**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 1.2.1. Revisions<br>Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.* | CP 1.2, CPS 1.2 | List of revisions, certificates issued are fully compliant with any exceptions having already been reported to Mozilla and resolved. |
| 1.2.2. Relevant Dates<br>Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.* | N/A | Let's Encrypt is fully compliant with each item. |
| 1.3.2. Registration Authorities<br>Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs (including non-delegation of domain validation to RAs).* | CP 1.3.2, CPS 1.3.2 | Let's Encrypt does not delegate RA services. |
| 1.5.2 Contact person<br>BR Section 4.9.3 requires that this section 1.5.2 contain clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. | CPS 1.5.2 | Compliant |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 2.1. Repositories<br>*Provide the direct URLs to the CA's repositories* | CPS 1.2 | https://letsencrypt.org/repository/ |
| 2.2 Publication of information - RFC 3647<br>"The Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**." | CP 2.2, CPS 1.1 | Our CP and CPS documents are structured per RFC 3647 |
| 2.2 Publication of information - CAA<br>**Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements.**<br><br>**It shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.** | CPS 4.2.1 | Let's Encrypt checks CAA records in accordance with the BRs and states as much, including our identifying domain, in our CPS. |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 2.2. Publication of information - BR text<br>"The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version."<br>--> ***Copy the specific text that is used into the explanation in this row. (in English)*** | CPS 1.1 | "The ISRG PKI conforms to the current version of the guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates ("Baseline Requirements"). CAB Forum documents can be found at https: //www.cabforum.org. If there is any conflict between this CPS and a relevant CAB Forum requirement or guideline, then the CAB Forum requirement or guideline shall take precedence." |
| 2.2. Publication of information - test websites<br>"The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired."<br>--> ***List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.*** | CP 2.2 | https://valid-isrgrootx1.letsencrypt.org/<br>https://revoked-isrgrootx1.letsencrypt.org/<br>https://expired-isrgrootx1.letsencrypt.org/<br>https://valid-isrgrootx2.letsencrypt.org/<br>https://revoked-isrgrootx2.letsencrypt.org/<br>https://expired-isrgrootx2.letsencrypt.org/ |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 2.3. Time or frequency of publication<br>"The CA SHALL ... **annually** update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document."<br><br>*Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.* | CP 2.3, CPS 9.12.1 | Our Policy Management Authority meets quarterly and regularly review our CP and CPS documents. We make updates in response to issues identified during these meetings and we often meet outside of the regularly sheduled meetings to update the documents. During these meetings we review diffs to the BRs since the last time we reviewed. |
| 2.4. Access controls on repositories<br>*Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.* | CP 2.2-2.4, CPS 2.1-2.4 | We will continue to make our Audit, CP, and CPS documetns publicly available. |
| 3.2.2.1 Identity<br>If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.* | | N/A as we only issue Domain Validation certificates |
| 3.2.2.2 DBA/Tradename<br>If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.* | | N/A as we only issue Domain Validation certificates |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 3.2.2.3 Verification of Country<br>If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.* | | N/A as we only issue Domain Validation certificates |
| 3.2.2.4 Validation of Domain Authorization or Control<br>*Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.*<br><br>***Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."*** | CP 3.2.2.4, CPS 3.2.2 | Our CPS states only the methods that we actually use. |
| 3.2.2.4.1 Validating the Applicant as a Domain Contact<br>T**his method SHALL NOT be used.** | **This method SHALL NOT be used.** | Not used |
| 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A as we only issue Domain Validation certificates |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 3.2.2.4.3 Phone Contact with Domain Contact<br>**This method has been replaced by 3.2.2.4.15 and SHALL NOT be used. (Validations completed as of 31-May-2019 may be used until 20-August-2021.)** | **This method SHALL NOT be used.** | Not used |
