

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of Internet Security Research Group (ISRG):

Scope

We have examined ISRG [management's assertion](#) that for its Certification Authority (CA) operations at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, throughout the period September 1, 2019, to August 31, 2020, 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 \(v2.9\)](#); and
 - [Certificate Policy \(v2.4\)](#)
- Maintained effective controls to provide reasonable assurance that:
 - ISRG's Certification Practice Statement is consistent with its Certificate Policy; and
 - ISRG 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; and
 - Subscriber information is properly authenticated (for the registration activities performed by ISRG)
- 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 [WebTrust Principles and Criteria for Certification Authorities - Version 2.2](#) (herein referred to as the "WebTrust for Certification Authorities").

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.

ISRG does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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, 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.

Emphasis on Matters

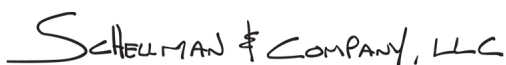
ISRG disclosed the following matters during the review period:

- ISRG publicly disclosed an incident on February 29, 2020, in which a bug was found in Boulder, its Let's Encrypt CA software, whereby the application checked for CAA records at the time it validated a subscriber's control of a domain name and relied on the same validation without checking for the presence of a CAA record on a subsequent certificate request of the same domain name if occurring within 30 days of the initial validation. The issue was confirmed and fixed on February 29, 2020, and Let's Encrypt halted issuance until a fix was deployed that re-enabled issuance.
- ISRG publicly disclosed an incident on June 8, 2020, in which its Let's Encrypt OCSP signing certificate expired four (4) days prior on June 4, 2020. During the period that it was expired, but not replaced, TLS clients building chains to ISRG Root X1 would experience OCSP validation errors if checking OCSP and validating the signing certificate. ISRG disclosed a design issue with an internal tool used to generate OCSP responses for their intermediate signing certificate. ISRG issued a fix to generate a new OCSP signing certificate on June 9, 2020, and the incident was resolved.

During our assessment, Schellman performed testing of certificate issuance, on a sample basis, and noted that there were no certificate deficiencies identified in any of the samples tested. As a result, our opinion is not modified with respect to these matters.

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 Centennial, 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.



Schellman & Company, LLC
Certified Public Accountants
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
October 2, 2020

**ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES
AND ITS CONTROLS OVER ITS CERTIFICATION AUTHORITY OPERATIONS
DURING THE PERIOD SEPTEMBER 1, 2019, TO AUGUST 31, 2020**

Internet Security Research Group (ISRG) operates the Certification Authority (CA) services known as Let's Encrypt for its root and subordinate CA certificates as listed in Appendix A 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 Certification Authority 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 Centennial, Colorado, USA, locations, throughout the period September 1, 2019, to August 31, 2020, 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 \(v2.9\)](#); and
 - [Certificate Policy \(v2.4\)](#)
- Maintained effective controls to provide reasonable assurance that:
 - ISRG's Certification Practice Statement is consistent with its Certificate Policy; and
 - ISRG 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; and
 - Subscriber information is properly authenticated (for the registration activities performed by ISRG)
- 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 [WebTrust Principles and Criteria for Certification Authorities - Version 2.2](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

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, Maintenance, and Change Management
- 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Certificate Lifecycle 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.

During the course of the assessment, ISRG disclosed the following matters during the review period:

- ISRG publicly disclosed an incident on February 29, 2020, in which a bug was found in Boulder, its Let's Encrypt CA software, whereby the application checked for CAA records at the time it validated a subscriber's control of a domain name and relied on the same validation without checking for the presence of a CAA record on a subsequent certificate request of the same domain name if occurring within 30 days of the initial validation. The issue was confirmed and fixed on February 29, 2020, and Let's Encrypt halted issuance until a fix was deployed that re-enabled issuance.
- ISRG publicly disclosed an incident on June 8, 2020, in which its Let's Encrypt OCSP signing certificate expired four (4) days prior on June 4, 2020. During the period that it was expired, but not replaced, TLS clients building chains to ISRG Root X1 would experience OCSP validation errors if checking OCSP and validating the signing certificate. ISRG disclosed a design issue with an internal tool used to generate OCSP responses for their intermediate signing certificate. ISRG issued a fix to generate a new OCSP signing certificate on June 9, 2020, and the incident was resolved.

Joshua Aas
Executive Director
Internet Security Research Group
October 2, 2020

APPENDIX A – ISRG ROOT AND ISSUING CAs

Distinguished Name	Certificate SHA-256 Fingerprint
Subject: C=US, O=Internet Security Research Group, CN=ISRG Root X1	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1	BDEE0D7C8F9C278F14EA9B6A4F90ED665A9F56DB0A56B1CDDA6765912F398A5E
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2	E4EB54A7FFA552EF64D8E1AE338B69BE909C29E6AF57170A2F6F44DF225E5A14
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	731D3D9CFAA061487A1D71445A42F67DF0AFCA2A6C2D2F98FF7B3CE112B1F568
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4	5DE9152BED31FA0515DD1FC746133F1327562EF72A84CF2D2403E748A604D0D4
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1	7FDCE3BF4103C2684B3ADBB5792884BD45C75094C217788863950346F79C90A3
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2	EC0C6CA496A67A13342FEC5221F68D4B3E53B1BC22F6E4BCCC9C68F0415CDEA4
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4	A74B0C32B65B95FE2C4F8F098947A68B695033BED0B51DD8B984ECAE89571BB6