GUIDELINES FOR ISSUANCE OF SSL CERTIFICATES

Version 1.4
Aug 2020

Controller of Certifying Authorities
Ministry of Electronics and Information Technology

GUIDELINES FOR ISSUANCE OF SSL CERTIFICATES

These guidelines are the subset of CCA India PKI Certificate Policy, and forms as additional guidelines to other applicable guidelines for SSL/TLS Certificates, including Interoperability Guidelines and OCSP Service Guidelines for CAs.

General Guidelines

1. The maximum validity of subscriber certificates shall be limited to 825 days.
2. CAs must restrict server authentication certificates to **.in** domains
3. Only authorized organizational persons are entitled to apply for SSL certificates on behalf of an organization.
4. CA shall not issue SSL certificates to any organizational entity unless it owns/controls that domain name.
5. Verification of Subject Identity Information shall be as per section 4.1 of IVG document.
6. The CA SHALL NOT issue a certificate with subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.
7. A CA shall issue SSL and code signing certificates from the issuing CA Certificates created specifically for that purpose.
8. The CA keys shall be operated in offline mode at Root CA and CA level.
9. Office of CCA will issue necessary guidelines to conform the latest Baseline requirements of CA Browser forum (and Network Security Requirements) time to time. The CA shall update the CPS and implement the guidelines immediately.
10. 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.
11. The CA maintains controls and procedures to provide reasonable assurance that
    a. 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.
    b. the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.
12. 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
13. 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.

14. CA shall implement risk detection techniques for every certificate request including subscriber information and CSR with globally acceptable sources like google safe browsing checks, Debian weak keys, other weak key detection techniques, etc.
15. 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
16. The CA shall maintain audit logs are retained for at least seven years.
17. CA shall not issue certificate to domain where the domain name is a TLD / ccTLD itself (eg: .in) or second level domains (eg: co.in, firm.in, net.in, org.in, gen.in, etc), or a Public Suffix List (eg: gov.in, nic.in, etc)
18. 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.
19. SignedCertificateTimestampList field must be populated with Signed Certificate Timestamp (SCT) returned by Log operators when a valid certificate is submitted to a log. This shall be adhered based on policies defined by major browsers like chromium.
20. CA shall perform the CAA record validation (in DNS Zone) and ensure that, it does not limit the issuance to some other CA. In case the domain's CAA record indicate the issuance authorization to any other CA, the CA shall ensure that the applicant/requestor modifies the CAA record to authorize them or remove the current record / authorization, before processing such requests.

CA certificate enrollment to Mozilla

Mozilla includes CCA SSL Root Certificate only after the independent enrolment of all SSL CA certificates. In order to facilitate the use of SSL certificates issued by Licensed CAs by the Indian Government and other entities in India, the CAs are allowed to enrol their SSL CA certificates in the Mozilla browser independently . Once all the SSL CA certificates are included in the Mozilla, the Root CA certificate will include in the Mozilla browser and Mozilla remove all SSL CA certificates. Therefore all CAs who issue SSL certificates and also wants to include their SSL CA certificate in Mozilla products shall directly approach Mozilla for inclusion of their SSL CA certificates.

Notwithstanding the requirements mentioned under the guidelines issued by CCA, for the purpose of issuance of SSL certificates by a Licensed CA under the India PKI special

purpose trust chain and also for the enrolment of SSL CA certificate in Mozilla products, the following conditions shall apply :-

1. CA should directly apply and manage the enrolment of their certificate in the Mozilla products according to Mozilla's requirements.
2. To issue SSL certificates under CCA India hierarchy, the CA certificate should have been certified by CCA
3. The SSL certificates issued under CCA India hierarchy shall contain applicable Policy ID of India PKI.
4. Both the certificates and CRLs issued under India PKI special purpose trust chain hierarchy should be made available in the CA repository designated for India PKI.
5. As far as possible, the infrastructure for management of SSL CA certificates to be included in the Mozilla products should be isolated from CA maintained for issuance of individual signature certificates.
6. The CA infrastructure and certificates issued under India PKI hierarchy shall be covered under annual compliance of CCA irrespective the fact that the audit of the SSL certificate issuance systems covered under other compliance audit.
7. In case of a separate CPS is maintained for issuance of SSL certificate, the reference of that CPS and additional requirements for issuance of SSL certificates under CCA India should be specified in CPS to be approved by CCA.

****