Online Certificate Status Protocol (OCSP) Service Guidelines for Certifying Authorities (CA)

Version 1.1

May 2015

Controller of Certifying Authorities

Department of Electronics and Information Technology

Ministry of Communications and Information Technology

Document Control

Document Name	OCSP Services Guidelines for CAs
Status	Release
Version	1.1
Last update	May 05 2015
Document Owner	Controller of Certifying Authorities, India

Introduction

Certifying Authorities publishes the Certificate Revocation List (CRL) in accordance with the provisions of Information Technology Act and Guidelines specified by the Office of CCA. Relying parties verify revocation status of DSC in an offline mode, by periodically downloading CRLs or by accessing CRLs from the CAs website. To provide more timely status information, all CAs should establish an Online Certificate Status Protocol (OCSP) Service to enable relying-party application software to determine the status of an identified Certificate in an online mode. The CAs should operate their OCSP service as per the requirements given in the X.509 Certificate Policy for India PKI, Interoperability Guidelines for DSC under IT Act and guidelines mentioned in this document.

The functional requirements of a Certificate Status Provider (CSP) service are mentioned in X.509 Certificate Policy for India PKI. A CSP service provides status of certificates and of the certification path. CSP services include:-

1. Online Certificate Status Protocol (OCSP) Responders that provide revocation status of certificates
2. Standard Based Certificate Validation Protocol (SCVP) Servers that validate certification paths

At present only OCSP services are to be provided by CAs

Additional OCSP Service Guidelines

1. The CA SHALL support an OCSP capability using the GET or the POST method for DSC issued under PKI India Hierarchy

2. The CA SHALL operate OCSP capability to provide a response time of ten seconds or less under normal operating conditions.

3. OCSP responses MUST be signed by an OCSP Responder whose Certificate is signed by the CA or its subCA that issued the Certificate whose revocation status is being checked.

4. In the case of certificates issued under special purpose trust chain for SSL and Code Signing, If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder MUST NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.

5. As part of Interoperability initiative, certificates issued by CAs should have *id-ad-ocsp accesslocation* pointing to the CA's OCSP responder..
6. The end to end process must be automated for providing OCSP response to a Relying Party. There must not be any manual intervention unless an error condition arises.
7. The OCSP must accept both signed and unsigned OCSP requests
8. The OCSP must not use precomputed or Cached responses for certificate Status
9. The OCSP Responder should be able to support nonce extension in request and responses
10. All CAs should modify their CPS to reflect the above requirements and the scope of the CA audit should include OCSP service operations.
11. The OCSP responder certificate and subscriber certificates shall comply with latest version of interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act

****