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

Introduction must include:

Introduction

1) CA's Legal Name

Beijing Certificate Authority Co.,Ltd. (referred to as "BJCA", or "数字认证")

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.

[BJCA Global Root CA1]

[ROOT] BJCA Global Root CA1 (D5EC8D7B4CBA79F4E7E8CB9D6BAE77831003216A)

Download http://repo.bjca.cn/global/cert/BJCA_Global_Root_CA1.crt

[SUBCA DV SSL] BJCA DV SSL CA1 (70B2B43140A8209FE3686476E455482E5591FB30)

Download http://repo.bjca.cn/global/cert/BJCA_DV_SSL_CA1.crt

[SUBCA IV SSL] BJCA IV SSL CA1 (19B542B7B97422418E28FAE255F98F9436EAE49B)

Download http://repo.bjca.cn/global/cert/BJCA_IV_SSL_CA1.crt

[SUBCA OV SSL] BJCA OV SSL CA1 (0A22BC3871D1402BDD48CDB0EA46969F3E40DCF1)

Download http://repo.bjca.cn/global/cert/BJCA_OV_SSL_CA1.crt

[SUBCA EV SSL] BJCA EV SSL CA1 (6C8C0FE05B07DF3EC60248A44EF5B07863D38CB2)

Download http://repo.bjca.cn/global/cert/BJCA_EV_SSL_CA1.crt

[BJCA Global Root CA2]

[ROOT] BJCA Global Root CA2 (F42786EB6EB86D88316702FBBA66A45300AA7AA6)

Download http://repo.bjca.cn/global/cert/BJCA_Global_Root_CA2.crt

[SUBCA DV SSL] BJCA DV SSL CA2 (BA0866235B8CA2DAE7E56495DEB0664BB67ADDAC)

Download http://repo.bjca.cn/global/cert/BJCA_DV_SSL_CA2.crt

[SUBCA IV SSL] BJCA IV SSL CA2 (07C381DFC16F3CC389F4628302E64BADC4112C33)

Download http://repo.bjca.cn/global/cert/BJCA_IV_SSL_CA2.crt

[SUBCA OV SSL] BJCA OV SSL CA2 (387EBE6C0015EA74B9EF42694C9EBB617E971D61)

Download http://repo.bjca.cn/global/cert/BJCA_OV_SSL_CA2.crt

[SUBCA EV SSL] BJCA EV SSL CA2 (925377774599ACA7417523DB15E8A5E5EC30E6C2)

Download http://repo.bjca.cn/global/cert/BJCA_EV_SSL_CA2.crt

3) Version(s) of the BRs that were used

Version v1.6.8 https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.8.pdf

4) Policy

[CP] Beijing Certificate Authority Co., Ltd. Global Certificate Policy v1.0.2 https://www.bjca.cn/cps/BJCA Global CP.pdf

[CPS] Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement v1.0.2 https://www.bjca.cn/cps/BJCA Global CPS.pdf

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.

Annually or when dictated by changes to industry standards.

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] Beijing Certificate Authority Co., Ltd. Global Certificate Policy v1.0.2 Effective Date: March 6, 2020 [CPS] Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement v1.0.2 Effective Date: March 6, 2020	BJCA are fully compliant with the items listed in this table.
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 Control Table.	Please refer to Version Control Table of the CP and CPS, BJCA are fully compliant with the items listed in this table.
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 (including non-delegation of domain validation to RAs).	CP/CPS 1.3.2	BJCA itself serves the role of RA and performs RA's operation in accordance with its CPS. BJCA does not permit any delegated third party to be the RA counter to verify the ownership or control of domain names or IP addresses.
1.5.2 Contact person 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.	CP/CPS 1.5.2	BJCA receives certificate problem reports and certificate revocation requests by mail or telephone.
2.1. Repositories *Provide the direct URLs to the CA's repositories*	CP/CPS 2.1 and 2.2	The website of BJCA repository is at https://www.bjca.cn
2.2 Publication of information - RFC 3647 "Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**."	CP v1.0.2 CPS v1.0.2	CP and CPS are structured according to RFC 3647.