| 3.2.2.4.4 Constructed Email to Domain Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |
| 3.2.2.4.5 Domain Authorization Document<br>"T**his method SHALL NOT be used**." | **This method SHALL NOT be used.** | Not used |
| 3.2.2.4.6 Agreed-Upon Change to Website<br>Replaced with BR section 3.2.2.4.18 (effective 3/3/2020) | **This method SHALL NOT be used.** | Not used |
| 3.2.2.4.7 DNS Change<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | CP 3.2.2.4.7, CPS 3.2.2 | We issue certificates in compliance with the method described in the BRs. |
| 3.2.2.4.8 IP Address<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |
| 3.2.2.4.9 Test Certificate<br>**"This method SHALL NOT be used."** | **This method SHALL NOT be used.** | Not used |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 3.2.2.4.10. TLS Using a Random Number<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*<br><br>*This subsection contains major vulnerabilities.* ***If the CA uses this method, then the CA should describe how they are mitigating those vulnerabilities. If not using this method, the CPS should say so.*** | **Further explanation is required if this method is used.** | Not used |
| 3.2.2.4.11 Any Other Method<br>**"This method SHALL NOT be used."** | **This method SHALL NOT be used.** | Not used |
| 3.2.2.4.12 Validating Applicant as a Domain Contact<br>"This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name."<br><br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | **Use of this method is restricted, per the BRs.** | Not used |
| 3.2.2.4.13 Email to DNS CAA Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |
| 3.2.2.4.14 Email to DNS TXT Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 3.2.2.4.15 Phone Contact with Domain Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |
| 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |
| 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact<br>If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* | | N/A, we do not use this method |
| 3.2.2.4.18 Agreed-Upon Change to Website v2<br>If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs. | | N/A, we do not use this method |
| 3.2.2.4.19 Agreed-Upon Change to Website - ACME<br>If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs. | CP 3.2.2.4.19, CPS 3.2.2 | We issue certificates in compliance with the method described in the BRs. |
| 3.2.2.4.20 TLS Using ALPN - If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs. | CP 3.2.2.4.20, CPS 3.2.2 | We issue certificates in compliance with the method described in the BRs. |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 3.2.2.5 Authentication for an IP Address<br>If your CA allows IP Addresss to be listed in certificates, ***indicate which methods your CA uses*** *and how your CA meets the requirements in this section of the BRs.*<br><br>**Section 2.2 of Mozilla's root store policy says: "the CA must ensure that the applicant has control over all IP Address(es) referenced in the certificate. This must be done using one or more of the methods documented in section 3.2.2.5 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.5 it is complying with."** | **Method 3.2.2.5.4, Any Other Method, SHALL NOT be used.**<br><br>"After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address." | N/A, we do not issue certificates for IP addresses |
| 3.2.2.6 Wildcard Domain Validation<br>If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.* | CP 3.2.2.6, CPS 3.2.2 | We issue certificates in compliance with the method described in the BRs. We require wildcard validation via method 3.2.2.4.7, DNS change. We will not issue wildcards via other validation methods. |
| 3.2.2.7 Data Source Accuracy<br>*Indicate how your CA meets the requirements in this section of the BRs.* | CP 3.2.2.7 | Let's Encrypt uses heavily tested validation methods and caches validation information for up to 30 days maximum. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 3.2.2.8 CAs MUST check and process CAA records<br>*Indicate how your CA meets the requirements in this section of the BRs.*<br><br>*Section 2.2 of the BRs states: "**CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."*** | CP 3.2.2.8, CPS 4.2.1 | Let's Encrypt checks CAA records at the same time as domain validation; if more than 8 hours elapse between then and issuance, CAA records are rechecked immediately prior to issuance.<br><br>We indicate our Issuer Domain Name in section 4.2.1 of our CPS. |
| 3.2.3. Authentication of Individual Identity | CP 3.2.3, CPS 3.2.3 | Let's Encrypt does not issue to individuals. |
| 3.2.5. Validation of Authority | CP 3.2.5, CPS 3.2.5 | Let's Encrypt does not issue to organizations. |
