Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, #800
St. Louis, MO 63105

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, SSL.COM CA's disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, the provision of services in accordance with its Certificate Policy and Certification Practice Statement, and the effectiveness of 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 lifecycle management operations, and over development, maintenance, and operation of CA systems integrity throughout the period September 20, 2016 to November 20, 2016 for its root and subordinate CAs listed in Appendix A.

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 Trust Service Principles and Criteria for Certification Authorities, 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 key and certificate lifecycle 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 lifecycle management operations and over development, maintenance and operation of systems integrity;

(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle 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.

During our examination, we noted a deficiency in the CA key generation script used in the generation of CA key pairs for an intermediate CA. Specially:

Impacted Trust Service Principles and Criteria for Certification Authorities Criterion		Control Deficiency Noted
4.1	The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts. The CA's disclosed business practices include but are not limited to: a) generation of CA keys are undertaken in a physically secured environment (see §3.4); b) generation of CA keys are performed by personnel in trusted roles (see §3.3) under the principles of multiple person control and split knowledge; c) generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS; d) generation of CA keys are witnessed by an independent party and/or videotaped; and e) CA key generation activities are logged. The CA key generation script includes the following: a) definition of roles and participant responsibilities; b) approval for conduct of the key generation ceremony; c) cryptographic hardware and activation materials required for the ceremony; d) specific steps performed during the key generation ceremony; e) physical security requirements for the ceremony location; f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony; g) sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and h) notation of any deviations from the key generation ceremony script.	For the one intermediate CA generated, the CA key generation script used in the CA key pair generation ceremony did not include the following required disclosures: • a complete list of the cryptographic hardware and activation materials used during the generation; • procedures for secure storage of cryptographic hardware and activation materials at the conclusion of the key pair generation; • indication the key pair generation was witnessed by an independent party and/or videotaped; and • physical security requirements for the ceremony location.

This caused the Trust Service Criterion 4.1 to not be met.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its SSL.COM CA Certificate Policy and Certification Practice Statement, Version 1.1

- maintained effective controls to provide reasonable assurance that SSL.COM CA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated; and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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 Trust Service Principles and Criteria for Certification Authorities, 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 the Trust Service Principles and Criteria for Certification Authorities, 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, and provides the following CA services:

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

The management of SSL.COM CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure in its repository, CA business practices management, CA environmental controls, CA key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 CA services. Based on that assessment, in SSL.COM CA management's opinion, in providing its CA services at Houston, Texas, throughout the period September 20, 2016 to November 20, 2016, SSL.COM CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its SSL.com Certificate Policy and Certification Practice Statement, Version 1.1

- maintained effective controls to provide reasonable assurance that SSL.COM CA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:

3100 Richmond Ave. Suite 503 Houston, TX 77098
Phone: 877 755 7325 Fax: 832 201 7706
Email: compliance@ssl.com

  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycle;
  - subscriber information is properly authenticated; and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- 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 Trust Service Principles and Criteria for Certification Authorities, Version 2.0, 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

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 Lifecycle 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 Lifecycle Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinated CA Certificate Lifecycle Management

except for the effects of the matter noted below:

Impacted Trust Service Principles and Criteria for Certification Authorities		Control Deficiency Noted
4.1	The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts. The CA's disclosed business practices include but are not limited to: a) generation of CA keys are undertaken in a physically secured environment (see §3.4); b) generation of CA keys are performed by personnel in trusted roles (see §3.3) under the principles of multiple person control and split knowledge; c) generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS; d) generation of CA keys are witnessed by an independent party and/or videotaped; and e) CA key generation activities are logged. The CA key generation script includes the following: a) definition of roles and participant responsibilities;	For the one intermediate CA generated, the CA key generation script used in the CA key pair generation ceremony did not include the following required disclosures: • a complete list of the cryptographic hardware and activation materials used during the generation; • procedures for secure storage of cryptographic hardware and activation materials at the conclusion of the key pair generation;

	b) approval for conduct of the key generation ceremony; c) cryptographic hardware and activation materials required for the ceremony; d) specific steps performed during the key generation ceremony; e) physical security requirements for the ceremony location; f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony; g) sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and h) notation of any deviations from the key generation ceremony script.	• indication the key pair generation was witnessed by an independent party and/or videotaped; and • physical security requirements for the ceremony location.

Leo Grove
Chief Executive Officer
January 20, 2017

3100 Richmond Ave. Suite 503 Houston, TX 77098
Phone: 877 755 7325 Fax: 832 201 7706
Email: compliance@ssl.com

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
SSL.com EV Code Signing Intermediate CA RSA R1	9b 53 1b 2b f2 b9 d2 69 13 f0 bb ce 7a 8d 7c 36 4d f1 45 5b
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

3100 Richmond Ave. Suite 503 Houston, TX 77098
Phone: 877 755 7325 Fax: 832 201 7706
Email: compliance@ssl.com