INTERNET SECURITY RESEARCH GROUP (LET'S ENCRYPT)

WEBTRUST FOR CERTIFICATION AUTHORITIES REPORT

SEPTEMBER 1, 2023, TO AUGUST 31, 2024

Attestation and Compliance Services

Table of Contents

SECTION I

INDEPENDENT ACCOUNTANT'S REPORT

schellman

REPORT OF THE INDEPENDENT ACCOUNTANT

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

Scope

We have examined ISRG's management 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 enumerated in Appendix A, ISRG has:

- Disclosed its business, key and certificate lifecycle management, and CA environmental control practices within its:
    - Combined Certificate Policy and Certification Practice Statement (v5.3, dated March 22, 2024)
    - Combined Certificate Policy and Certification Practice Statement (v5.2, dated February 7, 2024)
    - Combined Certificate Policy and Certification Practice Statement (v5.1, dated May 16, 2023)
- 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, 2023, to August 31, 2024, 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 2.23.140.1.2.1.

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 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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. 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.

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	keyCompromise key blocking deviation from CP/CPS	During PMA review of the Let's Encrypt CP/CPS, they noted that Section 4.9.12 stated that "Successful revocation requests with a reason code of key Compromise will result in the affected key being blocked for future issuance and all currently valid certificates with that key will be revoked." However, this does not accurately describe Let's Encrypt's behavior. The ACME protocol supports three different kinds of revocation requests: those signed by the ACME account key of the Subscriber who originally requested the certificate, those signed by the ACME account key of a different Subscriber who has demonstrated control over all identifiers in the certificate, and those signed by the keypair represented by the certificate itself. Only the last of these actually demonstrates that the key has been compromised, and so we only block the key and revoke other certificates sharing that key when the revocation request was signed by the certificate

Matter Topic		Matter Description
		key itself. This behavior was and remains a deliberate choice, to prevent a potential DoS vector detailed below. ISRG has changed the language in their Let's Encrypt CP/CPS to reflect the actual behavior and are filing this incident to reflect the time in which their behavior was in violation of their CPS.

During our assessment, Schellman performed testing of certificate issuance, on a sample basis, and found 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 on Bugzilla during the period September 1, 2023, to August 31, 2024, 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 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

Schellman & Company, LLC
4510 Kenny Road, Suite 9,
Columbus, Ohio, United States
November 20, 2024

SECTION 2

MANAGEMENT'S ASSERTION

Management's Assertion

Internet Security Research Group ("ISRG") operates the Certification Authority ("CA") services known as Let's Encrypt for its CA certificates as enumerated 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 disclosures on its website, CA business practices management, CA environmental controls, CA 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 can only provide 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, ISRG has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices within its:
  - Combined Certificate Policy and Certification Practice Statement (v5.3, dated March 22, 2024)
  - Combined Certificate Policy and Certification Practice Statement (v5.2, dated February 7, 2024)
  - Combined Certificate Policy and Certification Practice Statement (v5.1, dated May 16, 2023)
- 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, 2023, to August 31, 2024, 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 2.23.140.1.2.1, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy and Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System 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, 2023, to August 31, 2024.

Bug ID	Summary	Opened	Closed	Resolution
1886876	keyCompromise key blocking deviation from CP/CPS	2024-03-21	2024-04-17	Fixed

Signed by:
Joshua Aas
0188B009C837485...
Joshua Aas
Executive Director
Internet Security Research Group
November 20, 2024

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 = E1	46494E30379059DF18BE52124305E606FC59070E5B21076CE113954B60517CDA
Subject: C = US, O = Let's Encrypt, CN = E2	BACDE0463053CE1D62F8BE74370BBAE79D4FCAF19FC07643AEF195E6A59BD578
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 = E5	5DFDB3CF31B26F23D87C09F3A0CEF642F64069A9FB7CFE29270BB5DC0F1E16BB
Subject: C = US, O = Let's Encrypt, CN = E5	E788D14B0436B5120BBEE3F15C15BADF08C1407FE72568A4F16F9151C380E1E3
Subject: C = US, O = Let's Encrypt, CN = E6	76E9E288AAFC0E37F4390CBF946AAD997D5C1C901B3CE513D3D8FADBABE2AB85
Subject: C = US, O = Let's Encrypt, CN = E6	065AB7D2A050F947587121765D8D070C0E1330D5798FAA42C2072749ED293762
Subject: C = US, O = Let's Encrypt, CN = E7	AEB1FD7410E83BC96F5DA3C6A7C2C1BB836D1FA5CB86E708515890E428A8770B
Subject: C = US, O = Let's Encrypt, CN = E7	54715420224C5B65BEED018DC3940D7338C577E322D5488F633D8C6A8FED61B2
Subject: C = US, O = Let's Encrypt, CN = E8	83624FD338C8D9B023C18A67CB7A9C0519DA43D11775B4C6CBDAD45C3D997C52
Subject: C = US, O = Let's Encrypt, CN = E8	AC1274542267F17B525535B5563BF731FEBB182533B46A82DC869CB64EB528C0
Subject: C = US, O = Let's Encrypt, CN = E9	FDE88F2D4F8913D3DC1664D5F8DE51E07FE2ABFED93B45ACAD5A29BFEBAA23FB
Subject: C = US, O = Let's Encrypt, CN = E9	4185DF97806C2BA76F1D79823F112FFA639A49CCDC990908102067AB6412B886
Subject: C = US, O = Let's Encrypt, CN = R10	9D7C3F1AA6AD2B2EC0D5CF1E246F8D9AE6CBC9FD0755AD37BB974B1F2FB603F3
Subject: C = US, O = Let's Encrypt, CN = R11	591E9CE6C863D3A079E9FABE1478C7339A26B21269DDE795211361024AE31A44
Subject: C = US, O = Let's Encrypt, CN = R12	131FCE7784016899A5A00203A9EFC80F18EBBD75580717EDC1553580930836EC
Subject: C = US, O = Let's Encrypt, CN = R13	D3B128216A843F8EF1321501F5DF52A5DF52939EE2C19297712CD3DE4D419354
Subject: C = US, O = Let's Encrypt, CN = R14	24D45AA9B8D6053D281F3842C8CC0C6C1AF7CCDFD42DD5C12F6A74FA9323F7A2

Distinguished Name	Certificate SHA-256 Fingerprint
Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1	6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F