| 3.2.6. Criteria for Interoperation or Certification<br>Disclose all cross-certificates in the CA hierarchies under evaluation. | CP 3.2.6, CPS 3.2.6 | Let's Encrypt discloses all cross-certificates for which we arranged or accepted the trust relationship. |
| 4.1.1. Who Can Submit a Certificate Application<br>Indicate how your CA identifies suspicious certificate requests. | CP 4.1.1, CPS 4.1.1, CPS 4.2.2 | ISRG maintains a list of high-risk domains and blocks issuance of certificates for those domains. |
| 4.1.2. Enrollment Process and Responsibilities | CP 4.1.2, CPS 4.1.2 | Let's Encrypt's enrollment and certificate request process is specified by RFC 8555 |
| 4.2. Certificate application processing<br>BR section 2.2 says that section 4.2 of the CP/CPS SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names. | CP 4.2, CPS 4.2 | See subsections. CAA addressed in CPS 4.2.1. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 4.2.1. Performing Identification and Authentication Functions<br>Indicate how your CA identifies high risk certificate requests.<br>**Re-use of domain / IP address validation is limited to 398 days and re-use of other validation information is limited to 825 days** | CP 4.2.1, CPS 4.2.1, CPS 4.2.2 | ISRG maintains a list of high-risk domains and blocks issuance of certificates for those domains.<br>We only cache validation information for 30 days. |
| 4.2.2. Approval or Rejection of Certificate Applications<br>"CAs SHALL NOT issue certificates containing Internal Names." | CP 4.2.2, CPS 4.2.2 | Let's Encrypt only issues for names which are reachable on the public internet and which end in a name found in the Public Suffix List. |
| 4.3.1. CA Actions during Certificate Issuance | CP 4.3.1, CPS 4.3.1 | Compliant |
| 4.9.1.1 Reasons for Revoking a Subscriber Certificate<br>*Indicate how your CA's CP/CPS lists the reasons for revoking end entity certificates and is consistent with the timeframes required by this section of the BRs.* | CP 4.9.1.1, CPS 4.9.1 | Our CP lists all reasons specified by the BRs in the same timeframes. |
| 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate<br>*Indicate how your CA's CP/CPS lists the reasons for revoking subordinate CA certificates and is consistent with the timeframes required by this section of the BRs.* | CP 4.9.1.2, CPS 4.9.1 | Our CP lists all reasons specified by the BRs in the same timeframes. |
| 4.9.2. Who Can Request Revocation | CP 4.9.2, CPS 4.9.2 | CPS also lists ACME-standardized methods for requesting revocation. |
| 4.9.3. Procedure for Revocation Request<br>**The CA SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.** | CP 4.9.3, CPS 4.9.3, CPS 1.5.2 | Instructions for revocation request via both ACME API and certificate problem report (email) are given. Said instructions are readily available online. |
| 4.9.5. Time within which CA Must Process the Revocation Request | CP 4.9.5, CPS 4.9.5 | Exact timeline for investigation and subsequent revocation listed. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 4.9.7. CRL Issuance Frequency<br>*Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.* | CP 4.9.7, CPS 4.9.7 | CRLs for intermediates are issued within requirements, and are accessible from https: //letsencrypt.org/certificates/ |
| 4.9.9. On-line Revocation/Status Checking Availability | CP 4.9.9, CPS 4.9.9 | Compliant |
| 4.9.10. On-line Revocation Checking Requirements<br>*Indicate how your CA meets all of the requirements listed in this section, **including support of GET, update frequency (recently updated), and preventing errounious return of "good" status.*** | CP 4.9.10 | Let's Encrypt supports all requirements for 4.9.10. |
| 4.9.12 "CA's CP/CPS MUST clearly specify the methods that parties may use to demonstrate private key compromise." (MRSP 6) | CP 4.9.1.1, CPS 4.9.3 | Compliant |
| 4.9.13 Certificate suspension must not be supported | CP 4.9.13, CPS 4.9.13 | Compliant |
| 4.10.1. Operational Characteristics | CP 4.10.1, CPS 4.10.1 | Compliant |
| 4.10.2. Service Availability | CP 4.10.2, CPS 4.10.2 | Compliant |
| 5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS | CP 5, CPS 5 | Compliant |
| 5.2.2. Number of Individuals Required per Task | CP 5.2.2, CPS 5.2.2 | Compliant |
| 5.3.1. Qualifications, Experience, and Clearance Requirements | CP 5.3.1, CPS 5.3.1, CPS 5.3.2 | Compliant |
| 5.3.3. Training Requirements and Procedures | CP 5.3.3, CPS 5.3.3 | Compliant |
| 5.3.4. Retraining Frequency and Requirements | CP 5.3.4, CPS 5.3.4 | Compliant |
