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

| **BR 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. | | Entrust CAs are compliant with all items. |
| 1.2.2. Relevant Dates<br>Note the Compliance date for eachitem 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. | | |
| 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. | CPS 3.2.2.1, 3.2.2.2, 3.2.2.3 and 3.2.5 | Delegated third parties can support validation or identity and authorization to issue. All data is entered in the Entrust certificate management system, which is reviewed by the Entrust verification team and is available for annual audit. |
| 2.1. Repositories<br>Provide the direct URLs to the CA's repositories | http:www.entrust.net/CPS;<br>http://ocsp.entrust.net;<br>http://crl.entrust.net/level1f.crl;<br>http//crl.entrust.net/level1j.crl;<br>http://crl.entrust.net/level1k.crl;<br>http://crl.entrust.net/level1m.crl;<br>http://crl.entrust.net/level1n.crl; | |

| | | |
|---|---|---|
| 2.2. Publication of information<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 | Entrust conforms to the current version of the CA/Browser Forum Guidelines Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published at http://www.cabforum.org. The Baseline Requirements describe certain minimum requirements that a Certification Authority (CA) must meet in order to issue SSL Certificates. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this CPS. |
| 2.2. Publication of information<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. | https://2048test.entrust.net/;<br>https://expired2048.entrust.net/;<br>https://revoked2048.entrust.net/;<br>https://validg2.entrust.net/;<br>https://expiredg2.entrust.net/;<br>https://revokedg2.entrust.net/;<br>https://validev.entrust.net/;<br>https://expiredev.entrust.net/;<br>https://revokedev.entrust.net/;<br>https://validec.entrust.net/;<br>https://expiredec.entrust.net/;<br>https://revokedec.entrust.net/;<br>https://validg4.entrust.net/;<br>https://expiredg4.entrust.net/;<br>https://revokedg4.entrust.net/ | All links for the roots are provided |
| 2.3. Time or frequency of publication<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. | CPS 2.3 | Meets requirements of BR 2.3 |
| 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. | CPS 2.4 | Meets requirements of BR 2.4 |
| 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. | CPS 3.2.2.1 | Meets requirements of BR 3.2.2.1 |

| | | |
|---|---|---|
| 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. | CPS 3.2.2.2 | Meets requirements of BR 3.2.2.2 |
| 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. | CPS 3.2.2.3 | Meets requirements of BR 3.2.2.3 |
| 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. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation. | Covered in subsections to CPS 3.2.2.4 | Meets requirement to specify each acceptable method of domian validation |
| 3.2.2.4.1 Validating the Applicant as a 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. | CPS 3.2.2.4.1 | Meets requirements of BR 3.2.2.4.1 |
| 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. | CPS 3.2.2.4.2 | Meets requirements of BR 3.2.2.4.2 |
| 3.2.2.4.3 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. | CPS 3.2.2.4.3 | Meets requirements of BR 3.2.2.4.3 |
| 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. | CPS 3.2.2.4.4 | Meets requirements of BR 3.2.2.4.4 |
| 3.2.2.4.5 Domain Authorization Document<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. | Not applicable | Entrust does not use this method |
| 3.2.2.4.6 Agreed-Upon Change to Website<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. | CPS 3.2.2.4.6 | Meets requirements of BR 3.2.2.4.6 |

| | | |
|---|---|---|
| 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. | CPS 3.2.2.4.7 | Meets requirements of BR 3.2.2.4.7 |
| 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. | CPS 3.2.2.4.8 | Meets requirements of BR 3.2.2.4.8 |
| 3.2.2.4.9 Test Certificate<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. | Not applicable | Entrust does not use this method |
| 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. | Not applicable | Entrust does not use this method |
| 3.2.2.5 Authentication for an IP Address<br>If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs. | CPS 3.2.2.5 | Meets requirements of BR 3.2.2.5 methods 1, 2 and 3 |
| 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. | CPS 3.2.2.6 | Meets the requirements of BR 3.2.2.6 |
| 3.2.2.7 Data Source Accuracy<br>Indicate how your CA meets the requirements in this section of the BRs. | CPS 3.2.2.7 | Meets the requirements of BR 3.2.2.7 |
| 3.2.3. Authentication of Individual Identity | CPS 3.2.3 | Meets the requirements of BR 3.2.3 |
| 3.2.5. Validation of Authority | CPS 3.2.5 | Meets the requirements of BR 3.2.5 |
| 3.2.6. Criteria for Interoperation or Certification<br>Disclose all cross-certificates in the CA hierarchies under evaluation. | CPS 3.2.6 | Meets the requirements of BR 3.2.6 |
| 4.1.1. Who Can Submit a Certificate Application<br>Indicate how your CA identifies suspicious certificate requests. | CPS 4.1.1 | Meets the requirements of BR 4.1.1 |
| 4.1.2. Enrollment Process and Responsibilities | CPS 4.1.2 | Meets the requirements of BR 4.1.2 |
| 4.2. Certificate application processing | N/A as BR has no requirements | N/A |
| 4.2.1. Performing Identification and Authentication Functions<br>Indicate how your CA identifies high risk certificate requests. | CPS 4.2.1 | Meets the requirements of BR 4.2.1 |

