REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

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

We have examined ISRG’s 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, 2020, to August 31, 2021, 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 (v4.1); and
  - Certificate Policy (v3.1);
- 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); and
- 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 2.2.1.

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 perform key transportation or key migration services, and does not provide subscriber key generation services, certificate rekeys, subscriber key management services, subscriber key storage and recovery services, integrated circuit card lifecycle management, certificate suspension, and cross certificate services. Accordingly, our assertion does not extend to controls that would address those criteria.

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. The nature, timing, and extent of the procedures selected depend on our judgement, 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.

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.

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

**Emphasis of Matters**

ISRG has disclosed that during the period September 1, 2020, to August 31, 2021, the following incidents were identified and disclosed to the Web PKI community as follows:

- **Mozilla Bug ID 1666047:** On September 8, 2020, ISRG was made aware that the CA served OCSP responses older than three and one half (3.5) days for 268 certificate serial numbers. From September 12, 2020, ISRG served OCSP responses older than three and one half (3.5) days for an additional 34 certificate serial numbers. None of the OCSP responses were served beyond their validity period. The maximum age an OCSP response ever reached was five (5) days. For OCSP responses with a seven (7)-day validity period, the Microsoft Root Program specifies that updated responses be available within three and one half (3.5) days and the CA/B Forum Baseline Requirements specify four (4) days. ISRG was notified of the problem by an alert on elevated error-level logs. ISRG found that the errors were caused by a recent change to their RPC system that, in a certain error case, caused a particular column in its certificate status table to have a value of “0” for a specific empty field rather than either the expected value or NULL. ISRG collected serials and last-update timestamp information for affected entries and enacted a temporary manual plan for continued remediation of these entries. A Boulder CA software release was deployed to production on September 10, 2020, ensuring no future erroneous values would be added to the database.

- **Mozilla Bug ID 1684112:** On December 22, 2020, during a quarterly review of the CA/B Forum baseline requirements, ISRG noticed that it was not compliant with section 5.4.1.2.5. Let’s Encrypt logs an audit log event when OCSP is signed upon initial certificate issuance. Subsequent updates to the OCSP response throughout a certificate’s 90-day lifetime are not logged as audit log events. The CA/B Forum Baseline Requirements section 5.4.1.2.5 requires these events be logged as an audit level event and stored for a period of time. Revocation logs are properly logged as audit logs and not affected by this incident. ISRG implemented a fix to their Boulder CA Software to implement the logging on January 31, 2021.

- **Mozilla Bug IDs 1715455 and 1715672:** On June 8, 2021, ISRG was made aware that it was issuing certificates that were valid for 90 days plus one (1) second. ISRG historically issued certificates valid for 90 days by taking the issuance time and adding exactly 2,160 hours to yield the certificate’s “not after” date; however, RFC 5280 defines the validity period of a certificate as being the duration between the “not before” and “not after” timestamps, inclusive. This inclusivity means that the certificates were issued as being valid for 90 days plus one (1) second as described above. ISRG issued an update to the CA Boulder Software to fix the issue so that all future certificates issued were valid for 90 days. ISRG determined that revoking the affected certificates would not benefit the Web PKI and CA ecosystem and failing to revoke certificates within a specific timeframe would be a violation of the Baseline Requirements and its own CP/CPS.

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 14, 2021
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, 2020, to August 31, 2021, 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 (v4.1); and
  - Certificate Policy (v3.1);
- 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); and
- 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 2.2.1, 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
Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

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

During the assessment, ISRG disclosed that during the period September 1, 2020, to August 31, 2021, the following incidents were identified and disclosed to the Web PKI community as follows:

- Mozilla Bug ID 1666047: On September 8, 2020, ISRG was made aware that the CA served OCSP responses older than three and one half (3.5) days for 268 certificate serial numbers. From September 12, 2020, ISRG served OCSP responses older than three and one half (3.5) days for an additional 34 certificate serial numbers. None of the OCSP responses were served beyond their validity period. The maximum age an OCSP response ever reached was five (5) days. For OCSP responses with a seven (7)-day validity period, the Microsoft Root Program specifies that updated responses be available within three and one half (3.5) days and the CA/B Forum Baseline Requirements specify four (4) days. ISRG was notified of the problem by an alert on elevated error-level logs. ISRG found that the errors were caused by a recent change to their RPC system that, in a certain error case, caused a particular column in its certificate status table to have a value of "0" for a specific empty field rather than either the expected value or NULL. ISRG collected serials and last-update timestamp information for affected entries and enacted a temporary manual plan for continued remediation of these entries. A Boulder CA software release was deployed to production on September 10, 2020, ensuring no future erroneous values would be added to the database.

