INTERNET SECURITY RESEARCH GROUP
(LET'S ENCRYPT)

WEBTRUST FOR CERTIFICATION AUTHORITIES –
SSL BASELINE WITH NETWORK SECURITY REPORT

SEPTEMBER 1, 2022, TO AUGUST 31, 2023

Attestation and Compliance Services

TABLE OF CONTENTS

SECTION 1

INDEPENDENT ACCOUNTANT REPORT

REPORT OF THE INDEPENDENT ACCOUNTANT

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

Scope

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, for its root and subordinate CA certificates as listed in Appendix A, ISRG has:

- Disclosed its SSL certificate lifecycle business management 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)
  - Certificate Policy (v3.3, dated May 6, 2022)
  - 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)

  Including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Let's Encrypt website, and provided such services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL 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.
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

Throughout the period September 1, 2022, to August 31, 2023, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.6 for the relevant systems and processes used in the issuance of all certificates that assert policy object identifier 2.23.140.1.2..

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 – SSL Baseline with Network Security – v2.6.

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 SSL certificate lifecycle management practices, including its relevant controls over the issuance and revocation of SSL certificates, and obtaining an understanding of ISRG's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- 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:

Matter Topic		Matter Description
1	Certificates issued to Elliptic Curve Debian Weak Keys	Mozilla Bug ID 1789521: On 2022-07-08, Let's Encrypt was notified regarding a vulnerability which impacted Elliptic Curve keys in affected versions of OpenSSL on the Debian operating system. During the discovery phase of the investigation, the Let's Encrypt team discovered that only two certificates were issued matching the SPKI of the weak keys. The Let's Encrypt staff took actions to block the affected keys from being used and has stopped issuing certificates with Debian weak ECDA keys. The ticket was closed on 2022-10-26..
2	Incomplete and Inconsistent CRLs	Mozilla Bug ID 1793114: On 2022-09-29, Let's Encrypt became aware that incomplete CRLs were being issued and that inconsistent CRL partitions were being generated, with each shard containing a different subset of the revoked serial numbers each time the CRL was issued. Let's Encrypt staff resolved the incomplete CRLs by updating the CRL Updater's "certificateLifetime" configuration to the correct value of "2160h". Additionally, and to prevent further occurrences, Let's Encrypt made changes to the CRL Updater's logic and deployed additional monitoring to ensure certificates remain in the same shard for every generation of CRLs produced through expiration. This ticket was closed on 2022-11-26.
3	Delayed revocation for removed gTLD	Mozilla Bug ID 1795483: On 2022-10-14, Let's Encrypt became aware that three unexpired certificates which were associated with a deprecated ICANN gTLD domain were not revoked under that gTLD within five days. Automation to ensure that deprecated gTLD domains are added to a high-risk and forbidden issuance listing were designed to scan the preceding 72 hours' worth of issued certificates. As the last issuance under the deprecated domain occurred more than 72 hours earlier, the automation did not detect the previously issued certificates for recently removed gTLDs. Let's Encrypt revoked the certificates in question and updated internal documentation regarding the handling of gTLD removal to include searching for and administratively revoking any unexpired certificates under the deprecated gTLD. This ticket was closed on 2022-11-30.
4	End Entity CRLs Not Reissued On Time	Mozilla Bug ID 1799755: On 2022-11-08, Let's Encrypt was notified that for a period of 11 days from 2022-10-27, through 2022-11-08, new CRLs were not issued for two intermediate certificates. Although the revoked certificates for the two affected intermediate certificates were not reflected in the CRLs, up-to-date certificate revocation status was available via OCSP for the duration of this incident. During the investigation, Let's Encrypt staff identified errors within the CRL generation and publication process. Let's Encrypt staff made configuration changes to the CRL publication pipeline and added additional CRL publication monitoring to resolve this issue and to prevent it from re-occurring in the future. This ticket was closed on 2022-12-12.

