schellman

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of Internet Security Research Group:

We have examined the assertion by the management of the Internet Security Research Group ("ISRG") that in providing its SSL Certification Authority (CA) services at its Salt Lake City, Utah, and Denver, Colorado, locations for its root CAs:

- ISRG Root X1
- Let's Encrypt Authority X1
- Let's Encrypt Authority X2
- Let's Encrypt Authority X3
- Let's Encrypt Authority X4

for the program known as Let's Encrypt during the period from December 16, 2015, to December 15, 2016, management of ISRG has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
    - The Certificate Policy ("CP") and/or Certificate Practice Statement ("CPS") are available on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647;
    - Subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
    - 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 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
    - Network and Certificate System Security Requirements set forth by the CA/Browser Forum are met.

based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.

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

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 SSL certificate life cycle management business practices and its controls over key and SSL 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.

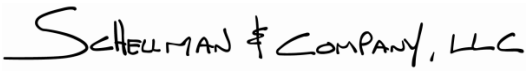
In our opinion, during the period from December 16, 2015, to December 15, 2016, ISRG's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for Certification Authorities on ISRG's website 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.

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 AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2, nor the suitability of any of ISRG's services for any customer's intended purpose.



Schellman & Company, LLC
Certified Public Accountants
Tampa, Florida
February 7, 2017

ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS SSL CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM DECEMBER 16, 2015, TO DECEMBER 15, 2016

February 7, 2017

Management has assessed the controls over its SSL CA operations. Based on that assessment, in ISRG management's opinion, in providing its SSL CA services at its Salt Lake City, Utah, and Denver, Colorado, locations, for its root CAs:

- ISRG Root X1
- Let's Encrypt Authority X1
- Let's Encrypt Authority X2
- Let's Encrypt Authority X3
- Let's Encrypt Authority X4

for the program known as Let's Encrypt, during the period from December 16, 2015, to December 15, 2016, ISRG has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
    - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647;
    - Subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
    - 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 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
    - Network and Certificate System Security Requirements set forth by the CA/Browser Forum are met

    based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.

Joshua Aas
Executive Director