OCSP Lints and Test Cases

Lints

Each lint is a short focused test on a given OCSP request/response pair designed to check for compliance with typically one (but possibly multiple) requirements.

Lint ID	Lint Description
LINT01	If the OCSP response is signed, ensure that the OCSP response was signed by the issuing CA or an OCSP responder issued by the issuing CA and containing the id-pkix-ocsp-nocheck extension.
LINT02	If the OCSP request was sent using HTTP GET, ensure that an HTTP 405 "Method Not Allowed" response does not result.
LINT03	If the OCSP request is for a subscriber certificate, ensure that all producedAt and thisUpdate dates in the OCSP response are no more than 4 days in the past.
LINT04	If the OCSP request is for a subscriber certificate, for each SingleResponse in the OCSP response ensure that the nextUpdate date is present and not more than 10 days after the thisUpdate date.
LINT05	If the OCSP request is for a subordinate CA certificate, ensure that all producedAt and thisUpdate dates in the OCSP response are no more than 365 days in the past.
LINT06	If the OCSP request is for a non-issued certificate and the the OCSP response is from a responder for a non technically constrained CA, ensure that the OCSP response contains a certStatus that is not good in the SingleResponse for the certificate.
LINT07	If the OCSP request is for an issued and revoked but not expired certificate, ensure that the OCSP response contains a certStatus of revoked in the SingleResponse for the certificate.
LINT08	After sending an OCSP request, ensure that an OCSP response is returned within 10 seconds.
LINT09	After sending an OCSP request, ensure that an HTTP response is returned (e.g. OCSP server is responding).
LINT10	If the OCSP response is signed, ensure that it is not signed with a signature algorithm that uses SHA-1.

Lint ID	Lint Description
LINT11	If the OCSP response is not malformed, ensure that the OCSP response is of type id-pkix-ocsp-basic.
LINT12	If the OCSP response status is successful, ensure that the OCSP response signature (BasicOCSPResponse.signature) is not empty.
LINT13	If the OCSP response is signed, ensure that the OCSP response was signed by the issuing CA, a trusted responder (defined by the client), or an authorized responder issued by the issuing CA and containing the id-kp-OCSPSigning extended key usage.
LINT14	If the OCSP request is for a non-issued certificate and the OCSP response status is revoked, ensure that the OCSP response contains the id-pkix-ocsp-extended-revoke response extension.
LINT15	If the OCSP request is for a non-issued certificate and the OCSP response is using the extended revoked definition, ensure that the OCSP response contains a revocationReason of certificateHold in the SingleResponse for the certificate.
LINT16	If the OCSP request is for a non-issued certificate and the OCSP response is using the extended revoked definition, ensure that the OCSP response contains a revocationTime of January 1, 1970 in the SingleResponse for the certificate.
LINT17	If the OCSP request is for a non-issued certificate and the OCSP response is using the extended revoked definition, ensure that the OCSP response does not contain any CRL references extensions in the SingleResponse for the certificate.
LINT18	If the OCSP request is for a non-issued certificate and the OCSP response is using the extended revoked definition, ensure that the OCSP response does not contain any CRL entry extensions in the SingleResponse for the certificate.
LINT19	For each SingleResponse returned in the OCSP response, ensure that the thisUpdate date is not in the future and not prior to the issuance date of the certificate.
LINT20	If the OCSP response is signed by a delegated responder, ensure that the signer certificate was issued by the responder's CA.

Lint ID	Lint Description
LINT21	If the OCSP request is for an issued certificate and contains non-critical unrecognized extensions, ensure that the OCSP response contains a responseStatus of successful.
LINT22	If the OCSP response is of type id-pkix-ocsp-basic, ensure that ResponseBytes.response contains a DER encoded BasicOCSPResponse.
LINT23	If the OCSP response is of type id-pkix-ocsp-basic, ensure that BasicOCSPResponse.signature was calculated over the DER encoding of the ResponseData structure found in BasicOCSPResponse.tbsResponseData (Note: this is done by attempting to verify the signature).
LINT24	If the OCSP response is signed, ensure that the OCSP response was signed by the issuing CA or an authorized responder containing the id-kp-OCSPSigning extended key usage.
LINT25	If the OCSP response is signed by a delegated responder, ensure that the signer certificate was issued by the CA identified in the OCSP request (CertID key and name match).
LINT26	If the OCSP response is signed by a delegated responder, ensure that the value of the id-pkix-ocsp-nocheck extension in the signer certificate is NULL.
LINT27	If the OCSP response is of type id-pkix-ocsp-basic, ensure that ResponseData.version is v1.
LINT28	If the OCSP response is of type id-pkix-ocsp-basic, ensure that ResponseData.responderID identifies the certificate used to sign the request (ResponderID key/name match).
LINT29	If the OCSP response is of type id-pkix-ocsp-basic, ensure that a SingleResponse value is provided for and corresponds to each Request value in the OCSP request.
LINT30	If the OCSP response is of type id-pkix-ocsp-basic and contains a id-pkix-ocsp-archive-cutoff extension in SingleResponse.singleExtensions, ensure that the extension value is of type GeneralizedTime.

