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 the assertions by the management of Let's Encrypt and IdenTrust Services, LLC ("IdenTrust"), an independent subservice organization that provides Certification Authority ("CA") data center services to Let's Encrypt, that for its CA operations in Utah and Colorado, in the United States of America, for its CAs enumerated in Attachment A, Let's Encrypt and IdenTrust have:

- 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 of September 1, 2024 to August 31, 2025 based on the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7 for the relevant systems and processes used in the issuance of all certificates that assert policy object identifier 2.23.140.1.2.1.

## Certification Authority's Responsibilities

Let's Encrypt'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 – Network Security v1.7.

## Subservice Organization's Responsibilities

IdenTrust has provided an accompanying assertion titled "IdenTrust Services, LLC Management's Assertion" (IdenTrust assertion) about the services provided to Let's Encrypt. IdenTrust Management is responsible for its assertion and providing services in accordance with the described practices of Let's Encrypt; and implementing, operating and documenting controls designed in accordance with Let's Encrypt's requirements, which enable Let's Encrypt to achieve the applicable WebTrust Criteria as set out in Let's Encrypt's assertion.

## Independent Accountant's responsibilities

Our responsibility is to express an opinion on 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

BDO USA refers to BDO USA, P.C., a Virginia professional corporation, also doing business in certain jurisdictions with an alternative identifying abbreviation, such as Corp. or P.S.C.

BDO USA, P.C. is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The relative effectiveness and significance of specific controls at Let’s Encrypt 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 unauthorised 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.

### Independent Accountant’s Opinion

In our opinion, Let’s Encrypt’s and IdenTrust’s management assertions, as referred to above, are fairly stated, in all material respects.

This report does not include any representation as to the quality of Let’s Encrypt or IdenTrust services other than its CA operations at Utah and Colorado, in the United States of America, nor the suitability of any of Let’s Encrypt or IdenTrust services for any customer's intended purpose.

### Other Matter

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

| Matter Topic | | Matter Description |
|---|---|---|
| 1 | Security Management | Let's Encrypt disclosed in Mozilla Bug #1955721 that for 2 out of the 4 quarters during the engagement period there was no documentation of analysis of critical vulnerabilities detected from the weekly scans. |

While the Let’s Encrypt assertion notes all issues disclosed on Bugzilla from September 1, 2024 through the date of this report, we have only noted those instances relevant to the CAs enumerated in Attachment A and applicable to the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7.

### Use of the WebTrust seal

Let’s Encrypt’s use of the WebTrust for Certification Authorities – 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.

BDO USA, P.C.

November 17, 2025

## ATTACHMENT A - IN-SCOPE CAs

| Root CA Certificates | | | |
|---|---|---|---|
| **Subject DN** | **SHA-256 Thumbprint** | **Valid From** | **Valid To** |
| CN=ISRG Root X1<br>O=Internet Security Research Group<br>C=US | 96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6 | 6/4/2015 | 6/4/2035 |
| CN=ISRG Root X2<br>O=Internet Security Research Group<br>C=US | 8B05B68CC659E5ED0FCB38F2C942FBFD200E6F2FF9F85D63C6994EF5E0B02701 | 9/4/2020 | 9/15/2025 |
| CN=ISRG Root X2<br>O=Internet Security Research Group<br>C=US | 69729B8E15A86EFC177A57AFB7171DFC64ADD28C2FCA8CF1507E34453CCB1470 | 9/4/2020 | 9/17/2040 |
| CN=ISRG Root X1<br>O=Internet Security Research Group<br>C=US | 6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F | 1/20/2021 | 9/30/2024 |