2.2 Publication of information - CAA Effective as of 8 September 2017 ... 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/CPS 2.2	The issuer domain names, that is, the Certification Authority CAA identifying domains for CAs, within BJCA's operational control are "bjca.cn".
2.2. Publication of information - BR text "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 1.1.2	BJCA follows the requirements of the latest versions of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements" for short), regularly review the updates and will continue to revise this CPS in accordance with the newly published versions. If there is any inconsistency between the terms of this CPS and the relevant specifications issued by the international CA/Browser forum, the specifications officially issued by the international CA/Browser forum shall prevail.
2.2. Publication of information - test websites "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.***	BJCA Global Root CA1 https://demossl-rsa-valid.bjca.org.cn https://demossl-rsa-expired.bjca.org.cn https://demossl-rsa-revoked.bjca.org.cn BJCA Global Root CA2 https://demossl-ecc-valid.bjca.org.cn https://demossl-ecc-expired.bjca.org.cn https://demossl-ecc-revoked.bjca.org.cn	All links for the root certificate are provided.

2.3. Time or frequency of publication "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. Section 3.3 of Mozilla's Root Store Policy states: "CPs and CPSes MUST be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements. **CAs MUST indicate that this has happened by incrementing the version number and adding a dated changelog entry**, even if no other changes are made to the document." *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 and 1.5.5	BJCA releases CP and CPS at least once a year. If there is no change in content, increase the version number and update the publish time, effective time and revision history.
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 2.1 and 2.4	BJCA repository is responsible for the publication and storage of root certificates and subordinate CA certificates, current and historical versions of CP and CPS, CRLs. The repository provides 24-hour round-the-clock service.
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 3.1.2 and 3.2.2.1	The subject names of organizations must conform to the subject naming regulations under our country's law and use the official registered name. Application information includes the organization name, location and representative name which is sufficient to identify an organization. The private organization shall provide the photocopies of the related identification documents which are issued by the supervisory authorities and/or legally authorized entities. BJCA shall confirm the existence of the organization as well as the authenticity of the

		application, representative identity and the representative's authority to represent the organization.
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	If the certificate subject contains a DBA or tradename, BJCA shall verify the applicant's right to use the DBA or tradename using at least one of the following ways. (1) Documents provided by a government agency in the jurisdiction of the applicant's legal creation, existence, or recognition. (2) A reliable data source. (eg: DUNS) (3) Communicate with a government agency responsible for the management of such DBAs or tradenames. (4) A utility bill, bank statement, government-issued tax document, or other form of identification that the CA determines to be reliable.
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	If the certificate subject contains an option of country, BJCA shall verify the country using one of the following ways. (1) Confirm ensure that the country where the applicant's IP address is located is consistent with the actual country where the applicant is located. (2) The ccTLD of the requested domain name. (3) Information provided by the domain name registrar. (4) The related identification

		documents which are issued by the supervisory authorities and/or legally authorized entities.
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.* ***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/CPS 3.2.2.4, 3.2.2.9, 3.2.2.10, 3.2.2.11 and 3.2.2.12	Please refer to Section 3.2.2.9 to Section 3.2.2.12, which meets the requirements of BR 3.2.2.4 methods 2, 4, 6 and 7. (1) For DV SSL certificate, BJCA shall validate the applicant's right to use or control each domain name in accordance with the Baseline Requirements. (2) For OV and IV SSL certificate, in addition to validate the applicant's domain control right, BJCA shall validate organization or individual's identity in accordance with the Baseline Requirements and Sections 3.2.2.1 or 3.2.3 of the CPS. (3) For EV SSL certificate, in addition to perform the above procedures (1) and (2), the authorization of the contract signer and certificate approver must be verified in accordance with the EV SSL Certificate Guidelines.
3.2.2.4.1 Validating the Applicant as a Domain Contact For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.	This method SHALL NOT be used.	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	Send a random value by email, and receive a confirming response using the random value to confirm the applicant's ownership of the FQDN. The random value must be sent to the domain name contact email address registered by WHOIS. (Based on the domain name validation method of Baseline Requirements Section 3.2.2.4.2) The random value used in the above validation method is remain valid for no more than 30 days from the time of creation.
3.2.2.4.3 Phone Contact with Domain Contact **CAs SHALL NOT perform validations using this method after May 31, 2019**. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.	This method SHALL NOT be used after May 31, 2019.	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 3.2.2.4.2	Send a random value by email, and receive a confirming response using the random value to confirm the applicant's ownership of the FQDN. The random value must be sent to the email address identified as the domain name contact or created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster', followed by the at-sign ("@"), followed by an authorized domain name. (Based on the domain name validation method of Baseline Requirements Section 3.2.2.4.4) The random value used in the above validation method is remain valid for no more than 30 days from the time of creation.
3.2.2.4.5 Domain Authorization Document "For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed	This method SHALL NOT be used.	No stipulation.

