Resource Certificate Profile

Geoff Huston, George Michaelson, Rob Loomans

APNIC

IETF 69
Resource Certificate Profile

Background:

- This certificate is intended to express a “right-of-use relationship between the subject and an IP number resource set, as certified by the certificate’s issuer

- The certificate structure is intended to follow the allocation path – each party certifies their own allocation actions, so that the Issuer’s attestation regarding “right-of-use” mirrors the Issuer’s allocation actions of the number resource to a Subject

- The base profile is RFC3280 PKI Certificate Profile and RFC3779 IP Address extensions

- The proposed profile for Resource Certificates is in `draft-ietf-sidr-res-certs`
• General constraints:
  – This certificate profile is intended to be used in the context of a certificate hierarchy that mirrors the resource allocation hierarchy for public number resources
  – RFC3779 extensions are a CRITICAL extension and MUST be present, using a sorted canonical representation
  – An Issuer cannot certify more resources than the Issuer has in existing valid resource certificates
draft-ietf-sidr-res-certs

• Currently at version 07
  – Incorporated comments received since IETF 68
    • Many non-normative textual improvements.

• Current suggestions:
  – Remove SubjectAltName field from the profile
  – Require PKCS#10 support and CRMF as an option for Certificate Requests
  – Subject name is Issuer-determined
  – RSYNC as a MUST for SIA and AIA – is MUST appropriate?
Normative Changes

• 3.9 Resource Certificate Version 3 Extension Fields
  – The following X.509 V3 extensions MUST be present in a conforming Resource Certificate, except where explicitly noted otherwise.

• 3.9.1 Basic Constraints
  – The Basic Constraints extension field is a critical extension in the Resource Certificate profile, and MUST be present when the subject is a CA, and MUST NOT be present otherwise.

• 3.9.6 Authority Information Access
  – Following text removed entirely
    • Alternatively, if the certificate issuer does not maintain a persistent URL for the must recent issued certificate for each subject, then the entity who is subject of a certificate MAY keep the most recent copy of the superior's issued certificate in the subject's publication space, and set the AIA to reference this subject-maintained copy of the immediate superior certificate.
Normative Changes (cont)

• 5.2 CRMF profile
  – This request may **MAY** be conveyed to the CA via a Registration Authority (RA), acting under the direction of a subject.

• 5.3 Certificate Extension Attributes in Certificate Requests
  – The following extensions may **MAY** appear in a PKCS#10 or CRMF Certificate Request. **Any other extensions MUST NOT appear in a Certificate Request.** This profile places the following additional constraints on these extensions:
    – Basic Constraints
      • replaced
        – If this is omitted then this field is assigned by the CA.
      • With
        – If this is omitted then the CA will issue an end entity certificate with the BasicConstraints extension not present in the issued certificate.
Normative Changes (cont)

- Basic Constraints (cont)
  - The CA MAY honour the SubjectType CA bit set of to off (End Entity certificate request), in which case the corresponding end entity certificate will not contain a BasicConstraints extension.

- AuthorityInformationAccess
  - changed MAY to MUST be omitted

- removed ASResources and IPResources entirely
Next Steps

• Generate an -08 version post IETF 69 based on comments

• Request WG chair for WG Last Call on this document