 2.1 requires that the CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following:</p> <ul style="list-style-type: none">• Issuer Information (See SSL Baseline Requirements Section 9.1)• Subject Information (See SSL Baseline Requirements Section 9.2)• Certificate Policy Identification (See SSL Baseline Requirements Section 9.3)• Validity Period (See SSL Baseline Requirements Section 9.4)• Public Key (See SSL Baseline Requirements Section 9.5)• Certificate Serial Number (See SSL Baseline Requirements Section 9.6)• Additional Technical Requirements (See SSL Baseline Requirements Section 9.7)<ul style="list-style-type: none">○ Appendix A - Cryptographic Algorithm and Key Requirements○ Appendix B - Certificate Extensions. <p>(See SSL Baseline Requirements Section 9)</p>	<p>It was noted Symantec disclosed an instance where a subscriber certificate was issued on 11/24/2016 from the RapidSSL SHA256 - G3 CA with a sequential serial number that did not meet the requirements listed in the GeoTrust CPS section 7.1 – Certificate Profile, that requires GeoTrust Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.</p> <p>This certificate issuance instance was approved by management on an exception basis in order to support emergency continuity of a customer's eCommerce application which would otherwise have had a major impact to consumers and businesses during a significant holiday shopping period. The application in question relied on a legacy intermediate CA that has since been replaced in part because it only supported certificate issuance using sequential serial numbers. Due to the criticality of this issue and the assessed impact, Symantec issued a replacement certificate, but limited the validity to only a three month period. We proactively disclosed this instance in the CA/Browser Forum and published the certificate record in certificate transparency (CT) logs. This certificate has since expired.</p>

Symantec Corporation



Roxane Divor
EVP and GM, Website Security

APPENDIX A –GeoTrust Root and SSL Issuing CAs**GeoTrust Root CAs:**

- GeoTrust Global CA
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority - G2
- GeoTrust Primary Certification Authority - G3
- GeoTrust Primary Certification Authority - G4
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- GeoTrust Global CA 2

GeoTrust SSL Issuing CAs:

- GeoTrust Extended Validation SSL CA
- GeoTrust Extended Validation SSL CA - G2
- GeoTrust EV SSL CA - G4
- GeoTrust Extended Validation SHA256 SSL CA
- GeoTrust EV SSL CA - G5
- GeoTrust ECC EV SSL CA
- GeoTrust SSL CA
- GeoTrust DV SSL CA
- RapidSSL CA
- GeoTrust SSL CA - G2
- RapidSSL Enterprise CA
- GeoTrust DV SSL CA - G2
- RapidSSL CA - G2
- GeoTrust SHA256 SSL CA
- GeoTrust DSA SSL CA
- GeoTrust SSL CA - G3
- RapidSSL Enterprise DSA SSL CA
- RapidSSL SHA256 CA
- GeoTrust DV SSL SHA256 CA
- RapidSSL SHA256 CA - G2
- GeoTrust DV SSL CA - G3
- GeoTrust DV SSL CA - G4
- RapidSSL SHA256 CA - G3
- GeoTrust SSL CA - G4
- GeoTrust DV SSL SHA256 CA - G2
- RapidSSL SHA256 CA - G4
- GeoTrust Secure Site Starter DV SSL CA - G1
- Secure Site Starter DV SSL CA - G2
- Secure Site Starter DV SSL CA - G3
- Volusion, Inc. DV SSL CA
- Volusion, Inc. DV SSL CA - G2
- Volusion, Inc. DV SSL CA - G3
- Intermediate Certificate DV SSL CA
- Intermediate Certificate DV SSL CA - G2
- Intermediate Certificate DV SSL CA - G3
- STRATO SSL
- STRATO SSL - G2
- STRATO SSL - G3
- Hostpoint DV SSL CA – G1
- Hostpoint DV SSL CA – G2
- Trust Provider B.V. DV SSL CA - G1
- Trust Provider B.V. DV SSL CA - G2
- AlwaysOnSSL CA - G1
- AlwaysOnSSL CA - G2
- TrustAsia Technologies, Inc. DV SSL CA - G1
- TrustAsia Technologies, Inc. DV SSL CA - G2
- STRATO SSL - G4
- STRATO SSL - G5
- Volusion, Inc. DV SSL CA - G4
- Volusion, Inc. DV SSL CA - G5
- DKHS Device CA
- DKHS Device CA - G2



**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**

February 28, 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 – SSL Baseline with Network Security v2.0 including the following:

CA Environmental Controls

- Physical and Environmental Security

Verisign, Inc.

A handwritten signature in black ink, appearing to read 'Joseph D. Pool', is written over the printed name.

Joseph David Pool
Senior Vice President of Architecture & Tech Services