INTERNET SECURITY RESEARCH GROUP
(LET’S ENCRYPT)

WEBTRUST FOR CERTIFICATION AUTHORITIES REPORT

SEPTEMBER 1, 2022, TO AUGUST 31, 2023

Proprietary & Confidential
Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Independent Accountant Report</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Management’s Assertion</td>
<td>6</td>
</tr>
<tr>
<td>A</td>
<td>ISRG’s Root and Issuing CAS</td>
<td>10</td>
</tr>
</tbody>
</table>
SECTION 1
INDEPENDENT ACCOUNTANT REPORT
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, for its root and subordinate CA certificates as listed in Appendix A, ISRG has:

- Disclosed its business, key and certificate lifecycle management, and CA environmental control practices in its:
  - Combined Certificate Policy and Certification Practice Statement (v5.1, dated May 16, 2023)
  - Combined Certificate Policy and Certification Practice Statement (v5.0, dated May 5, 2023)
  - Certificate Policy (v3.4, dated March 10, 2023)
  - Certification Practice Statement (v4.5, dated March 10, 2023)
  - Certification Practice Statement (v4.4, dated September 28, 2022)
  - Certification Practice Statement (v4.3, dated May 6, 2022)

- Maintained effective controls to provide reasonable assurance that:
  - 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.
  - 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.
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

throughout the period September 1, 2022, to August 31, 2023, based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2 for the relevant systems and processes used in the issuance of all certificates that assert policy object identifier 2.23.140.1.2.

ISRG does not escrow its CA keys and does not provide subscriber key generation services, subscriber key management services, certificate rekeys, subscriber key storage and recovery services, integrated circuit card lifecycle management, certificate suspension, or subordinate CA and cross certificate lifecycle management services. Accordingly, our examination did not extend to controls that would address those criteria.
Certification Authority’s Responsibilities

ISRG’s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Practitioner’s Responsibilities

Our responsibility is to express an opinion on ISRG 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 in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, management’s assertion is fairly stated, and, accordingly, included:

- Obtaining an understanding of ISRG’s key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance, and operation of systems integrity.
- Selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices.
- Testing and evaluating the operating effectiveness of the controls.
- Performing such other procedures as we considered necessary in the circumstances.

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.

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct Established by the AICPA and the International Ethics Standards Board for Accountants’ Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Control 1, Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services Engagements and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, ISRG 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 Centennial, Colorado, USA, locations, nor the suitability of any of ISRG’s services for any customer’s intended purpose.

Other Matters

Without modifying our opinion, we noted the following other matters during our procedures:

<table>
<thead>
<tr>
<th>Matter Topic</th>
<th>Matter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Certificates issued to Elliptic Curve Debian Weak Keys</td>
</tr>
<tr>
<td>2</td>
<td>Incomplete and Inconsistent CRLs</td>
</tr>
<tr>
<td>3</td>
<td>Delayed revocation for removed gTLD</td>
</tr>
<tr>
<td>Matter Topic</td>
<td>Matter Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>4</td>
<td>End Entity CRLs Not Reissued On Time</td>
</tr>
<tr>
<td>5</td>
<td>Duplicate Serial Numbers</td>
</tr>
</tbody>
</table>

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.

While ISRG disclosed its reported issues in Bugzilla during the period September 1, 2022, to August 31, 2023, Schellman has noted only those disclosures relevant to the CAs enumerated in Appendix A and applicable to the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

**Use of the WebTrust Seal**

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  
4010 W Boy Scout Blvd  
Suite 600  
Tampa, Florida, United States  
November 8, 2023
SECTION 2
MANAGEMENT’S ASSERTION
Internet Security Research Group (ISRG) operates the 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 disclosures on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 only provide 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 Centennial, Colorado, USA, locations, ISRG has:

- Disclosed its business, key and certificate lifecycle management, and CA environmental control practices in its:
  - Combined Certificate Policy and Certification Practice Statement (v5.1, dated May 16, 2023)
  - Combined Certificate Policy and Certification Practice Statement (v5.0, dated May 5, 2023)
  - Certificate Policy (v3.4, dated March 10, 2023)
  - Certification Practice Statement (v4.5, dated March 10, 2023)
  - Certification Practice Statement (v4.4, dated September 28, 2022)
  - Certification Practice Statement (v4.3, dated May 6, 2022)

- Maintained effective controls to provide reasonable assurance that:
  - 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.
  - 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.
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.
throughout the period September 1, 2022, to August 31, 2023, based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2 for the relevant systems and processes used in the issuance of all certificates that assert policy object identifier 2.23.140.1.2, including the following:

