Resource Certificate Profile
SIDR WG Meeting
IETF 66, July 2006

draft-ietf-sidr-res-certs-01

Geoff Huston
Rob Loomans
George Michaelson

Objective

- Take RFC3280 profile and RFC3779 extension
- Provide a profile for “right-of-use” certificates
  - That reflect legitimate “right of use” of public number resources
  - Where validation can be based on the existing address allocation framework
  - That provides a consistent and bounded set of fields and values within the context of resource certificates
  - That can be used as a validation framework for secure IDR approaches

The Profile

- Applies to
  - X.509 Version 3 PKI Resource Certificates
  - X.509 Version 2 PKI Certificate Revocation List
  - RFC4211 Certificate Requests
  - [*PCKS#10 Certificate Request Profile to be added*]

X.509 V3 PKI Resource Certificates (1)

- Notes:
  1. Serial Number: unique per issuer

     Not monotonic increasing sequence
  2. Signature: sha-256 with RSA
  3. Subject Public Key: 2048 bits

     One alternative option is to specify "no less than 2048 bits" and allow for longer key sizes. On the other hand it may be preferable to move to EC-DSA instead of RSA, in which case allowing for the option of longer RSA key sizes may be considered inappropriate.
  4. Basic Constraints: Critical, No Path Length Constraint
  5. Subject Key Identifier: non-Critical, MUST be present
  6. Authority Key Identifier: non-Critical, MUST be present

X.509 V3 PKI Resource Certificates (2)

- Notes (con't)

7. CRLDP: RSYNC URI

   The reason for the specification of an RSYNC URI as a MUST in this profile is to ensure that relying parties who wish to maintain a local copy of a synchronized repository are not forced to maintain a retrieval capability using a potentially unbounded set of URI types. The profile is attempting to ensure that rsync should be all that is required to perform a repository synchronization operation.

X.509 V3 PKI Resource Certificates (3)

- Notes (con't)
  8. Authority Information Access

     propose to use Access Method of "id-ad-caRepository"
  9. Subject Information Access

     propose to use CA Access Method of ""id-ad-caRepository" and non-CA Access Method of ?
  10. Certificate Policies: Critical extension
  11. IP Resources: Critical extension
  12. AS Resources: Critical extension

      Either, or both must be present

X.509 V2 PKI Certificate Revocation List

- Notes:
  1. No indirection (CRL issuer is the CA)
  2. Scope is all certificates issued by this CA
  3. No Delta CRLs
  4. CRL Number: determines “most recent” CRL

X.509 Request CRMF (RFC 4211)

1. Subject Name: should be considered by the issuer
2. CRLDP

   The issue of where and how to specify where the subject will publish the CRL if the CA bit is set and honoured by the issuer is described here as information that is either provided in this field in the certificate request or provided via an "out-of-band" exchange. An alternative is to say that this field MUST be provided if the CA bit is set in the request
3. SIA

   If this field is missing than it is also an option for the Issuer to deny the request and not issue a certificate if the issued certificate was to have the CA bit set
4. IP Resources, AS Resources

X.509 Request CRMF (RFC 4211)

1. Control Fields: Authenticator Control

   The method of generation and authentication of this field is to be specified. The desirable properties include the ability to validate the subject and the authenticity of the provided public key.

2. Control Fields: Resource Class

   This specification of the resource class is related the various forms of resource allocation which imply that an entity may be the holder of resources with differing validation dates and differing validation paths. It may not be possible to issue a single certificate with an all-encompassing resource set. This allows for the issue of a certificate that is encompassing within a nominated resource class. The alternative is to specify the resources for which the certificate is to be issued, which assumes that the specified resources fall under the same resource class

Trust Anchors

- Use existing address distribution framework as a template for trust anchor selection
- Use a set of self-signed RIR resource certificates
- Each RIR self-signs against those resources where it has administrative responsibility
  - No cross-certification
- Potential to use a single IANA root in the future

Resource Certificate Validation

1. The certificate can be verified using the Issuer's public key and the signature algorithm
2. The current time lies within the certificate's Validity From and To values.
3. The certificate contains all fields that MUST be present and contains field values as specified in this profile for all field values that MUST be present.
4. No field value that MUST NOT be present is present in the certificate.
5. The Issuer has not revoked the certificate by placing the certificate's serial number on the Issuer's current Certificate Revocation List, and the CRL is itself valid.
6. That the resource extension data is equal to or more specific than the resource extension data contained in a valid certificate where this Issuer is the Subject (the previous certificate in the ordered sequence)
7. The Certificate Path originates at a trust anchor, and there exists a signing chain across the Certificate Path where the Subject of Certificate x in the Certificate Path matches the Issuer in Certificate x+1 in the Certificate Path.
8. The Issuer’s certificate is valid

Next Steps

- Refine current open issues
  - Subject Public Key
  - Access Method for AIA, SIA
  - Certificate Request Control Fields
- PKCS#10 Request Profile
- Security Considerations