| Subordinate CA Certificates | | | |
|---|---|---|---|
| **Subject DN** | **SHA-256 Thumbprint** | **Valid From** | **Valid To** |
| CN=E1<br>O=Let's Encrypt<br>C=US | 46494E30379059DF18BE52124305E606FC59070E5B21076CE113954B60517CDA | 9/4/2020 | 9/15/2025 |
| CN=E2<br>O=Let's Encrypt<br>C=US | BACDE0463053CE1D62F8BE74370BBAE79D4FCAF19FC07643AEF195E6A59BD578 | 9/4/2020 | 9/15/2025 |
| CN=R3<br>O=Let's Encrypt<br>C=US | 67ADD1166B020AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD | 9/4/2020 | 9/15/2025 |
| CN=R4<br>O=Let's Encrypt<br>C=US | 1A07529A8B3F01D231DFAD2ABDF71899200BB65CD7E03C59FA82272533355B74 | 9/4/2020 | 9/15/2025 |
| CN=E5<br>O=Let's Encrypt<br>C=US | 5DFDB3CF31B26F23D87C09F3A0CEF642F64069A9FB7CFE29270BB5DC0F1E16BB | 3/13/2024 | 3/12/2027 |
| CN=E5<br>O=Let's Encrypt<br>C=US | E788D14B0436B5120BBEE3F15C15BADF08C1407FE72568A4F16F9151C380E1E3 | 3/13/2024 | 3/12/2027 |
| CN=E6<br>O=Let's Encrypt<br>C=US | 76E9E288AAFC0E37F4390CBF946AAD997D5C1C901B3CE513D3D8FADBABE2AB85 | 3/13/2024 | 3/12/2027 |
| CN=E6<br>O=Let's Encrypt<br>C=US | 065AB7D2A050F947587121765D8D070C0E1330D5798FAA42C2072749ED293762 | 3/13/2024 | 3/12/2027 |
| CN=E7<br>O=Let's Encrypt<br>C=US | AEB1FD7410E83BC96F5DA3C6A7C2C1BB836D1FA5CB86E708515890E428A8770B | 3/13/2024 | 3/12/2027 |
| CN=E7<br>O=Let's Encrypt<br>C=US | 54715420224C5B65BEED018DC3940D7338C577E322D5488F633D8C6A8FED61B2 | 3/13/2024 | 3/12/2027 |
| CN=E8<br>O=Let's Encrypt<br>C=US | 83624FD338C8D9B023C18A67CB7A9C0519DA43D11775B4C6CBDAD45C3D997C52 | 3/13/2024 | 3/12/2027 |
| CN=E8<br>O=Let's Encrypt<br>C=US | AC1274542267F17B525535B5563BF731FEBB182533B46A82DC869CB64EB528C0 | 3/13/2024 | 3/12/2027 |
| CN=E9<br>O=Let's Encrypt<br>C=US | FDE88F2D4F8913D3DC1664D5F8DE51E07FE2ABFED93B45ACAD5A29BFEBAA23FB | 3/13/2024 | 3/12/2027 |
| CN=E9<br>O=Let's Encrypt<br>C=US | 4185DF97806C2BA76F1D79823F112FFA639A49CCDC990908102067AB6412B886 | 3/13/2024 | 3/12/2027 |
| CN=R10<br>O=Let's Encrypt<br>C=US | 9D7C3F1AA6AD2B2EC0D5CF1E246F8D9AE6CBC9FD0755AD37BB974B1F2FB603F3 | 3/13/2024 | 3/12/2027 |

| Subordinate CA Certificates | | | |
|---|---|---|---|
| **Subject DN** | **SHA-256 Thumbprint** | **Valid From** | **Valid To** |
| CN=R11<br>O=Let's Encrypt<br>C=US | 591E9CE6C863D3A079E9FABE1478C7339A26B21269DDE795211361024AE31A44 | 3/13/2024 | 3/12/2027 |
| CN=R12<br>O=Let's Encrypt<br>C=US | 131FCE7784016899A5A00203A9EFC80F18EBBD75580717EDC1553580930836EC | 3/13/2024 | 3/12/2027 |
| CN=R13<br>O=Let's Encrypt<br>C=US | D3B128216A843F8EF1321501F5DF52A5DF52939EE2C19297712CD3DE4D419354 | 3/13/2024 | 3/12/2027 |
| CN=R14<br>O=Let's Encrypt<br>C=US | 24D45AA9B8D6053D281F3842C8CC0C6C1AF7CCDFD42DD5C12F6A74FA9323F7A2 | 3/13/2024 | 3/12/2027 |

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

**11/17/2025**

## INTERNET SECURITY RESEARCH GROUP MANAGEMENT'S ASSERTION

Internet Security Research Group ("Let's Encrypt") operates the CA services for the root and subordinate CAs enumerated in Attachment A and provides SSL CA services.