validations using this method SHALL NOT be used for the issuance of certificates."		
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 3.2.2.4.3	Confirm the subscriber's ownership of the FQDN by making changes to the agreed information under the "/.well-known/pki-validation" directory. (Based on the domain name validation method of Baseline Requirements Section 3.2.2.4.6)
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 3.2.2.4.4	Confirm the subscriber's ownership of the domain name by confirming the presence of a negotiated random value in a DNS CNAME, TXT or CAA record. (Based on the validation method of domain name in Baseline Requirements Section 3.2.2.4.7) The random value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.
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.*	No stipulation.	No stipulation.
3.2.2.4.9 Test Certificate **"This method has been retired and MUST NOT be used."**	This method SHALL NOT be used.	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.* *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.***	No stipulation.	No stipulation.
3.2.2.4.11 Any Other Method **"This method has been retired and**	This method SHALL NOT be used.	No stipulation.

MUST NOT be used."		
3.2.2.4.12 Validating Applicant as a Domain Contact "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." 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.*	No stipulation.	No stipulation.
3.2.2.4.13 Email to DNS CAA 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.*	No stipulation.	No stipulation.
3.2.2.4.14 Email to DNS TXT 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.*	No stipulation.	No stipulation.
3.2.2.4.15 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.*	No stipulation.	No stipulation.
3.2.2.4.16 Phone Contact with DNS TXT Record Phone 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.*	No stipulation.	No stipulation.
3.2.2.4.17 Phone Contact with DNS CAA Phone 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.*	No stipulation.	No stipulation.
3.2.2.4.18 Agreed-Upon Change to Website v2 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.	No stipulation.	No stipulation.

3.2.2.4.19 Agreed-Upon Change to Website - ACME 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.	No stipulation.	No stipulation.
3.2.2.5 Authentication for an IP Address 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.* **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."**	CP/CPS 3.2.2.5, 3.2.2.9, 3.2.2.10 and 3.2.2.11	Please refer to Section 3.2.2.9 to Section 3.2.2.11, which meets the requirements of BR 3.2.2.5 methods 1, 2, 3, and 5. BJCA do not allow IP Addresses to be listed in EV SSL certificate.
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	BJCA shall confirm the applicant's ownership of and control over the domain name to the right of the wildcard through the verification and authentication method of the domain name in Section 3.2.2.4
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 BJCA are described in this section. Meets the requirements of BR 3.2.2.7.
3.2.2.8 CAs MUST check and process CAA records *Indicate how your CA meets the requirements in this section of the BRs.* *Section 2.2 of the BRs states: "****CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain***	CP/CPS 3.2.2.8	BJCA will check for CAA records for each dNSName in the certificate subject alias extension before issuing the SSL certificate that meets the requirements of the CA/Browser Forum Baseline Requirements and EV Guidelines. The CA will issue a certificate to the certificate applicant within 8

Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."		hours of the CAA record. If it exceeds 8 hours, the CA will re-check the CAA.
3.2.3. Authentication of Individual Identity	CP/CPS 3.2.3	Please refer to Section 3.2.3, the content in this section meets the requirements of BR 3.2.3.
3.2.5. Validation of Authority	CP/CPS 3.2.5	Please refer to Section 3.2.5, the content in this section meets the requirements of BR 3.2.5.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CP/CPS 3.2.6	By now, BJCA has not issued any cross-certification certificate.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CP/CPS 4.1.1 and 4.2.2	The certificate application entities include individuals and organizations with independent legal personality. After BJCA identifies and authenticates the identity of the certificate applicant according to the identity authentication procedure stipulated in this CPS 3.2, it decides to approve or reject the certificate application according to the identification result.
4.1.2. Enrollment Process and Responsibilities	CP/CPS 4.1.2	Enrollment Process and Responsibilities are listed in Section 4.1.2.
4.2. Certificate application processing	CP/CPS 4.2	Certificate application processing are listed in Section 4.2.

