SIDR
Internet-Draft
Intended status: Best Current Practice
Expires: December 21, 2006

G. Huston
R. Loomans
G. Michaelson
APNIC
June 19, 2006

A Profile for X.509 PKIX Resource Certificates
draft-ietf-sidr-res-certs-01.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a profile for X.509 certificates for the purposes of supporting validation of assertions of "right-to- use" of an Internet Number Resource (IP Addresses and Autonomous System Numbers). This profile is used to convey the authorization of the subject to be regarded as the current unique controlled of the IP addresses and AS numbers that are described in a Resource Certificate.

Table of Contents

1. Introduction

This document defines a profile for X.509 certificates for use in the context of Resources Certificates. Resource Certificates are X.509 certificates that conform to the PKIX profile [RFC3280] and to this additional profile, and attest that the subject has the "right-to-use" a listed set of IP addresses and Autonomous Numbers.

A Resource Certificate describes an action by an Issuer that binds a list of IP address blocks and AS numbers to the Subject of a certificate, identified by the unique association of the Subject's private key with the public key contained in the Resource Certificate.

In the context of the public Internet it is intended that Resource Certificates are used in a manner that is aligned to the public number resource distribution function, Specifically, when a number resource is allocated or assigned by a Registry to an entity, this allocation is described by a Resource Certificate issued by the Registry with a subject corresponding to the entity that is the recipient of this assignment or allocation. This corresponds to a hierarchical PKI structure, where Resource Certificates are only issued in one 'direction' and there is a single unique path from a "Root CA" to any valid certificate.

Validation of a certificate in such a hierarchical PKI can be undertaken by creating a valid issuer - subject chain from the trust anchor allocation authorities to the certificate [RFC4158].

Resource Certificates may be used in the context of secure inter-domain routing protocols to convey a right-to-use of an IP number resource that is being passed within the routing protocol, to verify legitimacy and correctness of routing information. Related use contexts include validation of access to Internet Routing Registries for nominated routing objects, validation of routing requests, and detection of potential unauthorized used of IP addresses.

This profile defines those fields that are used in a Resource Certificate that MUST be present for the certificate to be valid. Relying Parties SHOULD check that a Resource Certificate conforms to this profile as a requisite for validation of a Resource Certificate.

1.1. Terminology

It is assumed that the reader is familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC3280], "X.509 Extensions for IP Addresses and AS Identifiers" [RFC3779], "Internet

Protocol" [RFC0791], "Internet Protocol Version 6 (IPv6) Addressing Architecture" [RFC4291], "Internet Registry IP Allocation Guidelines" [RFC2050], and related regional Internet registry address management policy documents.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. Describing Resources in Certificates

The framework for describing an association between the subject of a certificate and the resources currently under the subject's current control is described in [RFC3779].

There are three aspects of this resource extension that are noted in this profile:

1. RFC 3779 notes that this resource extension SHOULD be a CRITICAL extension to the X.509 Certificate. This Resource Certificate profile further defines that the use of this certificate

extension MUST be used and MUST be marked as CRITICAL.

2. RFC 3779 defines a sorted canonical form of describing a resource set, with maximal spanning ranges and maximal spanning prefix masks as appropriate. All valid certificates in this profile MUST use this sorted canonical form of resource description

3. A test of the resource extension in the context of certificate unique value token within the context of certificates issued by the validity includes the first condition that the resources described in the Issuer's resource extension must encompass those of the Subject's resource extension. In this context "encompass" allows for the Issuer's resource set to be the same as, or a strict superset of, any subject's resource set. Certificate validity in the context of this profile also includes a second condition that no two (or more) certificates issued by a single Issuer to two (or more) different subjects have a non-null intersection of resources. In other words an Issuer can certify at most one unique subject as the unique holder of a right-to-use for any particular resource.

This implies that a test of certificate validity implies that there exists a set of valid certificates in an issuer-subject chain from one, and only one, trust anchor to the certificate in question, and that the resource extensions from the trust anchor to the certificate form a sequence of encompassing relationships.