| | | |
|---|---|---|
| 4.2.2. Approval or Rejection of Certificate Applications | Not applicable | BR 4.2.2 is not applicable as this section corresponds to Internal certificates which Cas have not issued as of November 1, 2015. |
| 4.3.1. CA Actions during Certificate Issuance | CPS 4.3.1 | Meets the requirements of BR 4.3.1 |
| 4.9.1.1 Reasons for Revoking a Subscriber Certificate<br>Reasons for revoking certificates must be listed in the CA's CP/CPS. | CPS 4.9.1.1 | Meets the requirements specified in BR 4.9.1.1 |
| 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate | CPS 4.9.1.2 | Meets the requirements specified in BR 4.9.1.2 |
| 4.9.2. Who Can Request Revocation | CPS 4.9.2 | Meets the requirements specified in BR 4.9.2 |
| 4.9.3. Procedure for Revocation Request | CPS 4.9.3 | Meets the requirements specified in BR 4.9.3 |
| 4.9.5. Time within which CA Must Process the Revocation Request | CPS 4.9.5 | Meets the requirements specified in BR 4.9.5 |
| 4.9.7. CRL Issuance Frequency | CPS 4.9.7 | Meets the requirements specified in BR 4.9.7 |
| 4.9.9. On-line Revocation/Status Checking Availability | CPS 4.9.9 | Meets the requirements specified in BR 4.9.9 |
| 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, preventing errounious return of "good" status. | CPS 4.9.10 | Meets the requirements specified in BR 4.9.10 |
| 4.9.11. Other Forms of Revocation Advertisements Available<br>Indicate if your CA supports OCSP stapling. | Not applicable | Entrust does not rely on stapling to distribute OCSP responses. |
| 4.10.1. Operational Characteristics | CPS 4.10.1 | Meets the requirements specified in BR 4.10.1 |
| 4.10.2. Service Availability | CPS 4.10.2 | Meets the requirements specified in BR 4.10.2 |
| 5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS | CPS 5 and sections | Meets the requirements specified in BR 5 |
| 5.2.2. Number of Individuals Required per Task | CPS 5.2.2 | Meets the requirements specified in BR 5.2.2 |
| 5.3.1. Qualifications, Experience, and Clearance Requirements | CPS 5.3.1 | Meets the requirements specified in BR 5.3.1 |
| 5.3.3. Training Requirements and Procedures | CPS 5.3.3 | Meets the requirements specified in BR 5.3.3 |
| 5.3.4. Retraining Frequency and Requirements | CPS 5.3.4 | Meets the requirements specified in BR 5.3.4 |
| 5.3.7. Independent Contractor Controls | CPS 5.3.7 | Meets the requirements specified in BR 5.3.7 |
| 5.4.1. Types of Events Recorded | CPS 5.4.1 | Meets the requirements specified in BR 5.4.1 |
| 5.4.3. Retention Period for Audit Logs | CPS 5.4.3 | Meets the requirements specified in BR 5.4.3 |
| 5.4.8. Vulnerability Assessments | CPS 5.4.8 | Meets the requirements specified in BR 5.4.8 |
| 5.5.2. Retention Period for Archive | CPS 5.5.2 | Meets the requirements specified in BR 5.5.2 |
| 5.7.1. Incident and Compromise Handling Procedures | CPS 5.7 | Meets the requirements specified in BR 5.7.1 |
| 6.1.1. Key Pair Generation | CPS 6.1.1 | Meets the requirements specified in BR 6.1.1 |
| 6.1.2. Private Key Delivery to Subscriber | CPS 6.1.2 | Meets the requirements specified in BR 6.1.2 |
| 6.1.5. Key Sizes | CPS 6.1.5 | Meets the requirements specified in BR 6.1.5 |
| 6.1.6. Public Key Parameters Generation and Quality Checking | CPS 6.1.6 | Meets the requirements specified in BR 6.1.6 |