- Mozilla Bug ID 1684112: On December 22, 2020, during a quarterly review of the CA/B Forum baseline requirements, ISRG noticed that it was not compliant with section 5.4.1.2.5. Let’s Encrypt logs an audit log event when OCSP is signed upon initial certificate issuance. Subsequent updates to the OCSP response throughout a certificate’s 90-day lifetime are not logged as audit log events. The CA/B Forum Baseline Requirements section 5.4.1.2.5 requires these events be logged as an audit level event and stored for a period of time. Revocation logs are properly logged as audit logs and not affected by this incident. ISRG implemented a fix to their Boulder CA Software to implement the logging on January 31, 2021.

- Mozilla Bug IDs 1715455 and 1715672: On June 8, 2021, ISRG was made aware that it was issuing certificates that were valid for 90 days plus one (1) second. ISRG historically issued certificates valid for 90 days by taking the issuance time and adding exactly 2,160 hours to yield the certificate’s “not after” date; however, RFC 5280 defines the validity period of a certificate as being the duration between the “not before” and “not after” timestamps, inclusive. This inclusivity means that the certificates were issued as being valid for 90 days plus one (1) second as described above. ISRG issued an update to the CA Boulder Software to fix the issue so that all future certificates issued were valid for 90 days. ISRG determined that revoking the affected certificates would not benefit the Web PKI and CA ecosystem and failing to revoke certificates within a specific timeframe would be a violation of the Baseline Requirements and its own CP/CPS.

Incidents not relevant to the assessed criteria are included in Appendix B.

Joshua Aas
Executive Director
Internet Security Research Group
October 14, 2021
APPENDIX A – ISRG ROOT AND ISSUING CAs

<table>
<thead>
<tr>
<th>Distinguished Name</th>
<th>Certificate SHA-256 Fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1</td>
<td>96BCEC06264976F37460779ACF28C5A7CF8E8A3C0AE11A8FFCEE05C0BDDF08C6</td>
</tr>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X2</td>
<td>69729B8E15A86EFC177A57AFB7171DFC64ADD28C2FCA8CF1507E34453CCB1470</td>
</tr>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X2</td>
<td>8B05B68CC6599E5ED0FB38F2C942FBFD200E6F2FF9F85D63C6994EF5E0B20701</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3*</td>
<td>731D3D9CFAA061487A1D71445A42F67DF0AFCA2A6C2D2F98FF7B3CE112B1F568</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X4</td>
<td>5DE9152BED31FA0515DD1FC746133F1327562EF72A84CFD2D403E748A604D0D4</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = R3</td>
<td>67ADD1166B020AE61B8F5FC96813C04C2AA58996079686572A3C7E737613DFD</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = R4</td>
<td>1A07529A8B3F01D231DFAD2ABDF7189920BB65CD7E03C59FA82272533355B74</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = E1</td>
<td>4694E30379059DF18BE52124305E606FC590705EB21076CE113954B60517CDA</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = E2</td>
<td>BACDE0463053CE1D62F8E74370BBAE79D4FCAF19FC07643AEF195E6A59BD578</td>
</tr>
</tbody>
</table>

The following certificates were signed by IdenTrust for ISRG.

<table>
<thead>
<tr>
<th>Distinguished Name</th>
<th>Certificate SHA-256 Fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1</td>
<td>6D99FB265EB1C53B3744765FCBC648F3CD8E1BFFAFD4C2F99BD47CF7FF1C24F</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X1</td>
<td>7FDCE3BF4103C2684B3ADBB5792884BD45C75094C217788863950346F79C90A3</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X1</td>
<td>23D29B9707396BCCA317F9EF1B1E6A626C4E481283CD85F74A516FF6CAB997ED</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X2</td>
<td>EC0C6CA496A67A13342FEC5221F68D4B3E53B1BC22F6E4BCC9C68F0415CDEA4</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X2</td>
<td>2F45659D64DC74CCEC9E2A4290715828F95FA8CC7A6C8800D3968F14DFCF1DB7</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3</td>
<td>25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D</td>
</tr>
</tbody>
</table>
The following incident(s) occurred prior to the audit period and disclosed because the associated Mozilla Bugzilla ticket was open at some point during the audit period.

<table>
<thead>
<tr>
<th>Mozilla Bugzilla ID</th>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1619047</td>
<td>2020.02.28</td>
<td>CAA Rechecking bug</td>
</tr>
</tbody>
</table>