Let's Encrypt uses IdenTrust Services, LLC ("IdenTrust"), an independent subservice organization, to provide Certification Authority ("CA") data center services to Let's Encrypt.

The management of Let's Encrypt is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system 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 Let's Encrypt's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Let's Encrypt's management has assessed its disclosures over its SSL CA services. Based on that assessment, in providing its SSL CA services in Utah and Colorado, in the United States of America, Let's Encrypt has:

- 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 of September 1, 2024 to August 31, 2025 based on the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7.

Let's Encrypt 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, 2024 through the date of this report.

| Bug ID | Summary | Opened | Closed | Resolution |
|---|---|---|---|---|
| #1921573 | Let's Encrypt: No Meaningful Subject Distinguished Name | 9/27/2024 | 11/6/2024 | FIXED |
| #1954861 | Let's Encrypt: Early CRL Removal Incident | 3/18/2025 | 4/9/2025 | FIXED |
| #1955721 | Let's Encrypt: Failure to Document Analysis of Detected Vulnerabilities | 3/21/2025 | 6/10/2025 | FIXED |
| #1966515 | Let's Encrypt: Issuance for Invalid Internationalized Domain Name | 5/14/2025 | 6/4/2025 | INVALID |
| #1972745 | Let's Encrypt: Deployed Unreviewed Boulder Code | 6/17/2025 | 7/30/2025 | FIXED |

DocuSigned by:
Josh Aas
F08BC535FDD84DD...

11/19/2025

Josh Aas
Executive Director

## ATTACHMENT A – IN-SCOPE CAs

**Root CA Certificates**

| Subject DN | SHA-256 Thumbprint | Valid From | Valid To |
|---|---|---|---|
| CN=ISRG Root X1<br>O=Internet Security Research Group<br>C=US | 96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6 | 6/4/2015 | 6/4/2035 |
| CN=ISRG Root X2<br>O=Internet Security Research Group<br>C=US | 8B05B68CC659E5ED0FCB38F2C942FBFD200E6F2FF9F85D63C6994EF5E0B02701 | 9/4/2020 | 9/15/2025 |
| CN=ISRG Root X2<br>O=Internet Security Research Group<br>C=US | 69729B8E15A86EFC177A57AFB7171DFC64ADD28C2FCA8CF1507E34453CCB1470 | 9/4/2020 | 9/17/2040 |
| CN=ISRG Root X1<br>O=Internet Security Research Group<br>C=US | 6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F | 1/20/2021 | 9/30/2024 |

**Subordinate CA Certificates**

| Subject DN | SHA-256 Thumbprint | Valid From | Valid To |
|---|---|---|---|
| CN=E1<br>O=Let's Encrypt<br>C=US | 46494E30379059DF18BE52124305E606FC59070E5B21076CE113954B60517CDA | 9/4/2020 | 9/15/2025 |
| CN=E2<br>O=Let's Encrypt<br>C=US | BACDE0463053CE1D62F8BE74370BBAE79D4FCAF19FC07643AEF195E6A59BD578 | 9/4/2020 | 9/15/2025 |
| CN=R3<br>O=Let's Encrypt<br>C=US | 67ADD1166B020AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD | 9/4/2020 | 9/15/2025 |
| CN=R4<br>O=Let's Encrypt<br>C=US | 1A07529A8B3F01D231DFAD2ABDF71899200BB65CD7E03C59FA82272533355B74 | 9/4/2020 | 9/15/2025 |
| CN=E5<br>O=Let's Encrypt<br>C=US | 5DFDB3CF31B26F23D87C09F3A0CEF642F64069A9FB7CFE29270BB5DC0F1E16BB | 3/13/2024 | 3/12/2027 |
| CN=E5<br>O=Let's Encrypt<br>C=US | E788D14B0436B5120BBEE3F15C15BADF08C1407FE72568A4F16F9151C380E1E3 | 3/13/2024 | 3/12/2027 |
| CN=E6<br>O=Let's Encrypt<br>C=US | 76E9E288AAFC0E37F4390CBF946AAD997D5C1C901B3CE513D3D8FADBABE2AB85 | 3/13/2024 | 3/12/2027 |
| CN=E6<br>O=Let's Encrypt<br>C=US | 065AB7D2A050F947587121765D8D070C0E1330D5798FAA42C2072749ED293762 | 3/13/2024 | 3/12/2027 |
| CN=E7<br>O=Let's Encrypt<br>C=US | AEB1FD7410E83BC96F5DA3C6A7C2C1BB836D1FA5CB86E708515890E428A8770B | 3/13/2024 | 3/12/2027 |
| CN=E7<br>O=Let's Encrypt<br>C=US | 54715420224C5B65BEED018DC3940D7338C577E322D5488F633D8C6A8FED61B2 | 3/13/2024 | 3/12/2027 |
| CN=E8<br>O=Let's Encrypt<br>C=US | 83624FD338C8D9B023C18A67CB7A9C0519DA43D11775B4C6CBDAD45C3D997C52 | 3/13/2024 | 3/12/2027 |
| CN=E8<br>O=Let's Encrypt<br>C=US | AC1274542267F17B525535B5563BF731FEBB182533B46A82DC869CB64EB528C0 | 3/13/2024 | 3/12/2027 |
| CN=E9<br>O=Let's Encrypt<br>C=US | FDE88F2D4F8913D3DC1664D5F8DE51E07FE2ABFED93B45ACAD5A29BFEBAA23FB | 3/13/2024 | 3/12/2027 |