| | | |
|---|---|---|
| 6.1.7. Key Usage Purposes | CPS 6.1.7 | Meets the requirements specified in BR 6.1.7 |
| 6.2. Private Key Protection and Cryptographic Module Engineering Controls | CPS 6.2 | Meets the requirements specified in BR 6.2 |
| 6.2.5. Private Key Archival | CPS 6.2.5 | Meets the requirements specified in BR 6.2.5 |
| 6.2.6. Private Key Transfer into or from a Cryptographic Module | CPS 6.2.6 | Meets the requirements specified in BR 6.2.6 |
| 6.2.7. Private Key Storage on Cryptographic Module | CPS 6.2.7 | Meets the requirements specified in BR 6.2.7 |
| 6.3.2. Certificate Operational Periods and Key Pair Usage Periods | CPS 6.3.2 | Meets the requirements specified in BR 6.3.2 |
| 6.5.1. Specific Computer Security Technical Requirements | CPS 6.5.1 | Meets the requirements specified in BR 6.5.1 |
| 7.1. Certificate profile | CPS 7.1 | Meet the requirements specified in BR 7.1 |
| 7.1.1. Version Number(s) | CPS 7.1.1 | Meet the requirements specified in BR 7.1.1 |
| 7.1.2. Certificate Content and Extensions; Application of RFC 5280 | N/A as BR has no requirements | N/A |
| 7.1.2.1 Root CA Certificate | CPS 7.1.2.1 and Appendix A | Meet the requirements specified in BR 7.1.2.1 |
| 7.1.2.2 Subordinate CA Certificate | CPS 7.1.2.2 and Appendix A | Meet the requirements specified in BR 7.1.2.2 |
| 7.1.2.3 Subscriber Certificate | CPS 7.1.2.3 and Appendix A | Meet the requirements specified in BR 7.1.2.3 |
| 7.1.2.4 All Certificates | CPS 7.1.2.4 and Appendix A | Meet the requirements specified in BR 7.1.2.4 |
| 7.1.2.5 Application of RFC 5280 | CPS 7.1.2.5 | Meet the requirements specified in BR 7.1.2.5 |
| 7.1.3. Algorithm Object Identifiers | CPS 7.1.3 | Meet the requirements specified in BR 7.1.3 |
| 7.1.4. Name Forms | N/R as BR has no requirements | N/A |
| 7.1.4.1 Issuer Information | CPS 7.1.4.1 and Appendix A | Meet the requirements specified in BR 7.1.4.1 |
| 7.1.4.2 Subject Information | CPS 7.1.4.2 and Appendix A | Meet the requirements specified in BR 7.1.4.2 |
| 7.1.4.3 Subject Information - Subordinate CA Certificates | CPS 7.1.4.3 and Appendix A | Meet the requirements specified in BR 7.1.4.3 |
| 7.1.5. Name Constraints | N/A | Entrust does not use name constraints |
| 7.1.6. Certificate Policy Object Identifier | N/A as BR has no requirements | N/A |
| 7.1.6.1 Reserved Certificate Policy Identifiers | CPS 7.1.6.1 | Meet the requirements specified in BR 7.1.6.1 |
| 7.1.6.2 Root CA Certificates | CPS 7.1.6.2 | Meet the requirements specified in BR 7.1.6.2 |
| 7.1.6.3 Subordinate CA Certificates | CPS 7.1.6.3 | Meet the requirements specified in BR 7.1.6.3 |
| 7.1.6.4 Subscriber Certificates | CPS 7.1.6.4 | Meet the requirements specified in BR 7.1.6.4 |
| 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS | CPS 1.1, 8.4, 9.14 | Meet the requirements specified in BR 8 |
| 8.1. Frequency or circumstances of assessment | CPS 8.1 | Meet the requirements specified in BR 8.1 |
| 8.2. Identity/qualifications of assessor | CPS 8.2 | Meet the requirements specified in BR 8.2 |
| 8.4. Topics covered by assessment | CPS 8.4 | Meet the requirements specified in BR 8.4 |
| 8.6. Communication of results | CPS 8.6 | Meet the requirements specified in BR 8.6 |
| 8.7. Self-Audits | CPS 8.7 | Meet the requirements specified in BR 8.7 |
| 9.6.1. CA Representations and Warranties | CPS 1.1 (2nd paragraph); CPS 9.6.1 | Meets the requirements specified in BR 9.6.1 |
| 9.6.3. Subscriber Representations and Warranties | CPS 9.6.3; Subscription Agreement 4 | Meets the requirements specified in BR 9.6.3 |
| 9.8. Limitations of liability | CPS 9.8; Subscription Agreement 8; RPA 4 | Meets the requirements specified in BR 9.8 |
| 9.9.1. Indemnification by CAs | CPS 9.9.1 | Meets the requirements specified in BR 9.9.1 |

|  |  |  |
|---|---|---|
| 9.16.3. Severability | CPS 9.16.3 | Meets the requirements specified in BR 9.16.3; no conflicts or modified requirements reported. |