4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.* **Re-use of validation information is limited to 825 days**	CP/CPS 4.2.1 and 4.2.2	BJCA identifies and authenticates the identity of the applicant according to the identity authentication procedure stipulated in this CPS 3.2. Prior to the issuance of a SSL Certificate, if the time of obtaining data or certification by the CA under Section 3.2 of this CPS does not exceed the maximum validity period 2 years of the server certificate as specified in Section 6.3.2 of this CPS, and the information has not changed, the CA can reuse the data or supporting documents to identify and authenticate the subscriber identity. BJCA establishes and maintains a list of high-risk applicants for certificates, and will check the list when accepting certificate applications. For applicants in the list, the CA will reject the application. For issued certificates, they will be reviewed periodically according to the list. Once the certificate holder is found in the list, the CA has the right to revoke the certificate or take appropriate mechanism to deal with it.
4.2.2. Approval or Rejection of Certificate Applications "Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each	CP/CPS 4.2.2	BJCA has the right to reject the certificate application if: 1) According to the provisions of Section 3.2, not all necessary subscriber information can be identified and authenticated; 2) The subscriber cannot provide the required identity documents; 3) The subscriber objected or could not accept the relevant content and requirements of the subscriber agreement; 4) The subscriber fails to or cannot pay corresponding fees as required; 5) The certificate applied for

Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name."		contains a new top-level domain name under consideration by ICANN; 6) The CA believes that the approval of the application will bring disputes, legal disputes or losses to BJCA.
4.3.1. CA Actions during Certificate Issuance	CP/CPS 4.3.1	During the issuance process of the subscriber certificate, the entry clerk of the CA is responsible for entering the information submitted by the applicant, and the reviewer is responsible for the approval of the application, and the request for certificate is sent to the CA certificate issuance system by operating the RA system. The certificate issuance request information issued by the RA requires the identity authentication and information security measures of the RA, and ensures that the request is sent to the right CA. After obtaining the certificate issuance request, the CA shall determine its validity, and issue the certificate after approving the application. The issuance of the certificate means that the CA has approved the certificate application completely and formally.
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	All revocation requirements in the BR are listed in this section.

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	All revocation requirements in the BR are listed in this section. BJCA shall revoke a subordinate CA certificate within 7 days if one or more of the following occurs: 1. The CA obtains evidence that the private key of the subordinate CA corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of Baseline Requirements; 2. The CA obtains evidence that the certificate was misused; 3. The CA is made aware that the certificate was not issued in accordance with the Baseline Requirements or relevant requirements of the CP/CPS issued by the CA; 4. The CA determines that any of the information appearing in the certificate is inaccurate or misleading; 5. The CA or the subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate; 6. The CA's rights to issue certificates under Baseline Requirements expires, or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP repository.
4.9.2. Who Can Request Revocation	CP/CPS 4.9.2	Depending on the circumstances, the subscriber, CA, or the RA can initiate revocation. In addition, subscribers, relying parties, application software suppliers and other third parties may submit certificate problem reports informing the CA of reasonable cause to revoke the

		certificate.
4.9.3. Procedure for Revocation Request	CP/CPS 4.9.3	Procedure for Revocation Request are listed in Section 4.9.3. 1) A Subscriber Makes An Application for Revocation on One's Own Initiative; 2) A Subscriber is Forced to Revoke A Certificate; 3) Revocation of electronic certification service organization certificate.
4.9.5. Time within which CA Must Process the Revocation Request	CP/CPS 4.9.5	within 24 hours from receipt of the Revocation Request.
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	The subscriber certificate CRLs are generally issued regularly for 24 hours, and the subscriber certificate CRLs are valid for no more than 3 days. The subordinate CA certificate CRLs are generally issued every 12 months.
4.9.9. On-line Revocation/Status Checking Availability	CP/CPS 4.9.9	BJCA provides the Online Certificate Status Protocol (OCSP) service to subscribers and relying parties. The OCSP response complies with RFC 6960 and will be signed by the CA and OCSP responders that verify their certificate revocation status. The certificate of signing certificate server used by the OCSP responder is issued by the same CA as the certificate being queried, and contains an extension of type id-pkix-ocsp-nocheck defined by RFC 6960.

