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

Introduction must include:
1) CA's Legal Name: iTrusChina Co., Ltd.(北京天威诚信电子商务服务有限公司)
2) Clear indication (subject and SHA1 or SHA256 fingerprints) about which root certificates are being evaluated, and their full CA hierarchy. In considering a root certificate for inclusion in NSS, Mozilla must also evaluate the current subordinate CAs and the selection/approval criteria for future subordinate CAs. Mozilla's CA Certificate Policy requires full disclosure of non-technically-constrained intermediate certificates chaining up to root certificates in NSS.
SHA256 fingerprints:
vTrus Root CA
8A:71:DE:65:59:33:6F:42:6C:26:E5:38:80:D0:0D:88:A1:8D:A4:C6:A9:1F:0D:CB:61:94:E2:06:C5:C9:63:87
vTrus ECC Root CA
30:FB:BA:2C:32:23:8E:2A:98:54:7A:F9:79:31:E5:50:42:8B:9B:3F:1C:8E:EB:66:33:DC:FA:86:C5:B2:7D:D3
As for the CA hierarchy, please see the attachments "iTrusChina CA Hierarchy"
3) List the specific version(s) of the BRs that you used.
BR version 1.6.4
4) List the specific versions of the CA's documents that were evaluated, and provide direct URLs to those documents. All provided CA documents must be public-facing, available on the CA's website, and translated into English.
Please visit https://www.itrus.com.cn/repository and download the version 1.3 CP and CPS.
5) If you intend to submit your self-assessment with statements such as "will add/update in our next version of CP/CPS", indicate when you plan to provide the updated documents.
Not applicable.

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 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/CPS Version Description page	CP/CPS Version Description page
1.2.2. Relevant Dates 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.*	CP/CPS Version Description page	The CP and CPS are up to date and the stated practices are fully implemented.
1.3.2. Registration Authorities 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.*	CP/CPS 1.3.2	iTrusChina is also the RA and no more delegate RA.
2.1. Repositories *Provide the direct URLs to the CA's repositories*	CP/CPS 2.1	https://www.itrus.com.cn/repository
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." *--> Copy the specific text that is used into the explanation in this row. (in English)*	CP/CPS V1.2 2.2	iTrusChina provides CRL and OCSP service.The publications are available on this site: https://www.itrus.com.cn/repository

2.2. Publication of information "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." *--> 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/CPS 2.2	iTrusChina provides CRL and OCSP service.The publications are available on this site: https://www.itrus.com.cn/repository
2.3. Time or frequency of publication *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/CPS 2.3	iTrusChina releases CP and CPS at least once a year. And iTrusChina performs BR self-assessment every year according to BR.
2.4. Access controls on repositories *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/CPS 2.4	The CPS states that the Repository is publicly available.
3.2.2.1 Identity 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.	CP/CPS 3.2.2.1	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.2 DBA/Tradename 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.	CP/CPS 3.2.2.2	Not applicable
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	CP/CPS 3.2.2.3	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.4 Validation of Domain Authorization or Control *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.***	CP/CPS 3.2.2.4	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.4.1 Validating the Applicant as a Domain Contact 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	No stipulation
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact 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/CPS 3.2.2.4.1	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.4.3 Phone Contact with Domain Contact 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	No stipulation

3.2.2.4.4 Constructed Email to Domain Contact 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/CPS 3.2.2.4.1	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.4.5 Domain Authorization Document 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	No stipulation
3.2.2.4.6 Agreed - Upon Change to Website 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/CPS 3.2.2.4.2	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.4.7 DNS Change 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/CPS 3.2.2.4.3	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.4.8 IP Address 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	No stipulation
3.2.2.4.9 Test Certificate 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	No stipulation
3.2.2.4.10. TLS Using a Random Number 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	No stipulation
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, *indicate how your CA meets the requirements in this section of the BRs.*	CP/CPS 3.2.2.5	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.6 Wildcard Domain Validation 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/CPS 3.2.2.6	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	CP/CPS 3.2.2.7	The certificate validation methods used by iTrusChina are described in this section.
3.2.2.8 CAs MUST check and process CAA records *Indicate your CA's understanding that this section is a requirement as of September 8, 2017, and how your CA meets the requirements in this section of the BRs.*	CP/CPS中3.2.2.8	As described in this section.
3.2.3. Authentication of Individual Identity	CP/CPS 3.2.3	As described in this section.
3.2.5. Validation of Authority	CP/CPS 3.2.5	As described in this section.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CP/CPS 3.2.6	As described in this section.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CP/CPS 4.1.1	
4.1.2. Enrollment Process and Responsibilities	CP/CPS 4.1.2	As described in this section.
4.2. Certificate application processing	CP/CPS 4.2	As described in this section.

