IETF PARIS 2012 PKIX meeting
about : draft-ietf-pkix-rfc2560bis-04

Denis Pinkas

Denis.Pinkas@bull.net

March 27, 2012

Issues with both RFC 2560 and rfc2560bis-04

- RFC 2560 was unclear and wrong on several topics.

- draft-ietf-pkix-rfc2560bis-04 :
  - does not provide the missing explanations,
  - does not provide the adequate corrections,
  - does not provide backwards compatibility,
  - introduces a new order of magnitude of complexity.

What is simple in RFC 2560 but unexplained

- RFC 2560 is simple when :
  - there is a status request for a single certificate, and
  - when the OCSP response is signed by the same key that has issued the target certificate.

- However, even for this simple case :
  - the way to pick the right certificate to verify the signature from the OCSP response is not clearly explained,
  - which keyUsage bits and extended key usage OIDs shall be present in the CA certificate is not even said !

What is less simple in RFC 2560

- RFC 2560 gets more complicated when:
  - there is a status request for a one or more certificates from the same CA, and
  - when the response is signed by a designated OCSP responder whose certificate has been issued by the CA under the same key that has issued the target certificate.
- However, even for this case :
  - the way to pick the right certificate to verify the signature from the OCSPResponse is not clearly explained.

What is much more complicated in RFC 2560

- RFC 2560 gets much more complicated when :
  - The status request is for several certificates from different CAs, and
  - when the response is signed by a designated OCSP responder which has received several OCSP certificates from different CAs.

- For this case:
  - the explanations both in RFC 2560 and in rfc2560bis-04 are wrong,
  - the validity of the BasicOCSPResponse cannot be globally checked, since only the validity of every SingleResponse can be checked.

- Therefore:
  - the OCSP client must check for every SingleResponse if the OCSP responder has a valid OCSP certificate from the right CA.

- Note: a single key must be used to sign the OCSPResponse, which means that every CA must certify the same OCSP key (which is only said in the Appendix).

rfc2560bis-04: “same key” issue

- RFC 2560 uses the wording “same key” in only two occurrences:

2.6 OCSP Signature Authority Delegation

The key that signs a certificate's status information need not be the same key that signed the certificate. A certificate's issuer explicitly delegates OCSP signing authority by issuing a certificate containing a unique value for extendedKeyUsage in the OCSP signer's certificate. This certificate MUST be issued directly to the responder by the cognizant CA.

4.2.2.2 Authorized Responders

The key that signs a certificate's status information need not be the same key that signed the certificate. It is necessary however to ensure that the entity signing this information is authorized to do so. Therefore, a certificate's issuer MUST either sign the OCSP responses itself or it MUST explicitly designate this authority to another entity.

- Most people understand that the key that signs the OCSP response may be different from the key that signed the target certificate, only when there is an explicit delegation to an OPCSP responder.

Text from rfc2560bis-04

- Text from rfc2560bis-04:

- **2.3.6.2. Verifying Responder's Authorization**
  - **Systems or applications that rely on OCSP responses MUST reject a response if the certificate required to validate the signature on the response fails to meet at least one of the following criteria:**

    1. Matches a local configuration (...) .

    2. Is the certificate of the CA that issued the certificate in question.

    (For this criterion to be satisfied, the subject DN in the certificate required to validate the signature on the OCSP response MUST be the same as the issuer DN in the certificate in question.)

With such a sentence, when there is no delegation, the key that signs a certificate's status information may not be the same key that signed the certificate.

Comparison with CRLs

- When a CA issues a certificate, it may include :
  - a CRL Distribution Point (CRLDP) and /or
  - an accessLocation field in an authorityInfoAccess extension.
- When there is no delegation, the key that signs the CRL is the same key that issued the certificate, whether that has already been a CA key rollover or not.
- When there is no delegation, the same applies for OCSP responses.
- When two CA keys are valid at a given time (this is the usual case), then the CA maintains two different accessLocations.

Compatibility issue

- Text from rfc2560bis-04:

2.3.5.1. Authorized Responders

Note: Some OCSP clients, when accepting responses from an integrated OCSP responder, will only accept responses that are signed using the same key as the target certificate(s).

Note: Some OCSP clients, when accepting responses from a designated OCSP responder, will only accept responses if the certificate required to validate the signature on the response was signed using the same key as the target certificate(s).

- This applies in particular to cases 3 & 7 from Appendix E.

rfc2560bis-04: same key

- rfc2560bis-04 :
  - introduces new use cases related to CA key rollover which are not covered by RFC 2560,
  - and thus does not provide backwards compatibility.

- With rfc2560bis-04 :
  - the response may be signed by the new CA key rather than by the CA key that signed the target certificate,
    - for supporting this case, OCSP clients MUST now be able to support “old-by-new” certificates.

- These new use cases only appear in Appendix E (which few people read):

> **Appendix E. Example PKIs With OCSP Responders.**
>
> **This appendix provides some examples of valid PKI architectures that include OCSP responders.**

- The status of Appendix E is not mentioned.
  It looks like being informative, but in practice it is normative.
- It deals with use cases which are not detailed, nor explained, in the main body of the document.

What is still wrong in rfc2560bis-04

- rfc2560bis-04 still does not explain correctly the overall verification process that shall be supported by an OCSP client.

- Sections 2.3.6 and 2.3.6.2 need to be fully revised to support the three cases:
    - integrated OCSP responder,
    - delegated OCSP responder and
    - locally trusted OCSP responder.