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	BJCA provides OCSP query services in both Get and Post methods. For the status of subscriber certificates, the CA shall update information provided via the OCSP at least every four days. OCSP responses must have a maximum expiration time of 10 days. For certificates that have been revoked, update the OCSP immediately. For the status of subordinate CA certificates, the CA shall update information provided via the OCSP at least every 12 months and within 24 hours after revoking a subordinate CA certificate. If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder shall not respond with a “good” status.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CP/CPS 4.9.11	Certificate revocation information can be obtained through CRL or OCSP services. BJCA does not provide other forms of certificate revocation information.
4.10.1. Operational Characteristics	CP/CPS 4.10.1	The status of the certificate can be queried through the CRL and OCSP services provided by BJCA. For a certificate that has been revoked, BJCA does not delete its revocation record in the CRL. BJCA does not delete the revocation record in the OCSP server.
4.10.2. Service Availability	CP/CPS 4.10.2	BJCA provides a 7X24 hours certificate status query service with a query response time of no more than 10 seconds.
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	covered by the CPS	Meets the requirements specified in BR 5.
5.2.2. Number of Individuals Required per Task	CP/CPS 5.2.2 and 5.2.4	As stated in the table of this section, which meets the

		requirements of BR 5.2.2.
5.3.1. Qualifications, Experience, and Clearance Requirements	CP/CPS 5.3.1 and 5.3.2	Meets the requirements of BR 5.3.1.
5.3.3. Training Requirements and Procedures	CP/CPS 5.3.3	As stated in the table of this section, which meets the requirements of BR 5.3.3.
5.3.4. Retraining Frequency and Requirements	CP/CPS 5.3.4	For those who act as trusted or other important roles, they shall be trained at least once a year by BJCA to ensure that they maintain the skill level that enables them to perform such duties satisfactorily. When the Certification Policy is adjusted and the system is updated, all personnel shall be retrained to adapt to new changes.
5.3.7. Independent Contractor Controls	CP/CPS 5.3.7	BJCA 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	The required items are listed in this section of CP and CPS.
5.4.3. Retention Period for Audit Logs	CP/CPS 5.4.3	The CA system audit logs shall be retained for at least ten years and be available to qualified auditors upon request.
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	CP/CPS 5.4.8	BJCA conducts vulnerability assessments on the system, such as a vulnerability scan on a quarterly basis, a penetration testing on a yearly basis, and conducts risk assessments, such as identifying internal and external threats, certificate data and management risks, and whether policies and procedures for responding to these risks are complete so as to reduce the risk of system operation.
5.5.2. Retention Period for Archive	CP/CPS 5.5.2	All archived records shall be retained for ten years after the certificate expires.

5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	CP/CPS 5.7.1	For the failure event, BJCA has developed a comprehensive Incident Response Plan and a Disaster Recovery Plan. When a failure occurs, BJCA will execute the corresponding handling procedures and record the process. BJCA annually tests, reviews, and updates the Incident Response Plan and Disaster Recovery Plan to ensure effectiveness.
6.1.1. Key Pair Generation	CP/CPS 6.1.1	Meets the requirements of BR 6.1.1.
6.1.2. Private Key Delivery to Subscriber	CP/CPS 6.1.2	If BJCA generates the private key inside the USBKey on behalf of the subscriber, BJCA will mail the USBKey to the subscriber; If the private key is generated by the subscriber itself, it is not necessary to transmit the private key to the subscriber.
6.1.5. Key Sizes	CP/CPS 6.1.5 and 7.1.2	key pairs provided by BJCA include two types: 2048-bit or 4096-bit RSA keys, and 256-bit or 384-bit ECC keys. The root CA's key size 4096-bit RSA keys, and 384-bit ECC keys. The subordinate CA's key size 2048-bit RSA keys, and 256-bit ECC keys. The subscriber key size 2048-bit RSA keys, and 256-bit ECC keys.
6.1.6. Public Key Parameters Generation and Quality Checking	CP/CPS 6.1.6	For subscribers using the hardware cryptographic modules, the public key parameters are generated by an encryption device that complies with the FIPS 140-2 Level 2 security specifications; for the CA, the public key parameters are generated by an encryption device that complies with the FIPS 140-2 Level 3 security specifications and comply with

