Updating OCSP

David Cooper

Background

- Concerns raised about text in RFC 2560 being misinterpreted, particularly Section 4.2.2.2 on Authorized Responders
- Working group agreed to develop an update to RFC 2560
- Scope of update effort limited to clarifying the protocol.
- This means the update will not make any changes to the protocol described in RFC 2560, except …

Changes in RFC 5019[1]

- Section 2.2.1 states that while an RFC 5019-compliant request MUST request status for only one certificate, a response MAY include status information for more than one certificate.
- Section 2.2.3 extends the definition of the "unauthorized" error code from:
  - The response "unauthorized" is returned in cases where the client is not authorized to make this query to this server **or the server is not capable of responding authoritatively**.

[1] The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

Changes in draft-ietf-pkix-ocspagility

- Updates set of mandatory and optional cryptographic algorithms.
- Defines a new request extension, PreferredSignatureAlgorithms.
- Specifies rules for responder signature algorithm selection.

Clarifying Authorized Responders

- RFC 2560 states the key used to sign the response must belong to one of the following:
  - [Integrated OCSP Responder] the CA who issued the certificate in question
  - [Locally Trusted OCSP Responder] a Trusted Responder whose public key is trusted by the requester
  - [Designated OCSP Responder] a CA Designated Responder (Authorized Responder) who holds a specially marked certificate issued directly by the CA.

Integrated OCSP Responder

- Update clarifies meaning of “the CA who issued the certificate in question”:
  - OCSP response does not need to be signed with same key as target certificate
  - Subject DN in OCSP responder's certificate must be the same as issuer DN in target certificate
- Appendix D includes four examples that involve integrated OCSP responders.

Designated OCSP Responder

- Update clarifies requirement for OCSP responder's certificate to be “issued by the CA that issued the certificate in question”:
  - CA may use different keys to sign OCSP responder's certificate and target certificate.
  - Issuer DN in OCSP responder's certificate must be the same as issuer DN in target certificate.
- Appendix D includes six examples that involve designated OCSP responders.

Locally Trusted OCSP Responder

- Reinforces that “local configuration” is client's local configuration, not CA's local configuration.
- Emphasizes that locally trusted OCSP responders are usually created by an organization for use by its own clients, not by a CA for use by all clients validating certificates issued by that CA.
- Appendix D includes one example involving a locally trusted OCSP responder.

Editor's Notes

- Draft -00 contains 10 editor's notes
  - Some highlight change made in protocol, providing rationale for change.
  - Some request additional information (e.g., syntax of nonce extension).
  - Some propose consideration of changes in future drafts.

Next Steps

- Working groups needs to decide whether to:
  - Use draft-cooper-pkix-rfc2560bis as the starting point for development of OCSP update; or
  - Start over with a new approach to developing an update to OCSP.
- If draft-cooper-pkix-rfc2560bis is accepted, David Cooper and Stefan Santesson (and possibly others) will update the draft and submit a revised version as a working group document.

Questions

New Issues

- Handling unrecognized critical extensions:
  - requestExtension: Return an "unauthorized" error response?
  - singleRequestExtension: return a certStatus of "unknown" (or "unauthorized" error response if responder can only provide pre-generated responses)?

New Issues

- Problem:
  - OCSP responder basis responses on CRL
  - Returns "unknown" certStatus if certificate was not issued at time CRL was generated
  - Returned certStatus for recently issued certificate continues to be "unknown" until responder obtains new CRL.
- Should definition of "unknown" be reworded to encourage responders to return status of "good" rather than "unknown" under these circumstances?

Editor's Notes

- Syntax of nonce extension – RFC 2560 specifies an OID for the nonce extension, but not an ASN.1 structure for the extension value.
  - How do current implementations populate extnValue for the nonce extension? Is it always populated with the DER encoding of some ASN.1 syntax?
- Responder processing of nonce extension:
  - Next draft will be changed to state that response may include a nonce even if request did not include one.
  - Text will be added to explain why this is permitted.

Editor's Notes (continued)

- Preferred signature Algorithms
  - Use of parameters in sigIdentifier for RSA signature algorithms? Are parameters included or omitted?
- Service Locator extension
  - RFC 2560 does not specify the “processing performed by the OCSP Responder”.
    - Which OCSP responder signs response that is received by client? Responder that received request from client? Authoritative responder to which request was routed? Either?
  - Should update clarify this?

Editor's Notes (continued)

- Syntax of id-pkix-ocsp-nocheck extension.
  - RFC 2560 says extnValue SHOULD be NULL.
  - Do any certificates include a nocheck extension where extnValue is not NULL?
  - Can update say that extnValue **SHALL** be NULL?
- CRL entry extensions as singleExtensions in responses:
  - RFC 2560 states that all CRL entry extensions from RFC 2459 are supported as singleExtensions
  - Update only mentions invalidityDate.

Editor's Notes (continued)

- Response verification requires clients to confirm that “the identity of the signer matches the intended recipient of the request”.
  - Should this requirement be removed or modified?
  - Under what circumstances does the client know the identity of the intended recipient of the request?
    - When following a URL in an AIA extension, identity of recipient isn't known.
    - When using a locally configured OCSP responder, could local OCSP responder relay request to a CA designated responder and return the response signed by that responder (especially if request included a service locator extension)?

Editor's notes (continued)

- What are the requirements for including an AIA extension in target certificates:
  - Integrated or designated responder that provides status for the certificate? [SHOULD or MUST]
  - Responder that provides status for the certificate that is neither integrated nor designated (i.e., can only be used as a locally trusted OCSP responder)? [SHOULD NOT or MUST NOT]
- Is the only requirement that CA products be capable of including an AIA extension in certificates?

Editor's Notes (continued)

- 1998 ASN.1 from RFC 2560:
  - Module did not have an OID
    - Added OID, copied from draft-ietf-pkix-ocspagility-08
  - Module imports Certificate, AlgorithmIdentifier, and CRLReason from AuthenticationFramework rather than PKIX1Explicit88 and PKIX1Implicit88
    - Is there a reason for this? Should it be changed?
    - No changes were made in draft-cooper-pkix-rfc2560bis.