GUIDELINES FOR ISSUANCE OF SSL CERTIFICATES

Version 1.2
Jan 2019

Controller of Certifying Authorities
Ministry of Electronics and Information Technology

GUIDELINES FOR ISSUANCE OF SSL CERTIFICATES

In addition to the requirements mentioned for the issuance of SSL certificates by CA in the Identity Verification Guidelines, DSC Interoperability Guidelines, India PKI CP and OCSP Service Guidelines for CAs, these additional guidelines shall also be complied by CA for issuance of SSL certificates.

1. Only authorised organisational persons are entitled to apply for SSL certificates on behalf of an organisation.
2. Verification of Subject Identity Information shall be as per 4 of Identity Verification Guidelines issued by Controller and published at www.cca.gov.in
3. The CA SHALL NOT issue a certificate with subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.
4. A CA shall issue SSL and code signing certificates from the trust chain created specifically for that purpose. The special purpose trust chain shall be operated in offline mode at Root CA and CA level.
5. Office of CCA will issue necessary guidelines to conform the latest Baseline requirements of CA Browser forum time to time. The CA shall update the CPS and implement the guidelines immediately.
6. The subscriber agreement contains provisions imposing obligations and warranties on the Application relating to the accuracy of information, protection of Private Key, acceptance of certificate, use of certificate, reporting and revocation, termination of use of certificate, responsiveness and acknowledgement & acceptance.
7. The CA maintains controls and procedures to provide reasonable assurance that
    - it screens proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located, when the subjectcountryName field is present.
    - the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.
8. The CA maintains controls to provide reasonable assurance that OCSP responses do not respond with a “good” status for Certificates that have not been issued
9. The CA maintains controls to provide reasonable assurance that it performs ongoing self assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self assessment samples was taken.
10. The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions

11. The CA shall maintain audit logs are retained for at least seven years.
12. Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”. If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace.
13. CAs must restrict server authentication certificates to .in domains and may only issues other certificates to the ISO3166 country codes that the country has sovereign control over.
14. Separate CA certificates must be used to issue Server Authentication, Code Signing certificates and Time Stamping certificates.
15. SignedCertificateTimestampList field must be populated with Signed Certificate Timestamp (SCT) returned by Log operators when a valid certificate is submitted to a log.

****