		generating specifications and standards for these devices. For the quality checking standard of the generated public key parameters, the built-in protocols and algorithms of these devices have reached sufficient security level requirements.
6.1.7. Key Usage Purposes	CP/CPS 6.1.7	The root CA key is only used to sign the following certificates: 1) Self-signed root CA certificates issued for the root CA itself; 2) Certificates for subordinate CA; 3) Certificates for OCSP response verification. The subscriber's key can be used to provide security services, such as identity authentication, information encryption and decryption, non-repudiation and information integrity.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	covered by CP/CPS 6.2	Private Key Protection and Cryptographic Module Engineering Controls are listed in Section 6.2.
6.2.5. Private Key Archival	CP/CPS 6.2.5	After the CA's private keys expires, BJCA shall archive and retain the CA's private keys for no less than ten years. The way to archive the CA's private keys is to encrypt and store them in an external storage medium in a secure area. BJCA does not archive the private key of the subscriber's certificate.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CP/CPS 6.2.6	The CA private key is generated in the hardware cryptographic module. When a CA private key needs to be backed up or transfered, the private key exported from a cryptographic module shall be encrypted and

		controlled by multiple people. The subscriber's private key is not allowed to be exported from a hardware cryptographic module.
6.2.7. Private Key Storage on Cryptographic Module	CP/CPS 6.2.7	The private key is encrypted and stored on a hardware cryptographic module. The subscriber's private key is stored in file certificate or the USBKey medium. The used USBKey conforms to the FIPS 140-2 Level 2 security specifications. The CA system uses the cryptographic module that complies with the FIPS 140-2 Level 3 security specifications.
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 CA's root CA certificates have a validity period no greater than 25 years. The CA subordinate certificates have a validity period no greater than 15 years. The SSL Global Server Certificates have a validity period no greater than 2 years.
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	BJCA enforces two-factor authentication for all accounts capable of directly causing certificate issuance.
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.*	CP/CPS 7.1	The detailed format of the certificate issued by this CA conforms to the X.509 V3 format and complies with the RFC 5280 standard. Every certificate is issued with a distinct serial number. The serial number contains an entropy of at least 80 bits and is generated by a cryptographically secure pseudo-random number generator (CSPRNG).

7.1.1. Version Number(s)	CP/CPS 7.1.1	X.509 V3
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CP/CPS 7.1.2	The certificate using the X.509 V3 certificate standard items and standard extensions. The certificate extensions comply with the RFC 5280 standard and comply with the requirements of the EV Guidelines.
7.1.2.1 Root CA Certificate	CP/CPS 7.1.2	The table for the certificate content and extensions for Root CA Certificate in this section meets the requirements of BR 7.1.2.1.
7.1.2.2 Subordinate CA Certificate	CP/CPS 7.1.2	The table for the certificate content and extensions for Subordinate CA Certificate in this section meets the requirements of BR 7.1.2.2.
7.1.2.3 Subscriber Certificate	CP/CPS 7.1.2	The table for the certificate content and extensions for Subscriber Certificatee in this section meets the requirements of BR 7.1.2.3.
7.1.2.4 All Certificates	CP/CPS 7.1.2	audited by WebTrust auditor.
7.1.2.5 Application of RFC 5280	CP/CPS 7.1.2	audited by WebTrust auditor.
7.1.3. Algorithm Object Identifiers	CP/CPS 7.1.3	The root CA's algorithm object identifiers are sha256RSA, and sha384ECDSA. The subordinate CA's algorithm object identifiers are sha256RSA, and sha256ECDSA. The subscriber algorithm object identifiers are sha256RSA, and sha256ECDSA.
7.1.4. Name Forms	CP/CPS 7.1.4	The certificates issued by BJCA have the format and content of the name forms conforming to the X.501 DN format and conform to the requirements of Section 7.1.4 of the CA/Browser Forum Baseline Requirements.
7.1.4.1 Issuer Information	CP/CPS 7.1.4	audited by WebTrust auditor.
7.1.4.2 Subject Information - Subscriber Certificates	CP/CPS 7.1.4	audited by WebTrust auditor.

