RPKI Certificate Policy

Stephen Kent, Derrick Kong, Ronald Watro, Karen Seo

July 21, 2010

Addition of Normative Language

Originally the CP was an I-D. It was changed to be a regular document and as part of this the RFC 2119 keywords were removed. We've added them back in.

Keyword	Previous #	Current #
MAY	0	21
SHOULD	0	20
MUST	1	103
MUST NOT	0	2

Other changes

The other edits/comments fell into 3 categories:

1. Straightforward, minor, e.g., correction of typos, deletion of the word “unique” in Intro/overview; question re: redundancy and level of detail (due to using template); etc. (Comments so far on current version -- need to delete a sentence fragment, add a missing “be”, correct IESG contact info.)
2. Clarifications:
    - ISPs can distribute AS numbers (as well as address blocks)
    - CAs in the chain of certificates that terminate at a TA accepted by the RP

Other changes (2 of 2)

(2. Clarifications -- continued)

- "Expired and revoked certificates SHOULD be removed from the RPKI repository system, upon expiration or revocation, respectively.”

3. Items requiring an answer or more of a change (covered in subsequent slides):

- Publication of certification information
- Certificate modification re: revocation
- Use of OCSP or SCVP
- CA/RA termination

2.2 Publication of Certification Information

- "Is a CA responsible for publishing ALL certifications it issues, or can it be selective in publication?...a similar question is raised regarding CRLs and RPKI-signed objects. Is the CA requires to publish ALL such issued objects?"
  - "Each CA MUST publish the certificates (intended for public consumption) it issues via the repository system."
  - "Each CA MUST publish the CRL(s) that it issues via the repository system."
  - "Each CA MUST publish its RPKI-signed objects via the repository system (for all such objects intended for public consumption)."
- The above assumes that an RPKI CA issues a mix of certs (private and public) and thus needs to publish a single CRL that spans all of these certs. An alternative model is that an RPKI CA creates a subordinate CA for issuing private certs, and thus the CRL for that CA never need to be published.

4.8 Certification modification

- “why is the treatment of augmentation of a subject's INRs treated differently from reduction in a subject's INRs? While section 4.8 deals with the steps involved in issuing a new certification in the case where a subject's INR's are augmented, there is no corresponding description of the process in reduction, other than the single sentence in section 4.8.1 that does not refer to any other part of the CPS.”
- Augmentation does not entail revocation of the old certificate.

4.10 Certificate status services

- “is it true …that "This PKI does not make use of OCSP or SCVP" or is it more appropriate to state that "RPs SHOULD NOT rely on the use of OCSP or SCVP?”
- It is true because we prohibit the inclusion of the OCSP EKU in resource certificates. We also don't allow the corresponding AIA extension for OCSP in resource certificates. So the only way OCSP could be used is by local convention, where an authority configures all of its users to rely on it as an OCSP responder for everyone else. We reworded the text to be clearer on this point.

5.8 CA or RA termination

- “I am finding it difficult to reconcile this need for "an agreement" in the light of the observation that where a CA no longer has any INR resources then it cannot function as a CA in the RPKI, whether or not an agreement is reached, Why then is an agreement stipulated here?”
- From: "The termination of a CA shall therefore be subject to the agreement between the issuer and the subscriber and will be described in the CPS for the issuer."

  To: "Procedures associated with the termination of a CA MUST be described in the CPS for that CA."

Back up slides with more detail

Introduction and Overview

- "Uniqueness" is not an outcome of verification of a certificate. It would be more accurate to drop "uniqueness."
- Deleted "unique"from:
  - Introduction, paragraph 1: "These certificates will enable verification that the resources indicated in the certificate have been distributed to the holder of the associated private key and that this organization is the current, unique holder of these resources."
  - Section 1.1 Overview, paragraph 1: "The ability to verify such claims is essential to ensuring the unique, unambiguous distribution of these resources."

1.3.1 Certification Authorities

- “The document appears to preclude the actions of LIRs / ISPS in distributing AS numbers. I do not believe that this is appropriate, nor accurate, in today's environment.”
- From: "The organizations that distribute IP addresses IANA, RIRs, NIRs, ISPs) and AS numbers (IANA, RIRs, and NIRs) act as CAs in this PKI.”
- To: "The organizations that distribute IP addresses and AS numbers (IANA, RIRs, NIRs, ISPs) act as CAs in this PKI."

2.3 Time or frequency of publication

- “the document does not specify a CA's actions regarding the publication of expired and revoked certifications, nor indicate if the CA's CPS should include such information.”
- Added: "Expired and revoked certificates SHOULD be removed from the RPKI repository system, upon expiration or revocation, respectively.”
- Need to delete sentence fragment in last paragraph:
  - “The period of time within which a CA will publish a CRL with an entry for a revoked certificate after it revokes that certificate.”

3.2 Initial identity validation & 3.3.2 Identification and authentication for re-key

- “I am not sure that these need to be separate - for example is issuance after revocation any different from initial issuance - i.e. the same criteria of 3.2.1 ("Method to prove possession of private key"), 3.2.2 ("Authentication of organization identity"), 3.2.3 ("Authentication of individual identity") and 3.2.5 ("Validation of authority") apply, so why is 3.3.2 called out - what new information is being provided here that is not already provided in the previous section?”
- The draft follows the template (RFC 3647) established for a CP/CPS, which results in some redundant sections.

3.4 Identification and authentication for revocation request

- "why does this section of the text NOT refer to the actions of a CA as described in sections 3.2.1, 3.2.2, 3.2.3 and 3.2.5? It appears that revocation is described in more informal terms and issuance, yet the constraints on the CA to ensure that authenticity of the request are intended to be the same."
- As noted above, the draft follows the RFC 3647 template. Note: If the subject has lost access to its key, it cannot perform PoP (3.2.1).

4.5.2. Relying party public key and certificate usage

- “In the light of related work on local TA generation I am left with the question of what exactly is being referred to here in this "chain”. I would prefer this term to be defined.”
- From: "Before any act of reliance, relying parties shall independently …(2) assess the status of the certificate and all the CAs in the chain that issued the certificates relevant to the certificate in question."
- To: "Before any act of reliance, relying parties MUST independently …(2) assess the status of the certificate and all the CAs in the chain (terminating at a TA accepted by the RP) that issued the certificates relevant to the certificate in question.”