4.2.1 Re-use of validation information is limited to 825 days *Indicate your CA's understanding that this is a requirement as of March 1, 2018, and indicate how your CA meets the requirements of this section.*	CP/CPS 4.8.1	As described in this section.
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.*	CP/CPS 4.2.1	As described in this section.
4.2.2. Approval or Rejection of Certificate Applications	CP/CPS 4.2.2	As described in this section.
4.3.1. CA Actions during Certificate Issuance	CP/CPS 4.3.1	As described in this section.
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	CP/CPS 4.9.1.1	The reasons are listed in Section 4.9.1.1 CPS
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.	CP/CPS 4.9.1.2	As described in this section.
4.9.2. Who Can Request Revocation	CP/CPS 4.9.2	As described in this section.
4.9.3. Procedure for Revocation Request	CP/CPS 4.9.3	As described in this section.
4.9.5. Time within which CA Must Process the Revocation Request	CP/CPS 4.9.5	As described in this section.
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	CP/CPS 4.9.7	For the subscriber certificates, the CRL publication cycle of iTrusChina shall not exceed 96 hours. For the subordinate CA certificates, the CRL publication cycle of iTrusChina shall not exceed 12 months
4.9.8 Maximum Latency for CRLs	CP/CPS 4.9.8	The maximum latency for CRL publication of iTrusChina is within 24 hours after the publication cycle.
4.9.9. On-line Revocation/Status Checking Availability	CP/CPS 4.9.9	iTrusChina shall provide certificate subscribers and relying parties with online certificate status protocol (OCSP) services. OCSP service of iTrusChina meets the requirements of RFC6960 and are signed with special OCSP service certificates.
4.9.10. On-line Revocation Checking Requirements *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.*	CP/CPS 4.9.10	As described in this section.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CP/CPS 4.9.11	Apart from CRL or OCSP servers for certificate revocation information query, iTrusChina does not provide other publication forms of revocation information.
4.9.12Special Requirements Related to Key Compromise	CP/CPS 4.9.12	
4.9.13Circumstances for Certificate Suspension	CP/CPS 4.9.13	iTrusChina does not support certificate suspension.
4.9.14Who can Request Certificate Suspension	CP/CPS 4.9.14	Not applicable.
4.9.15Procedures for Suspension Reques	CP/CPS 4.9.15	Not applicable.
4.9.16Limits on Suspension Period	CP/CPS 4.9.16	Not applicable.
4.10.1. Operational Characteristics	CP/CPS 4.10.1	As described in this section.
4.10.2. Service Availability	CP/CPS 4.10.2	Both CRL and OCSP certificate status query services of iTrusChina are 7 * 24 available and designed to minimize downtime.
4.10.3Optional Features	N/A	N/A
4.11End of Subscription	CP/CPS 4.11	
4.12Key Escrow and Recovery	CP/CPS 4.12	iTrusChina does not hold any private key in escrow for SSL certificate subscribers, thereby not providing key recovery service.
4.12.1Policy and Practices of Key Escrow and Recovery	CP/CPS 4.12.1	Not applicable.
4.12.2Policy and Practices of Session Key Encapsulation and Recovery	CP/CPS 4.12.2	Not applicable.
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	CP/CPS 5	
5.2.2. Number of Individuals Required per Task	CP/CPS 5.2.2	