**Subordinate CA Certificates**

| Subject DN | SHA-256 Thumbprint | Valid From | Valid To |
|---|---|---|---|
| CN=E9<br>O=Let's Encrypt<br>C=US | 4185DF97806C2BA76F1D79823F112FFA639A49CCDC990908102067AB6412B886 | 3/13/2024 | 3/12/2027 |
| CN=R10<br>O=Let's Encrypt<br>C=US | 9D7C3F1AA6AD2B2EC0D5CF1E246F8D9AE6CBC9FD0755AD37BB974B1F2FB603F3 | 3/13/2024 | 3/12/2027 |
| CN=R11<br>O=Let's Encrypt<br>C=US | 591E9CE6C863D3A079E9FABE1478C7339A26B21269DDE795211361024AE31A44 | 3/13/2024 | 3/12/2027 |
| CN=R12<br>O=Let's Encrypt<br>C=US | 131FCE7784016899A5A00203A9EFC80F18EBBD75580717EDC1553580930836EC | 3/13/2024 | 3/12/2027 |
| CN=R13<br>O=Let's Encrypt<br>C=US | D3B128216A843F8EF1321501F5DF52A5DF52939EE2C19297712CD3DE4D419354 | 3/13/2024 | 3/12/2027 |
| CN=R14<br>O=Let's Encrypt<br>C=US | 24D45AA9B8D6053D281F3842C8CC0C6C1AF7CCDFD42DD5C12F6A74FA9323F7A2 | 3/13/2024 | 3/12/2027 |

IdenTrust
part of HID

IdenTrust Services, LLC
5225 Wiley Post Way
Suite 450
Salt Lake City, Utah, 84116

**11/17/2025**

## IDENTRUST SERVICES, LLC MANAGEMENT'S ASSERTION

IdenTrust Services, LLC ("IdenTrust") Certification Authority ("CA") data center services to Internet Security Research Group ("Let's Encrypt"), who operates the Certification Authority ("CA") services for the CAs enumerated in Attachment A.

The management of IdenTrust is responsible for establishing controls over its operations, to support Let's Encrypt's SSL CA operations, including its network and certificate security system 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 IdenTrust's PKI services. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

IdenTrust's management has assessed Let's Encrypt's disclosure of its certificate practices and IdenTrust's controls to provide its PKI services to Let's Encrypt. Based on that assessment, in IdenTrust management's opinion, in providing its PKI services at Utah and Colorado, in the United States of America, IdenTrust has:

- 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, 2024 to August 31, 2025 based on the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7.

IdenTrust services include controls to support the physical and environmental security for CA operations systems. These controls include the relevant logging and monitoring controls related to physical and environmental controls provided by IdenTrust. The controls provided by IdenTrust support some elements of criteria include in the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7, however, IdenTrust is not responsible for the entirety of the controls to address any single criterion.

IdenTrust Services, LLC

Signed by:
Don Johnson
5AEF09ABDA0A425...

11/18/2025

Don Johnson
Chief Information Officer