3. Resource Certificate Fields

A Resource Certificate is a valid X.509 v3 public key certificate, consistent with the PKIX profile [RFC3280], containing the fields listed in this section. Unless specifically noted as being OPTIONAL, all the fields listed here MUST be present, and any other field MUST NOT appear in a conforming Resource Certificate. Where a field value is specified here this value MUST be used in conforming Resource Certificates.

3.1. Version

Resource Certificates are X.509 Version 3 certificates. This field MUST be present, and the Version MUST be 3 (i.e. the value of this field is 2).

3.2. Serial number

The serial number value is a positive integer that is unique per Issuer.

3.3. Signature Algorithm

This field describes the algorithm used to compute the signature on this certificate. This profile uses SHA-256 with RSA (sha256WithRSAEncryption), and the value for this field MUST be the OID value 1.2.840.113549.1.1.11 [RFC4055].

3.4. Issuer

This field identifies the entity that has signed and issued the certificate. The value of this field is an X.501 name.

3.5. Subject

This field identifies the entity to whom the resource has been allocated / assigned. The value of this field is an X.500 name. In this profile the subject name is determined by the Issuer.

This field MUST be non-empty.

3.6. Valid From

The starting time at which point the certificate is valid. In this profile the "Valid From" time is to be no earlier than the time of certificate generation. As per Section 4.1.2.5 of [RFC3280], Certificate Authorities (CAs) conforming to this profile MUST always encode the certificate's "Valid From" date through the year 2049 as

UTCTime, and dates in 2050 or later MUST be encoded as GeneralizedTime. These two time formats are defined in [RFC3280].

3.7. Valid To

The Valid To time is the date and time at which point in time the certificate's validity ends. It represents the anticipated lifetime of the resource allocation / assignment arrangement between the

Issuer and the Subject. As per Section 4.1.2.5 of [RFC3280], CAs conforming to this profile MUST always encode the certificate's "Valid To" date through the year 2049 as UTCTime, and dates in 2050 or later MUST be encoded as GeneralizedTime. These two time formats are defined in [RFC3280].

3.8. Subject Public Key Info

This field specifies the subject's public key and the algorithm with which the key is used. The public key algorithm MUST be RSA, and thus the OID for the algorithm is 1.2.840.113549.1.1.1. A minimum key size of 1024 bits is mandated in this profile. Regional Registry CAs MUST use a key size of 2048 bits.

[Note - not for publication. 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.]

3.9. Resource Certificate Version 3 Extension Fields

As noted in Section 4.2 of [RFC3280], each extension in a certificate is designated as either critical or non-critical. A certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize; however, a non-critical extension MAY be ignored if it is not recognized [RFC3280].

The following X.509 V3 extensions MUST be present in a conforming Resource Certificate.

3.9.1. Basic Constraints

The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.

The Issuer determines whether the cA boolean is set. If this bit is set, then it indicates that the Subject is allowed to issue resources certificates within this overall framework (i.e. the subject is

permitted be a CA).

The Path Length Constraint is not specified in this profile and MUST NOT be present.

The Basic Constraints extension field is a critical extension in the Resource Certificate profile, and MUST be present.

[note - not for publication. It is unclear whether the CA bit should be set on in all cases.

3.9.2. Subject Key Identifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key. To facilitate certification path construction, this extension MUST appear in all Resource Certificates. This extension is non-critical.

The value of the subject key identifier MUST be the value placed in the key identifier field of the Authority Key Identifier extension of certificates issued by the subject of this certificate.

The Key Identifier used here is the 160-bit SHA-1 hash of the value of the DER-encoded ASN.1 bit string of the subject public key, as described in Section 4.2.1.2 of[RFC3280].

3.9.3. Authority Key Identifier

The subject key identifier extension provides a means of identifying certificates that are signed by a particular issuer's private key, by providing a hash value of the corresponding Issuer's public key. To facilitate path construction, this extension MUST appear in all Resource Certificates. The keyIdentifier subfield MUST be present. The authorityCertIssuer and authorityCertSerialNumber subfields MAY be present. This extension is non-critical.

The Key Identifier used here is the 160-bit SHA-1 hash of the value of the DER-encoded ASN.1 bit string of the issuer's public key, as described in Section 4.2.1.1 of [RFC3280].

3.9.4. Key Usage

This describes the purpose of the certificate. This is a critical extension, and it MUST be present.