7.1.4.2.1 Subject Alternative Name Extension 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. CAs SHALL NOT issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name. Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").	CP/CPS 7.1.4	audited by WebTrust auditor.
7.1.4.2.2 Subject Distinguished Name Fields 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/CPS 7.1.4	audited by WebTrust auditor.
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CP/CPS 7.1.4	audited by WebTrust auditor.
7.1.5. Name Constraints ***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.*** ***"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:*** ***MUST be audited in accordance with***	CP/CPS 7.1.5	No stipulation.

Mozilla's Root Store Policy. ... ***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. ..."***		
7.1.6. Certificate Policy Object Identifier	CP/CPS 7.1.6 and 1.2	Certificate Policy Object Identifiers are listed in Section 1.2.
7.1.6.1 Reserved Certificate Policy Identifiers	CP/CPS 7.1.6	audited by WebTrust auditor.
7.1.6.2 Root CA Certificates	CP/CPS 7.1.6	audited by WebTrust auditor.
7.1.6.3 Subordinate CA Certificates	CP/CPS 7.1.6	audited by WebTrust auditor.
7.1.6.4 Subscriber Certificates	CP/CPS 7.1.6	audited by WebTrust auditor.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CP/CPS 8	Meets the requirements of BR 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	In addition to internal audits and assessments, BJCA will engage an independent audit firm to conduct a third-party independent audit for WebTrust compliance anually.

8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	CP/CPS 8.2	BJCA will engage a qualified WebTrust practitioner that is familiar with IT operation management with years of industry experiences. The qualifications and skills required for external auditors are as follows: 1) Have third-party certification service qualifications related to public key infrastructure technology, information security, information technology and system auditing; 2) The auditor's organization has a licensed professional qualification with a good reputation in the industry; 3) Possess professional skills and tools to check the system operating performance; 4) Possess an effective WebTrust attestation service qualification; 5) Have an independent auditing spirit and be bound by laws, regulations and professional code of ethics.
8.4. Topics covered by assessment	CP/CPS 8.4	Are mentioned in the audit report and in the Management's Assertion as required by the WebTrust Standards, such as: Suitably designed, and placed into operation, controls. disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its CPS. Subscriber registration. Certificate renewal. Certificate rekey. Certificate issuance. Certificate distribution. Certificate revocation. Certificate validation. Subscriber key generation and management.

8.6. Communication of results	CP/CPS 8.6	BJCA internal audit results will be communicated only within the company. After BJCA accepts the assessment of a third-party external audit agency, it will publish the results on the company's official website http://www.bjca.cn.
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).** **....** **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**	the CA conducts periodical audits and make them public in the CA repository at the web site agreements and statements section.	See audit report.

service providers). “		
8.7. Self-Audits	CP/CPS 8.7	The self-audit assesses whether the electronic certification activities from the end of the last review period to the initial period of the current audit period meet the relevant regulations. The sample size of the sampling shall not be less than 3% of the total number of certificates issued during the period.
9.6.1. CA Representations and Warranties	CP/CPS 9.6.1	CA Representations and Warranties are listed in Section 9.6.1.
9.6.3. Subscriber Representations and Warranties	CP/CPS 9.6.3	Subscriber Representations and Warranties are listed in Section 9.6.3.
9.8. Limitations of liability	CP/CPS 9.8	If the CA is required to bear the indemnification and/or compensation liability according to the CPS or relevant laws and regulations and the judicial judgment, the CA institution

		shall bear the limited liability not exceeding the provisions of Section 9.9.
9.9.1. Indemnification by CAs	CP/CPS 9.9.1	Meets the requirements of BR 9.9.1.
9.16.3. Severability	CP/CPS 9.16.3	When any clause or application of this CPS is determined to be invalid or non-executive due to conflicts with the laws and regulations of the jurisdiction in which BJCA is located, BJCA may amend the clause to the extent necessary to continue to be effective, with the rest unaffected, BJCA will disclose the amended content in this Section. If the law no longer applies, or the requirements of the CA/Browser Forum are modified to make BJCA conform to both the Baseline Requirements and legal requirements of the CA/Browser Forum, any adjustments to the business operations of BJCA in this Section will no longer apply. The above-mentioned related adjustments to the business operations, the amendment of the CA's CPS, and the notification to the CA/Browser Forum will be completed within 90 days.