5.3.1. Qualifications, Experience, and Clearance Requirements	5.3.1 5.3.2	As described in this section.
5.3.3. Training Requirements and Procedures	CP/CPS 5.3.3	As described in this section.
5.3.4. Retraining Frequency and Requirements	CP/CPS 5.3.4	Those who act as trusted roles or other important roles receive a training organized by iTrusChina at least once a year. Those who are related to the certification system operation receive relevant skill and knowledge training at least once a year. In addition, iTrusChina will irregularly require the personnel to continue the training according to the requirements of system upgrades and configuration modifications, etc.
5.3.7. Independent Contractor Controls	CP/CPS 5.3.7	iTrusChina doesn't hire external personnel engaged in the work related to certificate validation for now
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	CP/CPS 5.4.1	As described in this section.
5.4.3. Retention Period for Audit Logs	CP/CPS 5.4.3	iTrusChina keeps the audit log of the CA service properly, and the audit log related to the certificate is retained for at least 7 years after the certificate expired
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	CP/CPS 5.4.8	According to security events found by the audit, iTrusChina will conduct the annual security vulnerability assessment of the system, physical sites, operation management, etc., and take measures to reduce the operational risk based on the assessment report.
5.5.2. Retention Period for Archive	CP/CPS 5.5.2	The life cycle management records of subscriber certificates are kept until 7 years after the certificate expired. The other records are retained for 7 years.
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	CP/CPS 5.7.1	As described in this section.
6.1.1. Key Pair Generation	CP/CPS 6.1.1	As described in this section.
6.1.2. Private Key Delivery to Subscriber	N/A	Not applicable.
6.1.5. Key Sizes	CP/CPS 6.1.5	Subscriber key pairs provided by iTrusChina include two types: 2048-bit or 4096-bit RSA keys, and 256-bit or 384-bit ECC keys. Signature algorithms are sha256RSA, sha384RSA, sha256ECDSA and sha384ECDSA.
6.1.6. Public Key Parameters Generation and Quality Checking	CP/CPS 6.1.6	As described in this section.
6.1.7. Key Usage Purposes	CP/CPS 6.1.7	As described in this section.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CP/CPS 6.2.1	As described in this section.
6.2.5. Private Key Archival	CP/CPS 6.2.5	As described in this section.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CP/CPS 6.2.6	As described in this section.
6.2.7. Private Key Storage on Cryptographic Module	CP/CPS 6.2.7	As described in this section.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	CP/CPS 6.3.2	The maximum validity period of the CA certificate is no more than 25 years, and the subscriber SSL certificate is valid for a maximum of 825 days.
6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. *Indicate how your CA meets the requirements of this section.*	CP/CPS 6.5.1	As described in this section.
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. *Indicate how your CA meets the requirements of this section.*	CPS7.1	
7.1.1. Version Number(s)	CPS7.1.1	X.509 V3
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CPS7.1.2	
7.1.2.1 Root CA Certificate	CPS7.1.2	
7.1.2.2 Subordinate CA Certificate	CPS7.1.2	
7.1.2.3 Subscriber Certificate	CPS7.1.2	
7.1.2.4 All Certificates	CPS7.1.2	
7.1.2.5 Application of RFC 5280	CPS7.1.2	
7.1.3. Algorithm Object Identifiers	CPS7.1.3	sha256RSA、sha384RSA、sha256ECDSA、sha384ECDSA
7.1.4. Name Forms	CPS7.1.4	

7.1.4.1 Issuer Information	CPS7.1.4	
7.1.4.2 Subject Information - Subscriber Certificates	CPS7.1.4	
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CPS7.1.4	
7.1.5. Name Constraints Indicate your CA's understanding of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section.	N/A	
7.1.6. Certificate Policy Object Identifier	CPS 7.1.6	As defined in this CPS 1.2.
7.1.6.1 Reserved Certificate Policy Identifiers	CPS 7.1.6	
7.1.6.2 Root CA Certificates	CPS 7.1.6	
7.1.6.3 Subordinate CA Certificates	CPS 7.1.6	
7.1.6.4 Subscriber Certificates	CPS 7.1.6	
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CP/CPS 8	
8.1. Frequency or circumstances of assessment 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. 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. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	CP/CPS 8.1	As described in this section.
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	CP/CPS 8.2	
8.4. Topics covered by assessment	CP/CPS 8.4	
8.6Delivery and Publication of Results	CP/CPS 8.6	
Also indicate your understanding and compliance with 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). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - 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		See audit report.
8.7Other Assessments	CP/CPS 8.7	According to the requirements of Electronic Signature Law of the People's Republic of China, Measures for the Administration of Electronic Certification Services, and Regulations on Cryptographic Management of Electronic Certification Services, etc., it is subject to certificate renewal and review by competent authorities every five years.
9.6.1. CA Representations and Warranties	CPS 9.6.1	As described in this section.
9.6.3. Subscriber Representations and Warranties	CPS 9.6.3	As described in this section.
9.8. Limitations of liability	CPS 9.8	Certificate subscribers and relying parties suffer losses in civil activities due to electronic certification services provided by iTrusChina, and iTrusChina will bear the limited liability of indemnification stipulated in Section 9.9 of this CPS.

9.9.1. Indemnification by Cas	CPS 9.9.1	As described in this section.
9.16.3. Severability	CPS 9.16.3	As described in this section.