In certificates issued to CAs only the keyCertSign and CRLSign bits are set to TRUE. In end-entity certificates the digitialSignature bit MUST be set and MUST be the only bit set to TRUE.

3.9.5. CRL Distribution Points

This field (CRLDP) identifies the location(s) of the CRL(s) associated with certificates issued by this Issuer. This profile uses the URI form of object identification. The preferred URI access mechanism is a single "rsync" URL that references a single inclusive CRL for each issuer.

In this profile the certificate issuer is also the CRL issuer, implying at the CRLIssuer subfield MUST be omitted, and the distributionPoint subfield MUST be present. The Reasons subfield MUST be omitted.

The distributionPoint MUST contain general names, and MUST NOT contain a nameRelativeToCRLIssuer. The type of the general name MUST be of type URI. Furthermore, as the scope of the CRL is all certificates issued by this issuer, the sequence of distributionPoint values MUST contain only a single DistributionPointName set. The DistributionPointName set MAY contain more than one URI value. An rsync URI MUST be present in the DistributionPointName set.

This extension MUST be present and it is non-critical.

[NOTE - not for publication. 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. A more restrictive potential condition here (and also in the SIA and AIA extensions) is that one and only one RSYNC URI is permitted. This would reduce some of the potential variations in certificates and also stress that certificate access and use by relying parties is critically dependent on RSYNC access, and that other forms of access are not necessarily available to relying parties.]

3.9.6. Authority Information Access

This field (AIA) identifies the location of all certificates that are issued by this Issuer that are signed with the Issuer's private key that signed this certificate. This profile uses a URI form of object identification. The preferred URI access mechanisms is "rsync", and an rsync URI MUST be specified with an accessMethod value of id-ad-caIssuers. Other access method URIs MAY also be included in the value sequence of this extension.

This field MUST be present, and is non-critical.

[Note - not for publication rfc3280 defines only two OIDs for the access method, id-ad-caIssuers and id-ad-ocsp. It would appear that id-ad-ocsp is not relevant here in that OCSP is not included as part of the resource certificate profile - which leaves id-ad-caIssuers. The text in 4.2.2.1 of RFC3280 notes that: "the id-ad-caIssuers OID is used when the additional information lists CAs that have issued certificates superior to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user" However there is no intention to require that such a list be included in this subfield in this profile. The question is: What accessMethod OID should be used here in the Access Description?]

3.9.7. Subject Information Access

This field (SIA) identifies the location of information and services relating to the subject of the certificate in which the SIA extension appears that relate to the subject public key that is certified in this certificate. Where the Subject is a CA for Resource Certificates this information and service collection will include all current valid certificates that have been issued by this subject that are signed with the subject's corresponding private key. This profile uses a URI form of location identification. The preferred URI access mechanism is "rsync", and an rsync URI SHOULD be specified, with an access method value of id-ad-caRepository when the subject of the certificate is a CA. Other access method URIs MAY also be included in the value sequence of this extension.

This field MUST be present when the subject is a CA, and is non-critical. Where the subject is not a CA this field MUST NOT be present.

[Note - not for publication. RFC3280 defines only two OIDs for the access method, id-ad-caRepository and id-ad-timeStamping, with the difference being whether the subject is a CA or not. The access method id-ad-caRepository appears to be appropriate where the subject is a CA. Where the subject is NOT a CA would it be useful to have the SIA extension point to where the subject stores digital objects

that have been signed by the subject? If this were considered to be desirable, then the id-ad-timeStamping appears to be inappropriate in this context. The general question is: What accessMethod OID should be used here in the Access Description? The approach currently used in this draft is that SIA should only be present for CAs and must be absent in the case of End Entity certificates.]

3.9.8. Certificate Policies

This extension MUST reference the Resource Certificate Policy, using the OID Policy Identifier value of "1.3.6.1.5.5.7.14.2". This field MUST be present and MUST contain only this value for Resource Certificates.

PolicyQualifiers MUST NOT be used in this profile.

This extension MUST be present and it is critical.

3.9.9. Subject Alternate Name

This is an optional extension, and MAY contain an X.501 Name as supplied by the subject in the Certificate Request or as assigned by the Issuer CA.

