

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of Internet Security Research Group:

Scope

We have examined the [assertion by the management](#) of Internet Security Research Group (“ISRG”) that in providing its Let’s Encrypt certification authority (CA) services at its Salt Lake City, Utah, USA, and Denver, Colorado, USA, locations, throughout the period from December 1, 2017, to November 30, 2018, for its root and subordinate CA certificates as listed in Appendix A, ISRG has:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control policies and practices in its:
 - [Certification Practice Statement \(v2.5\)](#); and
 - [Certificate Policy \(v2.2\)](#);
- Maintained effective controls to provide reasonable assurance that:
 - ISRG’s Certification Practice Statement is consistent with its Certificate Policy;
 - ISRG provides its services in accordance with its Certificate Policy and Certification Practice Statement;
 - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
 - Subscriber information is properly authenticated (for the registration activities performed by ISRG);
 - Logical and physical access to CA systems and data is restricted to authorized individuals;
 - The continuity of key and certificate management operations is maintained;
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity; and
 - Subscriber information was properly authenticated (for the registration activities performed by ISRG).

based on the [WebTrust Principles and Criteria for Certification Authorities - Version 2.1](#)

ISRG Responsibilities

ISRG’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

The relative effectiveness and significance of specific controls at ISRG 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.

Independent Certified Public Accountant’s Responsibilities

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

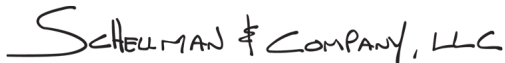
Because of the nature and inherent limitations of controls, ISRG's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies 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.

Opinion

In our opinion, management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ISRG's services other than its CA operations at its Salt Lake City, Utah, USA, and Denver, Colorado, USA, locations, nor the suitability of any of ISRG's services for any customer's intended purpose.

ISRG'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.

SCHHELLMAN & COMPANY, LLC

Schellman & Company, LLC
Certified Public Accountants
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
January 8, 2019



**ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER
ITS CERTIFICATION AUTHORITY OPERATIONS
DURING THE PERIOD DECEMBER 1, 2017, TO NOVEMBER 30, 2018**

January 8, 2019

Internet Security Research Group ("ISRG") operates the Certification Authority (CA) services known as Let's Encrypt and provides the following CA services:

- Subscriber registration
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of ISRG is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, and 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 provide only reasonable assurance with respect to ISRG's CA operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

ISRG management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ISRG management's opinion, in providing its CA services at its Salt Lake City, Utah, USA, and Denver, Colorado, USA, locations, throughout the period from December 1, 2017, to November 30, 2018, ISRG has:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control policies and practices in its:
 - [Certification Practice Statement \(v2.5\)](#); and
 - [Certificate Policy \(v2.2\)](#);
- Maintained effective controls to provide reasonable assurance that:
 - ISRG's Certification Practice Statement is consistent with its Certificate Policy;
 - ISRG provides its services in accordance with its Certificate Policy and Certification Practice Statement;
 - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
 - Subscriber information is properly authenticated (for the registration activities performed by ISRG);
 - Logical and physical access to CA systems and data is restricted to authorized individuals;
 - The continuity of key and certificate management operations is maintained;
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity; and

- Subscriber information was properly authenticated (for the registration activities performed by ISRG).

based on the [WebTrust Principles and Criteria for Certification Authorities - Version 2.1](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement
- Certificate Policy

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 and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Disaster Recovery, Backups, and 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 Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Issuance
- Certificate Distribution

- Certificate Revocation
- Certificate Validation

ISRG does not escrow its CA keys and does not provide subscriber key generation services, subscriber key management services, subscriber key storage and recovery services, integrated circuit card lifecycle management and certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

Joshua Aas
Executive Director
Internet Security Research Group
January 8, 2019

APPENDIX A – ISRG ROOT AND ISSUING CAs

Distinguished Name	Certificate Thumbprint (sha256)
Subject: C=US, O=Internet Security Research Group, CN=ISRG Root X1	96:BC:EC:06:26:49:76:F3:74:60:77:9A:CF:28:C5:A7:CF:E8:A3:C0:AA:E1:1A:8F:FC:EE:05:C0:BD:DF:08:C6
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1	BD:EE:0D:7C:8F:9C:27:8F:14:EA:9B:6A:4F:90:ED:66:5A:9F:56:DB:0A:56:B1:CD:DA:67:65:91:2F:39:8A:5E
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2	E4:EB:54:A7:FF:A5:52:EF:64:D8:E1:AE:33:8B:69:BE:90:9C:29:E6:AF:57:17:0A:2F:6F:44:DF:22:5E:5A:14
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	73:1D:3D:9C:FA:A0:61:48:7A:1D:71:44:5A:42:F6:7D:F0:AF:CA:2A:6C:2D:2F:98:FF:7B:3C:E1:12:B1:F5:68
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4	5D:E9:15:2B:ED:31:FA:05:15:DD:1F:C7:46:13:3F:13:27:56:2E:F7:2A:84:CF:2D:24:03:E7:48:A6:04:D0:D4