Lint ID	Lint Description
LINT31	If the OCSP response is of type id-pkix-ocsp-basic, ensure that a id-pkix-ocsp-extended-revoke extension does not appear in SingleResponse.singleExtensions.
LINT32	If the OCSP response is of type id-pkix-ocsp-basic and contains a id-pkix-ocsp-extended-revoke extension in ResponseData.responseExtensions, ensure that the extension value is NULL.
LINT33	If the OCSP response is of type id-pkix-ocsp-basic and contains a id-pkix-ocsp-extended-revoke extension in ResponseData.responseExtensions, ensure that the extension is not marked critical.
LINT34	If the OCSP response is signed, ensure that the signing algorithm is sufficiently/acceptably secure (RSA-based or EC-based using SHA224, SHA256, SHA384, or SHA512).
LINT35	If an HTTP 200 response is returned, ensure that the HTTP response content can be decoded/parsed successfully according to 'RFC 6960: Appendix B.1. OCSP in ASN.1 - 1998 Syntax'.
LINT36	If the OCSP request is for a subscriber certificate, the OCSP response is of type is of type id-pkix-ocsp-basic and BasicOCSPResponse.certs is present, ensure that no nextUpdate date is after the notAfter date of any certificate in BasicOCSPResponse.certs.
LINT37	If the OCSP request is for a subscriber certificate, the OCSP response is of type is of type id-pkix-ocsp-basic and BasicOCSPResponse.certs is omitted, ensure that no nextUpdate date is after the notAfter date of the CA certificate which issued the subscriber certificate.
LINT38	If the OCSP response is signed, ensure that either the signer certificate contains the id-kp-OCSPSigning extended key usage or the response is not signed with a signature algorithm that uses SHA-1.
LINT39	If the OCSP response is of type id-pkix-ocsp-basic, for each SingleResponse in the OCSP response ensure that the nextUpdate date is present and not less than 8 hours after the thisUpdate date.

Lint ID	Lint Description
LINT40	If the OCSP response is of type id-pkix-ocsp-basic, for each SingleResponse in the OCSP response ensure that the nextUpdate date is present and not more than 7 days after the thisUpdate date.
LINT41	If the OCSP response is of type id-pkix-ocsp-basic, for each SingleResponse in the OCSP response ensure that the nextUpdate date is present and not less than 8 hours after the current date.
LINT42	If the OCSP response is of type id-pkix-ocsp-basic, for each SingleResponse in the OCSP response that has a delta of more than 16 hours between thisUpdate and nextUpdate, ensure that nextUpdate is not less than 50% of the delta after the current date.

Lint Definitions

- OCSP request is not malformed
  - OCSP request can be parsed using the ASN.1 Module defined in RFC 6960 Appendix B.1: OCSP in ASN.1 - 1998 Syntax
- OCSP request is for a subscriber certificate
  - OCSP request is for a certificate with
    - id-ce-basicConstraints extension missing or
    - id-ce-basicConstraints extension present and
      - BasicConstraints.cA missing or
      - BasicConstraints.cA is FALSE
- OCSP request is for a subordinate CA certificate
  - OCSP request is for a certificate with
      - subject not equal issuer and
      - id-ce-basicConstraints extension present and
      - BasicConstraints.cA is TRUE
- OCSP response is not malformed
  - OCSP response can be parsed using the ASN.1 Module defined in RFC 6960 Appendix B.1: OCSP in ASN.1 - 1998 Syntax
- OCSP response is signed
  - OCSP response is not malformed and
  - OCSPResponse.responseBytes is present and
  - ResponseBytes.responseType is id-pkix-ocsp-basic

- OCSP response is signed by a delegated responder
  - OCSP response is signed and
  - signer certificate contains the id-kp-OCSPSigning extended key usage
- OCSP response is using the extended revoked definition
  - OCSP response is signed and
  - ResponseData.responseExtensions contains id-pkix-ocsp-extended-revoke and
  - SingleResponse.certStatus is revoked

Test Cases

Each test case consists of crafting an OCSP request (that may have certain characteristics), sending the OCSP request to the OCSP server, receiving the OCSP response, and finally running all lints to check for compliance violations.

- TC01: Valid Issued Certificate
- TC02: Revoked Issued Certificate
- TC03: Non-Issued Revoked Certificate
- TC04: Valid Issued Certificate - Unrecognized Request Extension
- TC05: Valid Issued Certificate - Only Weak Preferred Signature Algorithms (SHA1, MD5, MD2)
- TC06: Valid Issued Certificate - SHA224 CertID Hash Algorithm
- TC07: Valid Issued Certificate - SHA256 CertID Hash Algorithm
- TC08: Valid Issued Certificate - SHA384 CertID Hash Algorithm
- TC09: Valid Issued Certificate - SHA512 CertID Hash Algorithm
- TC10: Valid Issued Certificate - With 256-bit Nonce
- TC11: Valid Issued Certificate and Revoked Issued Certificate
- TC12: Valid Issued Certificate, Revoked Issued Certificate, and Non-Issued Certificate
- TC13: Empty Request List
- TC14: Valid Issued Pre-Certificate for which a Certificate Does Not Exist [CONDITIONAL]