



REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of SSL Corp d/b/a SSL.COM Certification Authority ("SSL.COM CA"):

We have examined for its Certification Authority (CA) operations at Houston, Texas, throughout the period September 20, 2016 to November 20, 2016 for its root and subordinate CAs in scope for SSL Baseline Requirements and Network Security Requirements listed in [Appendix A](#), SSL.COM CA has:

- disclosed its SSL certificate lifecycle management business practices in its [SSL.com Certificate Policy and Certification Practice Statement, Version 1.1](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement in the SSL.COM CA [repository](#), 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 lifecycles; and
 - SSL subscriber information is properly authenticated
- 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

And, for the list of root and subordinate CAs listed in Appendix A

- 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, Version 2.0](#).

These disclosures and controls are the responsibility of SSL.COM CA'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, Version 2.0., based on our examination.

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 SSL.COM CA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of SSL.COM CA'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 lifecycle 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.

During our examination, we noted a deficiency in the protection of a root CA. Specifically:

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		Control Deficiency Noted
4.1	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks 	<p>The SSL.com EV Root Certification Authority RSA was used in an online manner and not air-gapped from all other networks during the remote signing of a subordinate CA key.</p>

This caused the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security Criterion 4.1 to not be met.

In our opinion, except for the matter discussed in the preceding paragraph, throughout the period September 20, 2016 to November 20, 2016, SSL.COM CA has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices in its SSL.com Certificate Policy and Certification Practice Statement, Version 1.1, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement in the SSL.COM CA repository, 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 lifecycles; and
 - SSL subscriber information is properly authenticated
- 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



And, for the list of root and subordinate CAs listed in Appendix A

- 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, Version 2.0.

The relative effectiveness and significance of specific controls at SSL.COM CA 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, SSL.COM CA'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.

This report does not include any representation as to the quality of SSL.COM CA's services beyond those covered by WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security, Version 2.0, nor the suitability of any of SSL.COM CA's services for any customer's intended purpose.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
January 20, 2017



Trust is what we do.

SSL CORP CA MANAGEMENT'S ASSERTION

SSL Corp d/b/a SSL.COM Certification Authority ("SSL.COM CA") operates the Certification Authority (CA) services known as the root and subordinate CAs included in [Appendix A](#) in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

The management of SSL.COM CA 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 in its [repository](#), SSL key lifecycle management controls, and SSL certificate lifecycle 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 SSL.COM CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

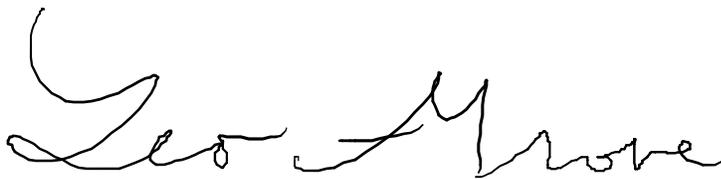
SSL.COM CA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in SSL.COM CA management's opinion, in providing its SSL CA services at Houston, Texas, throughout the period September 20, 2016 to November 20, 2016, SSL.COM CA has:

- disclosed its SSL certificate lifecycle management business practices in its [SSL.com Certificate Policy and Certification Practice Statement, Version 1.1](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement in the SSL.COM CA repository, 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 lifecycles; and
 - SSL subscriber information is properly authenticated for the registration activities performed by SSL.COM CA
- 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 met 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, Version 2.0](#), except for the effects of the matter noted below:

	Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security	Control Deficiency Noted
4.1	<p>The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks 	<p>The SSL.com EV Root Certification Authority RSA was used in a reasonably secure environment (protected via VPN and HSM vendor-supplied FIPS Certified encrypted secure messaging protocol), but ultimately in an online manner and not air-gapped from all other networks during the remote signing of a subordinate CA key.</p>



Leo Grove
Chief Executive Officer
January 20, 2017

APPENDIX A - IN-SCOPE CAs

Root CAs	Root CAs SHA 1 Thumbprint
SSL.com Root Certification Authority RSA	b7 ab 33 08 d1 ea 44 77 ba 14 80 12 5a 6f bd a9 36 49 0c bb
SSL.com EV Root Certification Authority RSA	1c b7 ed e1 76 bc df ef 0c 86 6f 46 fb f9 80 e9 01 e5 ce 35
SSL.com Root Certification Authority ECC	c3 19 7c 39 24 e6 54 af 1b c4 ab 20 95 7a e2 c3 0e 13 02 6a
SSL.com EV Root Certification Authority ECC	4c dd 51 a3 d1 f5 20 32 14 b0 c6 c5 32 23 03 91 c7 46 42 6d
CertLock Root Certification Authority RSA	73 76 45 8e f9 a0 72 97 a6 d1 5f 46 3a b6 26 f4 bb bf b2 94
CertLock EV Root Certification Authority RSA	c9 e9 c4 61 d0 36 17 8d 94 36 04 1f d3 3f a8 f0 0c 69 3c d0
CertLock Root Certification Authority ECC	d7 7b 5d 94 9a 72 93 e2 2c 0c 85 e0 04 65 fd 78 ef 30 c9 21
CertLock EV Root Certification Authority ECC	70 82 c5 ce 46 7f b6 d3 6c 2c c4 a5 c5 fc b1 70 d8 85 cb f8

Subordinate CAs	Subordinate CAs SHA 1 Thumbprint
SSL.com RSA SSL subCA	33 ee 4e 37 0a 8d 90 fd 4b 14 45 e6 72 22 6c 4b 82 9c c6 d2
SSL.com EV RSA SSL subCA	6c 78 fc 48 3b b6 9c 28 39 54 50 46 3d bd 4d f5 08 08 ae 21
SSL.com ECC SSL subCA	ad 3b 4f 82 ec 99 85 43 ee 8f 32 54 5d a3 11 9e 47 64 a5 85
SSL.com EV ECC SSL subCA	43 64 11 39 0d f6 0d 0a fc b1 b9 a7 5d 7d c1 ba 4d 2b 4f 6a
CertLock RSA SSL subCA	e5 f0 17 c2 23 03 01 a0 a0 1f 83 ee 36 e3 02 c3 bd dc 71 6b
CertLock EV RSA SSL subCA	ae cc 3d 0b ca 76 6a 6f c4 7f 43 c0 37 bc d6 19 84 e7 e6 e1
CertLock ECC SSL subCA	40 8b 37 90 d8 86 6b 00 e3 a6 f9 f0 55 3f e9 6c aa c4 72 93
CertLock EV ECC SSL subCA	6d 02 d5 c6 99 cd f0 47 91 f3 c2 47 06 b8 11 c4 3f 24 12 50