3.9.10. IP Resources

This field contains the list of IP address resources as per [RFC3779]. The value may specify the "inherit" element for a particular AFI value and an optional SAFI value. All Resource Certificates MUST include an IP Resources extension, an AS Resources extension, or both extensions.

This extension, if present, MUST be marked critical.

3.9.11. AS Resources

This field contains the list of AS number resources as per [RFC3779], or may specify the "inherit" element. All Resource Certificates MUST include an IP Resources extension, an AS Resources extension, or both

extensions. RDI values are NOT supported in this profile and MUST NOT be used.

This extension, if present, MUST be marked critical.

4. Resource Certificate Revocation List Profile

Each Resource CA MUST issue a version 2Certificate Revocation List (CRL), consistent with [RFC3280]. The CRL issuer is the CA, and no indirect CRLs are supported in this profile. The scope of the CRL MUST be "all certificates issued by this CA". The contents of the CRL are a list of all unexpired certificates issued by the CA that have been revoked by the CA.

An entry MUST NOT be removed from the CRL until it appears on one

regularly scheduled CRL issued beyond the revoked certificate's validity period.

This profile does not allow issuance of Delta CRLs.

The profile does not allow the issuance of multiple current CRLs with different scope by a single CA.

No CRL fields other than those listed below are allowed in CRLs issued under this profile. Unless otherwise indicated, these fields MUST be present in the CRL. Where two or more CRLs issued by a single CA are present in a certificate repository, the CRL with the highest value of the "CRL Number" field supersedes all other extant CRLs issued by this CA..

4.1. Version

Resource Certificate Revocation Lists are Version 2 certificates (the integer value of this field is 1).

4.2. Issuer Name

The value of this field is the X.501 name of the issuing CA who is also the signer of the CRL, and is identical to the Issuer name in the Resource Certificates.

4.3. This Update

This is the date and time that this CRL was issued. The value of this field MUST be encoded as UTCTime for dates through the year 2049, and MUST be encoded as GeneralizedTime for dates in the year 2050 or later.

4.4. Next Update

This is the date and time by which the next CRL will be issued. The value of this field MUST be encoded as UTCTime for dates through the year 2049, and MUST be encoded as GeneralizedTime for dates in the year 2050 or later.

4.5. Signature

This field contains the algorithm used to sign this CRL. The signature algorithm MUST be SHA-256 with RSA. This field MUST be present.

4.6. Revoked Certificate List

When there are no revoked certificates, then the revoked certificate list MUST be absent.

For each revoked resource certificate ONLY the following fields MUST be present. No CRL entry extensions are supported in this profile.

4.6.1. Serial Number

The serial number of the revoked certificate.

4.6.2. Revocation Date

The time the certificate was revoked. This time SHOULD NOT be a future date. The value of this field MUST be encoded as UTCTime for dates through the year 2049, and MUST be encoded as GeneralizedTime for dates in the year 2050 or later.

4.7. CRL Extensions

The X.509 v2 CRL format allows extensions to be placed in a CRL. The following extensions are supported in this profile, and MUST be present in a CRL.

4.7.1. Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. Conforming CRL issuers MUST use the key identifier method. The syntax for this CRL extension is defined in section 4.2.1.1 of [RFC3280].

This extension is non-critical.

4.7.2. CRL Number

The CRL Number extension conveys a monotonically increasing sequence number for a given CA. This extension allows users to easily determine when a particular CRL supersedes another CRL. The higher CRL Number value supersedes all other CRLs issued by the CA within the scope of this profile.

This extension is non-critical.

5. Resource Certificate Request Profile

This profile refines the specification in [RFC4211], as it relates to Resource Certificates. A Certificate Request Message object, formatted according to the Certificate Request Message Format (CRMF), is passed to a Certificate Authority as the initial step in issuing a certificate.

[Note - not for publication. RFC2986 references PKCS #10: Certification Request Syntax Specification, Version 1.7. Given the relative wide support of CMC, the extension of PKCS#10 that is

roughly equivalent to CMP, then it would appear that a CMC profile should also be included here. It is unclear at this point whether a PCKS#10 profile is also necessary in this profile.]

This request may be conveyed to the CA via a Registration Authority (RA), acting under the direction of a Subject.

