

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of Internet Security Research Group:

Scope

We have examined the [assertion by the management](#) of the Internet Security Research Group (“ISRG”) that in providing its Certification Authority (CA) services at its Salt Lake City, Utah, and Denver, Colorado, locations for its root and subordinate CA certificates:

- 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
- C=US O=Internet Security Research Group 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
- C=US O=Internet Security Research Group 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
- 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
- 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

for the program known as Let’s Encrypt during the period from December 16, 2016, to December 15, 2017, management of 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 (v2.0); and
 - Certificate Policy (v2.0);
- 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;
 - Logical and physical access to CA systems and data was restricted to authorized individuals;
 - The continuity of key and certificate management operations was maintained; and
 - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity.

based on the [AICPA/CPA Canada Trust Services Principles and Criteria for Certification Authorities Version 2.0 \(“WebTrust for Certification Authorities Principles and Criteria”\)](#).

ISRG’s Responsibilities

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

Independent Certified Public Accountant's Responsibilities

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ISRG's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy 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 and information privacy 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.

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.

Emphasis on a Matter

ISRG has disclosed that its Certificate Authority Authorization (CAA) checking algorithm was modified on September 14, 2017 to meet the new CAA checking rules that were added to the Baseline Requirements and went into effect on September 8, 2017.

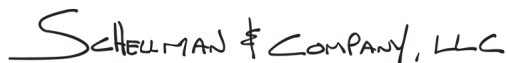
Opinion

In our opinion, for the period from December 16, 2016, to December 15, 2017, ISRG's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the [WebTrust for Certification Authorities Principles and Criteria](#).

The WebTrust seal of assurance for Certification Authorities ISRG's website constitutes a symbolic representation of the content of this report and it is not intended, nor should be construed, to update this report or provide any additional assurance.

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 external registration authorities, individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities, individual subscriber and relying party locations.

This report does not include any representation as to the quality of ISRG's services beyond those covered by the [WebTrust for Certification Authorities Principles and Criteria](#), nor the suitability of any of ISRG's services for any customer's intended purpose.



Schellman & Company, LLC
Certified Public Accountants
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
January 25, 2018



ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM DECEMBER 16, 2016, TO DECEMBER 15, 2017

January 25, 2018

The Internet Security Research Group (ISRG) operates as a Certification Authority (CA) for its root and subordinate CA certificates:

- 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
- C=US O=Internet Security Research Group 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
- C=US O=Internet Security Research Group 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
- 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
- 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

for the program known as Let's Encrypt. ISRG provides the following CA services:

- Certificate renewal
- Certificate issuance
- Certificate distribution (using online repository)
- Certificate revocation
- Certificate status information processing (using online repository)

Management of ISRG is responsible for establishing and maintaining effective controls over its CA operations, including service integrity (including key and certificate life cycle management controls), and CA environmental 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.

Management has assessed the controls over its CA operations. Based on that assessment, in ISRG management's opinion, in providing its CA services at its Salt Lake City, Utah, and Denver, Colorado, locations ISRG, during the period from December 16, 2016, to December 15, 2017:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control policies and practices in its
 - Certification Practice Statement (v2.0); and

- Certificate Policy (v2.0);
- 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;
 - Logical and physical access to CA systems and data was restricted to authorized individuals;
 - The continuity of key and certificate life cycle management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the [AICPA/CPA Canada Trust Services Principles and Criteria for Certification Authorities Version 2.0 \("WebTrust for Certification Authorities Principles and Criteria"\)](#) including the following:

CA Business Practices Disclosure

- *CA Business Practices Management*
 - Certification Practice Statement Management
 - Certificate Policy 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
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

Service Integrity

- *Key Life Cycle Management Controls*
 - CA Key Generation
 - CA Key Storage, Backup, and Recovery
 - Public Key Distribution

- Key Usage
- Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- *Certificate Life Cycle Management Controls*
 - Certificate Issuance
 - Certificate Distribution (using an online certificate management system)
 - Certificate Revocation
 - Certificate Validation

In addition to the above, Management has disclosed that its Certificate Authority Authorization (CAA) checking algorithm was modified on September 14, 2017 to meet the new CAA checking rules that were added to the Baseline Requirements and went into effect on September 8, 2017.



Joshua Aas
Executive Director
The Internet Security Research Group