| 5.3.7. Independent Contractor Controls | CP 5.3.7, CPS 5.3.7 | Compliant |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 5.4.1. Types of Events Recorded<br>*Indicate how your CA meets the requirements of this section.* | CP 5.4.1, CPS 5.4.1 | Compliant: Audit logs are generated for all events related to CA security (physical and logical) and certificate issuance. Logs are automatically generated whenever possible. When it is necessary to manually log information, logs are kept on paper with written confirmation from a witness and securely stored. All audit logs, electronic or otherwise, shall be retained and made available to compliance auditors upon request.<br><br>At a minimum, each audit record includes:<br><br>Date and time of entry;<br>Identity of the person (or machine) making the entry; and<br>Description of the entry. |
| 5.4.3. Retention Period for Audit Logs | CP 5.4.3, CPS 5.4.3 | Compliant |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |
| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
| 5.4.8. Vulnerability Assessments<br>*Indicate how your CA meets the requirements of this section.* | CP 5.4.8, CPS 5.4.8 | Compliant: Audit logs are monitored by Trusted Contributors, including operations and engineering staff. Anomalies indicating attempted breaches of CA security are reported and investigated.<br><br>Automated internal and external vulnerability scans occur at least every two weeks, though more typically every week.<br><br>Extensive vulnerability assessments for ISRG infrastructure are conducted at least annually by qualified third parties.<br><br>ISRG Security Officers perform a risk assessment at least annually. This risk assessment:<br><br>Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;<br><br>Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and<br><br>Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 5.5.2. Retention Period for Archive | CP 5.4.3, CPS 5.4.3 | Let's Encrypt retains issuance audit logs for a minimum of 7 years. |
| 5.7.1. Incident and Compromise Handling Procedures<br>*Indicate how your CA meets the requirements of this section, including notifying Mozilla in the event of key compromise.* | CP 5.7.1, CPS 5.7.1, CPS 5.7.2, CPS 5.7.3, and CPS 5.7.4 | Let's Encrypt regularly reviews, tests, and if necessary updates procedures for incident response, to include the Security Officers notifying root programs and subscribers that rely on the integrity of the private key material of any compromise, suspected or confirmed. |
| 6.1.1. Key Pair Generation | CP 6.1.1, CPS 5.2.2, CPS 6.1.1 | Key pairs are generated during ceremonies laid out in the CP 6.1.1.1, to include generating and following a scripted ceremony with video recording of the process in a secure environment. |
| 6.1.1.3 Subscriber Key Pair Generation - the CA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA. | CP 6.1.1.3 | Using the ACME protocol, Let's Encrypt never generates keys on behalf of the subscriber. |
| 6.1.2. Private Key Delivery to Subscriber | CPS 6.1.2 | Using the ACME protocol, Let's Encrypt never has access to subscriber private keys. |
| 6.1.5. Key Sizes | CP 6.1.5, CPS 6.1.5 | Private keys used by Let's Encrypt use RSA 2048 and RSA 4096, and P-384. |
| 6.1.6. Public Key Parameters Generation and Quality Checking | CP 6.1.6, CPS 6.1.6 | All of Let's Encrypt's RSA keys have the exponent of 65537 (0x10001), which is an odd number greater than 3. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 6.1.7. Key Usage Purposes | CP 6.1.7, CPS 6.1.7, CPS 7 | Let's Encrypt's root certificate private keys are only used to sign subordinate CAs, cross certificates, and certificates representing the Root CA itself. |
| 6.2. Private Key Protection and Cryptographic Module Engineering Controls | CP 6.2, CPS 6.2.1, CPS 6.2.2 | The private keys for Let's Encrypt are protected using HSMs meeting FIPS 140-2 Level 3 (or higher) requirements, and require multiple persons in Trusted Roles to access the private keys, both physically and logically, and for all copies of the private keys. |
| 6.2.5. Private Key Archival | CP 6.2.5, CPS 6.2.5 | Let's Encrypt does not archive private keys. |
| 6.2.6. Private Key Transfer into or from a Cryptographic Module | CP 6.2.56, CPS 6.2.6 | CPS 6.2.6 describes that keys are only transferred between HSMs, and are wrapped and unwrapped only within HSMs such that an unencrypted form never exists outside of an HSM. |
| 6.2.7. Private Key Storage on Cryptographic Module | CP 6.2.7, CPS 6.2.7 | The HSMs used for Let's Encrypt meet FIPS 140-2 Level 3 (or higher) requirements, as noted in CPS 6.2.1. |