[Note - not for publication: There are no profile-based qualifications regarding Proof-of-Possession. This may be refined in subsequent iterations of this draft.]

5.1. Resource Certificate Request Template Fields

This profile applies the following additional constraints to fields that may appear in a Certificate Request Template:

Version
: This field MAY be absent, or MAY specify the request of a Version 3 Certificate.

SerialNumber
: As per [RFC4211], this field is assigned by the CA and MUST be omitted in this profile.

SigningAlgorithm
: As per [RFC4211], this field is assigned by the CA and MUST be omitted in this profile.

Issuer
: This field is assigned by the CA and MUST be omitted in this profile.

Validity
: This field MAY be omitted. If omitted, the CA will issue a Certificate with Validity dates as determined by the CA. If specified, then the CA MAY override the requested values with

dates as determined by the CA.

Subject As the subject name is assigned by the CA, this field MAY be omitted, in which case the subject name will be generated by the CA. If specified, the CA SHOULD consider this as the subject's suggestion, but the CA is NOT bound to honour this suggestion.

PublicKey
This field MUST be present.

This profile applies the following additional constraints to X509 v3 Certificate extension fields that may appear in a Certificate Request:

BasicConstraints
If this is omitted then this field is assigned by the CA.

The Path Length Constraint is not supported in this Resource Certificate Profile, and this field MUST be omitted in this profile.

The CA MAY honour the SubjectType CA bit set to on. If this bit is set, then it indicates that the Subject is allowed to issue resources certificates within this overall framework.

The CA MAY honour the SubjectType CA bit set of off (End Entity certificate request).

[Note - not for publication. There are some potential variants on this model, where the CA bit may be considered as being set in all circumstances. For example, if the generation of signed resource objects, such as routing origination authorities requires the generation of special purpose resource certificates whose validity dates are implicitly the validity dates of the associated authority, then the subject needs to be able to issue certificates - i.e. there is a CA requirement. In this version of the draft this is left as a subject suggestion in the request that the CA may, or may not, honor in the issued certificate. In this model all the entities are CAs, except for the users of ROA signing shadow certs. In both cases, the CA knows the intended purpose (i.e. issue to others: CA, issue shadow to yourself: non-CA).]

SubjectKeyIdentifier
This field is assigned by the CA and MUST be omitted in this profile.

AuthorityKeyIdentifier
This field is assigned by the CA and MUST be omitted in this profile.

KeyUsage
The CA MAY honor KeyUsage extensions of CertificateSigning and CRLSigning if present, as long as this is consistent with the BasicConstraints SubjectType subfield, when specified.

CRLDistributionPoints
This field MAY be honoured by the CA on the condition that the CA issues a certificate with the BasicConstraints SubjectType CA bit set and the KeyUsage set to CertificateSigning and CRLSigning.

If specified, this field contains a sequence of URIs that references a CRL that will be published by the subject for subordinate certificates. This sequence MUST include a rsync URI. This field MAY be honoured by the CA if present.

If this field is omitted and KeyUsage is set to CertificateSigning then the CA MUST generate a CRLDistributionPoint URL based on out-of-band information that has been passed between the CA and the requester.

[Note - not for publication. The issue of where and how to specify where the subject will publish the CRL if the CA bit is set and honored 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.]

AuthorityInformationAccess
This field is assigned by the CA and MUST be omitted in this profile.

SubjectInformationAccess
This field MAY be honoured by the CA on the condition that the CA issues a certificate with the BasicConstraints SubjectType CA bit set and the KeyUsage set to CertificateSigning and CRLSigning.

If specified, this field contains a URI of the form of a single rsync URL that references a single publication point that will be used by the subject for all certificates that published by the subject for subordinate certificates, and MUST be honoured by the CA.

If this field is omitted and KeyUsage is set to CertificateSigning then the CA MUST generate a SIA URL based on out-of-band information that has been passed between the CA and the requester.

[Note not for publication - the same considerations with respect to the CRL DistributionPoints apply to this field as well. i.e. 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.]

CertificatePolicies
: This field is assigned by the CA and MUST be omitted in this profile.

SubjectAlternateName
: This field MAY be present, and the CA MAY use this as the SubjectAltName in the issued Certificate.