Matter Topic		Matter Description
5	Duplicate Serial Numbers	Mozilla Bug ID 1838667: On 2023-06-15, Let's Encrypt was notified that duplicate serial numbers were issued, which affected 645 serial numbers. Let's Encrypt deployed a certificate profile configuration change that removed the embedded ISRG CPS OID and related CPS URL from the Certificate Policies extension of newly issued end-entity certificates. For a few moments during the deployment, it was possible to issue a precertificate and final certificate with the same serial number but mismatched Certificate Policies extensions. This occurred when the respective issuance requests were routed to different backend instances with different configured certificate profiles. Let's Encrypt staff revoked all affected certificates which forced all compliant clients to renew immediately, which resolved the issue. Additionally, and to prevent further occurrences, Let's Encrypt introduced a new check which would ensure the correspondence between the precertificate and the proposed final certificate and runs as a pre-issuance check. This ticket was closed on 2023-07-05.

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, we have noted only those disclosures relevant to the CAs enumerated in Appendix A and applicable to the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.6.

Use of the WebTrust Seal

ISRG's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security 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

Schellman & Company, LLC
4010 W Boy Scout Blvd
Suite 600
Tampa, Florida, United States
November 8, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

Internet Security Research Group (ISRG) operates the CA services known as Let's Encrypt for its root and subordinate CA certificates as listed in Appendix A and provides SSL CA services.

The management of ISRG is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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 SSL CA services. Based on that assessment, in providing its SSL Certificate Authority ("CA") services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, ISRG has:

- Disclosed its SSL certificate lifecycle management business 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)
  - Certificate Policy (v3.3, dated May 6, 2022)
  - 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)

  Including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Let's Encrypt website, and provided such services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL 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.
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

Throughout the period September 1, 2022, to August 31, 2023, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – v2.6 for the relevant systems and processes used in the issuance of all certificates that assert policy object identifier 2.23.140.1.2.

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.

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

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

Distinguished Name	Certificate SHA-256 Fingerprint
Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X2	69729B8E15A86EFC177A57AFB7171DFC64ADD28C2FCA8CF1507E34453CCB1470
Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X2	8B05B68CC659E5ED0FCB38F2C942FBFD200E6F2FF9F85D63C6994EF5E0B02701
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 = R3	67ADD1166B020AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD
Subject: C = US, O = Let's Encrypt, CN = R4	1A07529A8B3F01D231DFAD2ABDF71899200BB65CD7E03C59FA82272533355B74
Subject: C = US, O = Let's Encrypt, CN = E1	46494E30379059DF18BE52124305E606FC59070E5B21076CE113954B60517CDA
Subject: C = US, O = Let's Encrypt, CN = E2	BACDE0463053CE1D62F8BE74370BBAE79D4FCAF19FC07643AEF195E6A59BD578

The following certificates were signed by IdenTrust for ISRG.

Distinguished Name	Certificate SHA-256 Fingerprint
Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1	6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F
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 X1	23D29B9707396BCCA317F9EF1B1E6A626C4E481283CD85F74A516FF6CAB997ED
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 X2	2F45659D64DC74CCEC9E2A4290715828F95FA8CC7A6C8800D3968F14DFCF1DB7
Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3	25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D

Distinguished Name	Certificate SHA-256 Fingerprint
Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X4	A74B0C32B65B95FE2C4F8F098947A68B695033BED0B51DD8B984ECAE89571BB6
Subject: C = US, O = Let's Encrypt, CN = R3	FEE765DA4CACF53C71AF202F89F3612420FD930D804E204FEEEFC9D78084BB7B
Subject: C = US, O = Let's Encrypt, CN = R3	730C1BDCD85F57CE5DC0BBA733E5F1BA5A925B2A771D640A26F7A454224DAD3B
Subject: C = US, O = Let's Encrypt, CN = R4	8E510575F07A97D5FADA3BFDA6187E03E77D3392318457EA8718A9D28B43396B
Subject: C = US, O = Let's Encrypt, CN = R4	5A8F16FDA448D783481CCA57A2428D174DAD8C60943CEB28F661AE31FD39A5FA