Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

8001 Forsyth Blvd, Suite 900
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of Internet Security Research Group ("Let's Encrypt"):

Scope

We have examined Let's Encrypt's management's assertion, that in generating and protecting its Root CA key pairs ("Root CAs") enumerated in Attachment A, on September 3, 2025, in Utah, in the United States of America, Let's Encrypt has:

- followed the CA key generation and protection requirements in its Internet Security Research Group Combined Certificate Policy and Certification Practice Statement ("Let's Encrypt CP/CPS")
- included appropriate, detailed procedures and controls in the Root Key Generation Script ("Key Generation Script"), dated September 3, 2025
- maintained effective controls to provide reasonable assurance that the Let's Encrypt Root CA keys were generated and protected in conformity with the procedures described in the Let's Encrypt CP/CPS, and Key Generation Script
- performed, during the root key generation process, all procedures required by the Key Generation Script
- generated the CA keys in a physically secured environment as described in the Let's Encrypt CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the Let's Encrypt CP/CPS

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Certification Authority's Responsibilities

Let's Encrypt's management is responsible for these procedures and for maintaining effective controls based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Independent Accountant's Responsibilities

Our responsibility is to express an opinion about 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. 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. Our examination, included:

(1) obtaining an understanding of Let's Encrypt's documented plan of procedures to be performed for the generation of the CA key pairs for the Let's Encrypt Root CAs;
(2) reviewing the detailed CA key generation script for conformance with industry standard practices;
(3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
(4) physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on September 3, 2025 were in accordance with the Key Generation Script for the Root CAs; and
(5) performing such other procedures as we considered necessary in the circumstances.

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 relevant ethical requirements relating to the engagement.

Independent Accountant's Opinion

In our opinion, Let's Encrypt 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 Let's Encrypt's services other than its CA key generation operations in Utah, United States of America, nor the suitability of any of Let's Encrypt's services for any customer's intended purpose.

BDO USA, P.C.

September 30, 2025

ATTACHMENT A – IN-SCOPE CAs

Root CA Certificates				
Subject DN	**Subject Key Identifier**	**SHA256 Thumbprint**	**Valid From**	**Valid To**
CN = Root YE O = ISRG C = US	A3C8265A8EA14CD03563FC9B23C83AAE56F34F56	E14FFCAD5B0025731006CAA43A121A22D8E9700F4FB9CF852F02A708AA5D5666	9/3/2025	9/2/2045
CN = Root YR O = ISRG C = US	DEE75B60D0226D40287D3F0D01FEA4B552B45194	E57B7E6F150C419102E8D5C055729FF967B9D1A829BF00CEC89CA604EBF4A86F	9/3/2025	9/2/2045

Internet Security Research Group
548 Market St, PMB 77519
San Francisco, California 94104-5401

INTERNET SECURITY RESEARCH GROUP MANAGEMENT'S ASSERTION

Internet Security Research Group ("Let's Encrypt") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consisting of self-signed Root CAs, collectively known as the "Root CAs", as enumerated in Attachment A. The CAs will serve as Root CAs for client certificate services. In order to allow the CAs to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CAs' private signing keys. This helps assure the non-refutability of the integrity of the Root CAs key pairs, and in particular, the private signing keys.

Let's Encrypt management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in the Internet Security Research Group Combined Certificate Policy and Certification Practice Statement ("Let's Encrypt CP/CPS") and the Root Key Generation Ceremony Script ("Key Generation Script"), which are based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Let's Encrypt management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

Let's Encrypt management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the Root CAs, and for the CA environmental controls relevant to the generation and protection of its CA keys.

Let's Encrypt management has assessed the procedures and controls for the generation of the Root CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys enumerated in Attachment A, on September 3, 2025, in Utah, in the United States of America, Let's Encrypt has:

- followed the CA key generation and protection requirements in its Internet Security Research Group Combined Certificate Policy and Certification Practice Statement ("Let's Encrypt CP/CPS")

- included appropriate, detailed procedures and controls in the Root Key Generation Script ("Key Generation Script"), dated September 3, 2025

- maintained effective controls to provide reasonable assurance that the Let's Encrypt Root CA keys were generated and protected in conformity with the procedures described in the Let's Encrypt CP/CPS, and Key Generation Script

Internet Security Research Group
548 Market St, PMB 77519
San Francisco, California 94104-5401

- performed, during the root key generation process, all procedures required by the Key Generation Script
- generated the CA keys in a physically secured environment as described in the Let's Encrypt CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the Let's Encrypt CP/CPS

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

DocuSigned by:
Josh Aas
F08BC535FDD84DD...

9/30/2025

Josh Aas
Executive Director

Internet Security Research Group
548 Market St, PMB 77519
San Francisco, California 94104-5401

ATTACHMENT A – IN-SCOPE CAs

Root CA Certificates				
Subject DN	**Subject Key Identifier**	**SHA256 Thumbprint**	**Valid From**	**Valid To**
CN = Root YE O = ISRG C = US	A3C8265A8EA14CD03563FC9B23C83AAE56F34F56	E14FFCAD5B0025731006CAA43A121A22D8E9700F4FB9CF852F02A708AA5D5666	9/3/2025	9/2/2045
CN = Root YR O = ISRG C = US	DEE75B60D0226D40287D3F0D01FEA4B552B45194	E57B7E6F150C419102E8D5C055729FF967B9D1A829BF00CEC89CA604EBF4A86F	9/3/2025	9/2/2045