| 6.3.2 Certificates issued SHOULD NOT have a Validity Period greater than **397 days** and MUST NOT have a Validity Period greater than **398 days**. Indicate how your CA meets the requirements of this section. | CP 6.3.2, CPS 6.3.2 | CPS 6.3.2 limits Let's Encrypt to issuing certificates with a validity period of less than 100 days. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 6.5.1. Specific Computer Security Technical Requirements<br>**The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.**<br>*Indicate how your CA meets the requirements of this section.* | CP 6.5.1, CPS 6.5.1 | Let's Encrypt uses MFA extensively, wherever possible, per our CPS. |
| 7.1. Certificate profile<br>**CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG.**<br>*Indicate how your CA meets the requirements of this section.* | CP 7.1, CPS 7.1 | The CPS 7.1 indicates subscriber certificates include 64 bits of a CSPRNG. Concretely, Let's Encrypt currently includes 136 bits of the CSPRNG, as defined in the Boulder serial generation code. |
| 7.1.1. Version Number(s) | CP 7.1.1, CPS 7.1.1 | Compliant |
| 7.1.2. Certificate Content and Extensions; Application of RFC 5280 | CP 7.1.2, CPS 7.1.2 | See subsections |
| 7.1.2.1 Root CA Certificate | CP 7.1.2.1, CPS 7.1.2 | Let's Encrypt Root certificates are compliant with the Baseline Requirements. |
| 7.1.2.2 Subordinate CA Certificate | CP 7.1.2.2, CPS 7.1.2 | Let's Encrypt intermediate/subordinate certificates are compliant with the Baseline Requirements. |
| 7.1.2.3 Subscriber Certificate | CP 7.1.2.3 | Let's Encrypt subscriber certificates are compliant with the Baseline Requirements. |
| 7.1.2.4 All Certificates | CP 7.1.2.4 | Let's Encrypt is fully compliant with each item. |
| 7.1.2.5 Application of RFC 5280 | CP 7.1.2.5, CPS 7.1 | The RFC 6962 poison extension is outlined in the DV-SSL End Entity Certificate section of CPS 7.1. |
| 7.1.3. Algorithm Object Identifiers | CP 7.1.3, CPS 7.1.3 | See subsections |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 7.1.3.1 SubjectPublicKeyInfo | CP 7.1.3.1, CPS 7.1.3.1 | Compliant |
| 7.1.3.2 Signature AlgorithmIdentifier | CP 7.1.3.2, CPS 7.1.3.2 | See subsections |
| 7.1.4. Name Forms | CP 7.1.4, CPS 7.1.4 | Let's Encrypt is fully compliant with each item. |
| 7.1.4.1 Name Encoding - Subject and Issuer Names for all possible certification paths MUST be byte-for-byte identical | CP 7.1.4.1 | Issuer information is compliant with the Baseline Requirements and RFC 5280, section 4.1.2.4 |
| 7.1.4.2 Subject Information - Subscriber Certificates | CP 7.1.4.2, CP 3.2.2.4, CP 3.2.2.5 | Compliant |
| 7.1.4.2.1 Subject Alternative Name Extension<br>**This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.**<br><br>**CAs SHALL NOT issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.**<br><br>**Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").** | CP 7.1.4.2.1 | Let's Encrypt is fully compliant with each item. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 7.1.4.2.2 Subject Distinguished Name Fields<br>If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1). | CP 7.1.4.2.2 | Let's Encrypt is fully compliant with each item. |
| 7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates | CP 7.1.4.3 | Compliant |
| 7.1.5. Name Constraints<br>***Indicate your CA's understanding of section 5.3 of Mozilla's root store policy, and requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section of the BRs.***<br><br>***"All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's root program:***<br>***MUST be audited in accordance with Mozilla's Root Store Policy. ...***<br>***MUST be publicly disclosed in the CCADB by the CA that has their certificate included in Mozilla's root program. The CA with a certificate included in Mozilla's root program MUST disclose this information within a week of certificate creation, and before any such subordinate CA is allowed to issue certificates. ..."*** | CP 7.1.5 | Let's Encrypt roots are audited and disclosed in CCADB as required. |
| 7.1.6. Certificate Policy Object Identifier | CP 7.1.6 | See subsections |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 7.1.6.1 Reserved Certificate Policy Identifiers | CP 7.1.6.1, CPS 7.1 | Compliant |
| 7.1.6.2 Root CA Certificates | CP 7.1.6.2 | The Let's Encrypt root certificates do not contain the certificate policies extension. |
| 7.1.6.3 Subordinate CA Certificates | CP 7.1.6.3 | Compliant |
| 7.1.6.4 Subscriber Certificates<br>Certificates MUST contain "one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc of {joint-iso-itu-t(2) international-organizations (23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1)." | CP 7.1.6.4, CPS 7.1 | Let's Encrypt includes policy 2.23.140.1.2.1 on all subscriber certificates. Certificates are validated with zlint to confirm this. |