IPResources
: This field is assigned by the CA and MUST be omitted in this profile.

ASResources
: This field is assigned by the CA and MUST be omitted in this profile.

With the exception of the publicKey field, the CA is permitted to alter any requested field.

5.2. Resource Certificate Request Control Fields

The following control fields are supported in this profile:

Authenticator Control

It is noted that the intended model of authentication of the subject in a long term one, and the advice as offered in [RFC4211] is that the Authenticator Control field be used.

[Note - not for publication: 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.]

Resource Class

The profile defines an additional control for Resource Certificate Requests, namely a Resource Class control.
The Subject MUST specify a Resource Class value as specified by the CA to which the request refers. The CA will issue a certificate with the IPAddress and AS Number resources that match the subject's right-of-use of these resources with the class of resources specified by the Resource Class control value.

[Note - not for publication: 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, even when the entity is the recipient of resources allocated from a single 'upstream' issuing registry. Due to this consideration it may not be possible to issue a single certificate with an all-encompassing resource set. Alternatively it is possible to define a structure where there is no Resource Class specified and the issuer issues a set of spanning certificates for all resources held by the subject (i.e. all resources that fall under the subject's "right-of-use")]

6. Resource Certificate Validation

This section describes the Resource Certificate validation procedure. This refines the generic procedure described in [RFC3280]:

To meet this goal, the path validation process verifies, among other

things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

1. for all x in {1, ..., n-1}, the subject of certificate x is the issuer of certificate x+1;

2. certificate 1 is issued by a trust anchor;

3. certificate n is the certificate to be validated; and

4. for all x in {1, ..., n}, the certificate was valid at the time in question.

6.1. Trust Anchors for Resource Certificates

The trust model used in the resource certificate framework in the context of validation of assertions of public number resources in public-use contexts is a top-down delegated CA model that mirrors the delegation of resources from a registry distribution point to the entities that are the direct recipients of these resources. Within the trust model these recipient entities may, in turn, operate a registry and perform further allocations or assignments. This is a strict hierarchy, in that any number resource and a corresponding recipient entity has only one 'parent' issuing registry for that number resource (i.e. there is always a unique parent entity for any resource and corresponding entity), and that the issuing registry is not a direct or indirect subordinate recipient entity of the recipient entity in question (i.e. no loops in the hierarchy). The only exception to the "no loop" condition are the nominated trust anchors, where a self-signed certificate is issued.

At the time of preparing this draft there are proposed to be multiple roots of this public number resource hierarchy, corresponding to multiple trust anchors. These trust anchors are the self-signed certificates that are issued by the Regional Internet Registries. Each self-signed certificate issued by a RIR contains a resource set that describes those resources where the RIR is administratively responsible. There MUST NOT be overlap of resources in the IP resource extensions across the collection of RIR self-signed

certificates. This implies that a validation path for any valid certificate is unique, in the sense that the path will terminate with a single trust anchor.

Cross-certification of these trust anchors, where one trust anchor entity issues a certificate with a subject of another trust anchor is not seen as providing any further substance to the integrity or ease of validation in this trust model, so cross-certification is not used in the trust anchor structure for this Resource Certificate framework.

The adoption of a single trust anchor as a unique distinguished root of this certificate hierarchy is a potential future option here, and within the proposed framework some care has been taken not to preclude the potential for a single distinguished root for this certificate framework that could issue a certificate to each RIR with a resource extension that matches the resource sets that fall under the administrative responsibility of each RIR.

6.2. Resource Extension Validation

The IP resource extension definition [RFC3779] defines a critical extensions for Internet number resources. These are ASN.1 encoded representations of the IPv4 and IPv6 address range (either as a prefix/length, or start-end pair) and the AS number set.

Valid Resource Certificates MUST have a valid IP address and/or AS number resource extension. In order to validate a Resource Certificate the resource extension must also be validated. This validation process relies on definitions of comparison of resource sets:

more specific Given two IP address or AS number contiguous ranges, A and B, A is "more specific" than B if range B includes all IP addresses or AS numbers described by range A, and if range B is larger than range A.

equal Given two IP address or AS number contiguous ranges, A and B,

A is "equal" to B if range A describes precisely the same collection of IP addresses or AS numbers as described by range B. The definition of "inheritance" in [RFC3779]is equivalent to this "equality" comparison.