- When the response includes status information from different CAs, every SingleResponse must be individually evaluated:
    - the OCSP client must verify that the OCSP responder got a valid OCSP certificate from the right CA.

- It would be worth to mention that the OCSP responder SHOULD include all the OCSP certificates in the `certs` field.

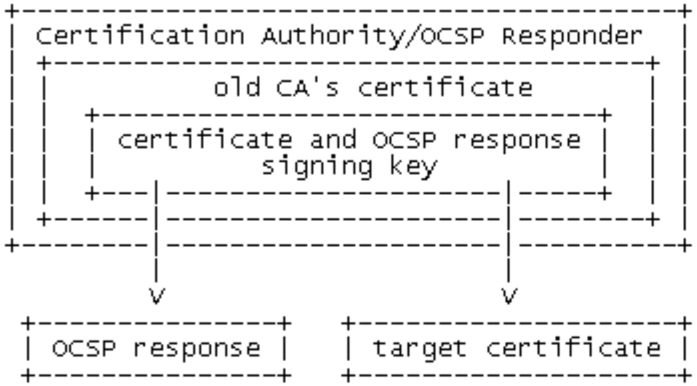
What is expected in rfc2560bis-05

- Correct explanations are awaited on:
  - How an OCSP client shall test every Single OCSP response in addition to the whole OCSP response,
  - How CA key rollover shall be handled:
    - by CAs,
    - by OCSP responders,
    - by OCSP clients.

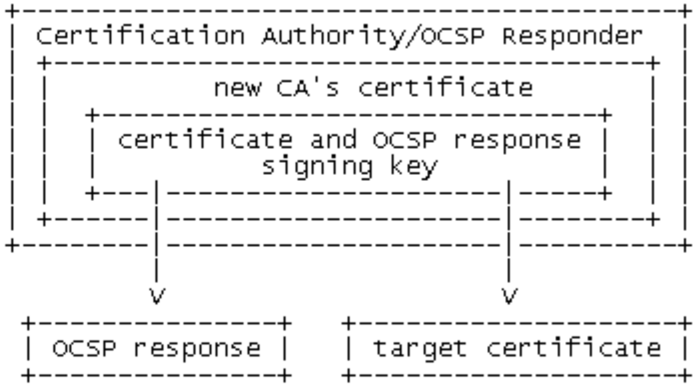
- Full backwards compatibility with RFC 2560 is required, therefore the following use cases from rfc2560bis-04 described in Appendix E should be deleted:
  - figure 2 : self-issued certificate. Delete but replace with figure 2 bis,
  - figure 3 : single key to sign all responses. Delete.
  - figure 5 : root key signs OCSP responses ! Delete.
  - figure 6 : self-issued certificate. Delete but replace.
  - figure 7 : single key to sign all responses. Delete.

Figure 2 bis for rfc2560bis-05

- Figure 2 bis illustrates a CA key rollover when a CA directly signs the OCSP responses:
- The CA shall include a URL in the accessLocation field from the authorityInfoAccess extension for every target certificate.
- The accessLocation field will be different whether the certificate was signed by the old CA key or the new CA key:
  - the key used to sign OCSP responses will be different for each accessLocation.



```
+-----------------------------------------+
| Certification Authority/OCSP Responder  |
| +-------------------------------------+ |
| |          old CA's certificate       | |
| |  +-------------------------------+  | |
| |  | certificate and OCSP response |  | |
| |  |          signing key          |  | |
| |  +---|---------------------|-----+  | |
| +------|---------------------|--------+ |
+--------|---------------------|----------+
         |                     |
         v                     v
 +---------------+   +--------------------+
 | OCSP response |   | target certificate |
 +---------------+   +--------------------+
```



```
+-----------------------------------------+
| Certification Authority/OCSP Responder  |
| +-------------------------------------+ |
| |          new CA's certificate       | |
| |  +-------------------------------+  | |
| |  | certificate and OCSP response |  | |
| |  |          signing key          |  | |
| |  +---|---------------------|-----+  | |
| +------|---------------------|--------+ |
+--------|---------------------|----------+
         |                     |
         v                     v
 +---------------+   +--------------------+
 | OCSP response |   | target certificate |
 +---------------+   +--------------------+
```

A small nit to be deleted in rfc2560bis-04

- Text from the security considerations section:
  - “long-term archival applications in which the status of a certificate is being <u>queried for a date in the distant past</u>”.

- Reason for the deletion: OCSP does not currently allow to request the status of a certificate for a date in the distant past.

What is proposed to be added to rfc2560bis-05

- Supporting the case where a single certificate status request is included the request is simpler than supporting the case where several certificate status requests for different CAs are included in the request.

- Since an OCSP client has full control of what it places in the request, it is proposed to define a profile for a certificate status request limited to one certificate.

- This case is the most supported and conformance to this profile may be achieved with less efforts.
- Fewer implementations support the more complicated cases.

Is there any text proposal for rfc2560bis-05 ?

- Text proposals have been posted to the list in 2010:
  - Thread: 12 comments on draft-cooper-pkix-rfc2560bis-00

- For example:
  - **Sep 08 2010**
    - http://www.ietf.org/mail-archive/web/pkix/current/msg28337.html
  - **Sep 30 2010**
    - http://www.ietf.org/mail-archive/web/pkix/current/msg28408.html
  - **Oct 08 2010**
    - http://www.ietf.org/mail-archive/web/pkix/current/msg28457.html
  - **Oct 12 2010**
    - http://www.ietf.org/mail-archive/web/pkix/current/msg28468.html