**CA Business Practices Disclosure**
- Certification Practice Statement (CPS)
- Certificate Policy (CP)

**CA Business Practices Management**

**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

**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 Compromise
- CA Cryptographic Hardware Lifecycle Management

**Certificate Lifecycle Management Controls**
- Subscriber Registration
- Certificate Renewal
- 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, certificate rekeys, subscriber key storage and recovery services, integrated circuit card lifecycle management, certificate suspension, or subordinate CA and cross certificate lifecycle management services. Accordingly, our assertion does not extend to controls that would address those criteria.
ISRG has disclosed the following matters publicly on Mozilla’s Bugzilla platform. These matters were included below due to being open during the period September 1, 2022, to August 31, 2023.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Summary</th>
<th>Opened</th>
<th>Closed</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1789521</td>
<td>Certificates issued to Elliptic Curve Debian Weak Keys</td>
<td>2022-09-06</td>
<td>2022-10-26</td>
<td>Fixed</td>
</tr>
<tr>
<td>1793114</td>
<td>Incomplete and Inconsistent CRLs</td>
<td>2022-09-30</td>
<td>2022-11-26</td>
<td>Fixed</td>
</tr>
<tr>
<td>1795483</td>
<td>Delayed revocation for removed gTLD</td>
<td>2022-10-14</td>
<td>2022-11-30</td>
<td>Fixed</td>
</tr>
<tr>
<td>1799755</td>
<td>End Entity CRLs Not Reissued On Time</td>
<td>2022-11-08</td>
<td>2022-12-12</td>
<td>Fixed</td>
</tr>
<tr>
<td>1838667</td>
<td>Duplicate Serial Numbers</td>
<td>2023-06-15</td>
<td>2023-07-05</td>
<td>Fixed</td>
</tr>
</tbody>
</table>

Joshua Aas  
Executive Director  
Internet Security Research Group  
November 8, 2023
APPENDIX A

ISRG’S ROOT AND ISSUING CAs
### ISRG’s 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>96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6</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>8B05B68CC659E5ED0FCB38F2C942FBFD200E6F2FF9F85D63C6994EF5E0B2701</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X3</td>
<td>731D3D9CFAA061487A1D7145A42F67DF0AFC2A62C2D2F987F7B3CE112B1F568</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X4</td>
<td>5DE9152BED31FA0515DD1FC746133F1327562EF72A84CF2D2403E748A604D0D4</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = R3</td>
<td>67ADD1166B020AE61B8F5FC96813C04C2AA588996079686572A3C7E737613FD</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = R4</td>
<td>1A07529A8B3F01D231DFAD2ABDF71899200BB65CD7E03C59FA82272533355B74</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = E1</td>
<td>46494E30379059DF18BE52124305E606FC59070E5B21076CE113954B60517CD</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = E2</td>
<td>BACDE0463053CE1D62F8BE74370BBAE79D4FCAF19FC07643AEF195E6A59BD578</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>6D99FB265EB1C5B3744765FBCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X1</td>
<td>7FDCE3BF4103C2684B3ADB5792884BD45C75094C217788863950346F79C90A</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X1</td>
<td>23D29B9707396BCCA3179F9EF1B1E6A626C4E481283CD85F74A516FF6CAB997ED</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X2</td>
<td>EC0C6CA496A67A13342FEC5221F68D4B3E53B1BC22F6E4BCCC9C68F0415CDEA4</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X2</td>
<td>2F45659D64DC744CCCEC9E2A4290715828F95FA8CC7A6C8800D3968F14DFCF1DB7</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X3</td>
<td>25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>Certificate SHA-256 Fingerprint</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = Let’s Encrypt Authority X4</td>
<td>A74B0C32B65B95FE2C4F8F098947A68B695033BED0B51DD8B984ECAE89571BB6</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = R3</td>
<td>FEE765DA4CACF53C71AF202F89F3612420FD930D804E204FEEFEC9D78084BB7B</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = R3</td>
<td>730C1BDCD85F57CE5DC0BBA733E5F1BA5A925B2A771D640A26F7A454224DAD3B</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = R4</td>
<td>8E510575F07A97D5FADA3BFDA6187E03E77D3392318457E8718A9D28B43396B</td>
</tr>
<tr>
<td>Subject: C = US, O = Let’s Encrypt, CN = R4</td>
<td>5A8F16FDA448D783481CCA57A2428D174DAD8C60943CEB28F661AE31FD39A5FA</td>
</tr>
</tbody>
</table>