Validation of a certificate's resource extension in the context of an ordered certification path of {1,2, ... , n} where '1'is a trust anchor and 'n' is the target certificate, implies that each of the contiguous resource sets of IP addresses and AS Numbers described in certificate x, for 'x' is greater than , are more specific or equal to the resources described in certificate x-1.

6.3. Resource Certificate Path Validation

Validation of signed resource data using a target resource certificate consists of assembling an ordered sequence (or 'Certificate Path') of certificates ({1,2,...n} where '1' is a trust anchor, and 'n' is the target certificate) verifying that all of the following conditions hold:

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.

Validation of a certificate may perform these tests in any chosen order.

A Resource Certificate may have a number of potential parent certificates, where a potential parent certificate is one where the subject name matches the issuer name of the resource certificate. A candidate parent certificate is any member of the parent certificate set where the resource extension validity constraint is satisfied, and a valid candidate parent certificate is any candidate parent certificate that also matches validity conditions 1 through 6. A valid parent certificate is a valid candidate parent certificate that also matches validity condition 7.

Certificates and CRLs used in this process may be found on a single repository, maintained by a regular top-down walk from the Root Trust Anchors via Issuer certificates and their SIA fields as forward pointers, plus the CRLDP. Alternatively, validation may be performed using a bottom-up process with on-line certificate access using the AIA and CRLDP pointers to guide the certificate retrieval process.

There exists the possibility of encountering certificate paths that are arbitrarily long, or attempting to generate paths with loops as means of creating a potential DOS attack on a certificate validator. Some further heuristics may be required to halt the validation process in order to avoid some of the issues associated with attempts to validate such structures. It is suggested that implementations of Resource Certificate validation MAY halt with a validation failure if the certificate path length exceeds a pre-determined configuration parameter.

In the context of Resource Certificates that are generated in respect

of public resources and with the framework of the associated resource distribution process, it is suggested that this configuration parameter of maximum certificate path length be set to a value of 100. (There is no particular reason for suggesting this value other than the observation that it appears to be comfortably longer than

any real distribution chain for public number resources, without being too long so as to pose potential DOS concerns for relying parties performing a validation operation.)

7. Security Considerations

[to be completed]

8. IANA Considerations

[An OID for a resource class option in a certificate request may need to be defined.]

9. Acknowledgements

The authors would like to acknowledge the valued contributions from Stephen Kent, Robert Kisteleki, Randy Bush, Russ Housley, Ricardo Patara and Rob Austein in the preparation and subsequent review of this document.

10. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2050] Hubbard, K., Kosters, M., Conrad, D., Karrenberg, D., and J. Postel, "INTERNET REGISTRY IP ALLOCATION GUIDELINES", BCP 12, RFC 2050, November 1996.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in

the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

[RFC4158] Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., and R. Nicholas, "Internet X.509 Public Key Infrastructure: Certification Path Building", RFC 4158, September 2005.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, September 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

Appendix A. Example Resource Certificate

The following is an example Resource Certificate.