| 7.2 and 7.3 - All OCSP and CRL responses for Subordinate CA Certificates MUST include a meaningful reason code. | CPS 7.2, 7.3 | Let's Encrypt validates and requires a meaningful reason code when revoking ceritificates. |
| 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS | CP 8, CPS 8 | Let's Encrypt operates its PKI with all the applicable laws to being a CA and issuing certificates. Let's encrypt complies and goes beyond the stated audit and assessment requirements. |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 8.1. Frequency or circumstances of assessment<br>**The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.**<br>For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.<br>*Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.* | CP 8.1, CPS 8.1 | All ISRG audits are available through GitHub and the Let's Encrypt website. ISRG currently has a valid audit report with the WebTrust audit scheme. The audits cover no more than one year and are scheduled by ISRG anually, every year with no gaps. |
| 8.2. Identity/qualifications of assessor<br>*Indicate how your CA meets the requirements of this section.* | CP 8.2, CPS 8.2 | ISRG's WebTrust compliance audits are performed by a qualified auditor, as defined in BR 8.2. |
| 8.4. Topics covered by assessment | CP 8.4, CPS 8.4 | Compliance audits happen annually and cover all the topics as defined by the WebTrust scheme of compliance. |

| | | |
|---|---|---|
| **Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1** | | |
| **CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)** | | |
| **ISRG / Let's Encrypt BR Self Assessment**<br><br>This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.<br><br>We used Baseline Requirements v1.7.4.<br>We used ISRG CP v2.6 and CPS v3.2. | | |
| | | |
| | | |

| **BR/RFC 3647 Section Number** | **List the specific documents and section numbers of those documents which meet the requirements of each BR section** | **Explain how the CA's listed documents meet the requirements of each BR section.** |
|---|---|---|
| 8.6. Communication of results<br>The Audit Report must contain certain information formatted in a certain way, including but not limited to:<br>- name of the company being audited;<br>- name and address of the organization performing the audit;<br>- Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope;<br>- audit criteria (with version number) that were used to audit each of the certificates;<br>- a list of the CA policy documents (with version numbers) referenced during the audit;<br>- whether the audit is for a period of time or a point in time;<br>- the start date and end date of the period, for those that cover a period of time;<br>- the point-in-time date, for those that are for a point in time;<br>- the date the report was issued (which will necessarily be after the end date or point-in-time date); and<br>- For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). . | CP 8.6, CPS 8.6 | All ISRG audits are available through GitHub and the Let's Encrypt website. Our audits comply with all the baseline requirements for the audit reports and the information contained within them. |
| **Also indicate your understanding and compliance with section 3 of Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps)."** | CP 8.1, CPS 8.1 | Let's Encrypt conducts WebTrust audits annually and contiguously. |

**Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1**

**CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)**

**ISRG / Let's Encrypt BR Self Assessment**

This self assessment covers all Let's Encrypt roots and intermediaries, as disclosed in CCADB.

We used Baseline Requirements v1.7.4.
We used ISRG CP v2.6 and CPS v3.2.

| BR/RFC 3647 Section Number | List the specific documents and section numbers of those documents which meet the requirements of each BR section | Explain how the CA's listed documents meet the requirements of each BR section. |
|---|---|---|
| 8.7. Self-Audits | CP 8.7, CPS 8.7 | Compliant |
| 9.6.1. CA Representations and Warranties | CP 9.6.1, CPS 9.6.1 | Compliant |
| 9.6.3. Subscriber Representations and Warranties | CP 9.6.3, CPS 9.6.3 | Compliant |
| 9.8. Limitations of liability | CP 9.8 | Compliant |
| 9.9.1. Indemnification by CAs | CP 9.9.1 | Compliant |
| 9.16.3. Severability | CP 9.16.3 | Compliant |
| APPENDIX A - RFC 6844 ERRATA 5065<br>To prevent resource exhaustion attacks, CAs SHOULD limit the length of CNAME chains that are accepted. However CAs MUST process CNAME chains that contain 8 or fewer CNAME records. | | Compliant |
| APPENDIX B – CAA CONTACT TAG<br>These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control. | | N/A, we do not support this |
| APPENDIX C - Issuance of Certificates for .onion Domain Names | | N/A, we do not support this |