Certificate Name: UDkyh1nUjIjk5_WpdkZMh3KuvYo-25f7.crt

```
Data:
  Version: 3
  Serial:  9719 (0x25f7)
  Signature Algorithm:
           Hash: SHA256, Encryption: RSA
  Issuer:  CN=APNIC-AP-IANA
  Validity:
           Not Before: Fri May 12 05:37:43 2006 GMT
           Not After:  Thu Aug 10 05:37:43 2006 GMT
  Subject: CN=FC9B85ADDF5B
  Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
           Modulus (1024 bit):
                00:f2:e5:63:d6:e3:89:45:47:02:13:90:b7:e5:39:
                a3:f0:8c:3b:27:0d:d1:90:92:46:9b:45:d0:52:34:
                f1:7c:c7:34:9f:be:d0:41:18:ab:35:43:62:89:2e:
                3e:32:ab:01:e2:86:76:2a:44:83:49:4c:83:02:b4:
                0c:2a:b0:b2:82:c6:35:24:7b:16:7a:35:42:36:15:
                18:50:fe:8b:7f:c9:04:18:69:6b:ed:59:0d:61:ea:
                20:ef:cd:19:30:9f:ce:b8:4a:f5:fb:ad:81:42:ab:
                57:72:0c:47:b0:d8:30:c0:0c:5b:52:dc:aa:94:95:
                3e:fe:44:ac:d5:b0:f4:d5:cb
           Exponent: 65537 (0x10001)
  X509v3 extensions:
    Basic Constraints:
```

```
            CA:TRUE
        Subject Key Identifier:
            keyid: 50:39:32:87:59:D4:8C:88:E4:E7:F5:A9:
                   76:46:4C:87:72:AE:BD:8A
        Authority Key Identifier:
            keyid: 19:54:CD:F2:81:C6:4E:31:09:6D:3A:15:
                   E6:88:39:30:21:A6:56:73
        Key Usage: critical
            Certificate Sign, CRL Sign
        CRL Distribution Points:
            URI:rsync://rsync.apnic.net/repository/
                       pvpjvwUeQix2e54X8fGbhmdYMo0/
                       GVTN8oHGTjEJbToV5og5MCGmVnM/
                       GVTN8oHGTjEJbToV5og5MCGmVnM.crl
        Authority Information Access:
            CA Issuers - URI:rsync://rsync.apnic.net/repository/
                                    pvpjvwUeQix2e54X8fGbhmdYMo0/
                                    GVTN8oHGTjEJbToV5og5MCGmVnM
        Subject Information Access:
            CA Repository - URI:rsync://rsync.apnic.net/repository/
                                   pvpjvwUeQix2e54X8fGbhmdYMo0/
                                   GVTN8oHGTjEJbToV5og5MCGmVnM/
                                   UDkyh1nUjIjk5_WpdkZMh3KuvYo
        Certificate Policies: critical
            Policy: 1.3.6.1.5.5.7.14.2
        ipAddrBlock: critical
            192.0.0.0/24
        autonomousSysNum: critical
            64512
        Subject Alternative Name:
            DirName:/CN=<subject_supplied_string>

    Signature:
            72:27:9c:bc:a8:7f:c0:f0:27:62:a1:1f:55:b3:c7:b1:31:c9:fc:
            42:84:71:30:3b:0d:c0:d6:ad:79:b1:f6:1d:14:e8:f3:0f:f3:dd:
            40:3d:ae:28:a6:33:96:b6:d3:7d:d2:f3:ac:d3:8e:d4:2e:ad:ab:
            71:4d:05:74:20:ed:bc:e3:bd:85:7f:af:8b:70:3e:b8:90:b6:2d:
            a5:e3:9d:2a:c8:a9:9b:73:3c:03:43:d2:b8:d2:4e:68:34:eb:db:
            3c:44:eb:eb:1e:3b:03:d9:3b:e0:64:a6:31:90:9b:2c:4a:26:8e:
            0e:36:4c:ee:c8:e9:29:6b:78:61:87:05:e2:f9
```

Appendix B. Example Certificate Revocation List

The following is an example Certificate Revocation List.


```
Certificate Name: GVTN8oHGTjEJbToV5og5MCGmVnM.crl

Data:
  Version: 2
  Issuer:  CN=APNIC-AP-IANA
  Effective Date: Fri May 12 05:37:43 2006 GMT
  Next Update:    Fri May 26 05:37:43 2006 GMT
  Signature algorithn
           Hash: SHA256, Encryption: RSA
  CRL V2 Extensions:
    Authority Key Identifier:
      Keyid: 19:54:cd:f2:81:c6:4e:31:09:6d:3a:15:
             e6:88:39:30:21:a6:56:73
      Certificate Issuer:
             CN=APNIC-AP-IANA
      Certificate Serial Number: 1b
    CRL Number:  1097
  Revocation List:
    Revoked Certificates
      Serial Number: 0b
        Revocation Date: Mon May 8 05:10:19 2006 GMT
      Serial Number: 0c
        Revocation Date: Mon May 8 05:10:19 2006 GMT
```

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net
URI: http://www.apnic.net

Robert Loomans

Asia Pacific Network Information Centre

Email: robertl@apnic.net
URI: http://www.apnic.net

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net
URI: http://www.apnic.net

Full Copyright Statement

Intellectual Property

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).