

Individual Submission
Internet-Draft
Intended status: Best Current
Practice
Expires: December 11, 2006

G. Huston
R. Loomans
G. Michaelson
APNIC
June 9, 2006

A Profile for X.509 PKIX Resource Certificates
draft-ietf-sidr-res-certs-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 11, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

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.

Internet-Draft

Resource Certificate Profile

June 2006

Table of Contents

1.	Introduction	4
1.1.	Terminology	4
2.	Describing Resources in Certificates	5
3.	Resource Certificate Fields	6
3.1.	Version	6
3.2.	Serial number	6
3.3.	Signature Algorithm	6
3.4.	Issuer	6
3.5.	Subject	6
3.6.	Valid From	7
3.7.	Valid To	7
3.8.	Subject Public Key Info	7
3.9.	Resource Certificate Version 3 Extension Fields	7
3.9.1.	Basic Constraints	7
3.9.2.	Subject Key Identifier	8
3.9.3.	Authority Key Identifier	8
3.9.4.	Key Usage	8
3.9.5.	CRL Distribution Points	8
3.9.6.	Authority Information Access	9
3.9.7.	Subject Information Access	9
3.9.8.	Certificate Policies	9
3.9.9.	Subject Alternate Name	9
3.9.10.	IP Resources	9
3.9.11.	AS Resources	10
4.	Resource Certificate Revocation List Profile	10
4.1.	Version	10
4.2.	Issuer Name	10
4.3.	This Update	10
4.4.	Next Update	11
4.5.	Signature	11
4.6.	Revoked Certificate List	11
4.6.1.	Serial Number	11
4.6.2.	Revocation Date	11
4.7.	CRL Extensions	11
4.7.1.	Authority Key Identifier	11
4.7.2.	CRL Number	12
5.	Resource Certificate Request Profile	12
5.1.	Resource Certificate Request Template Fields	12
5.2.	Resource Certificate Request Control Fields	15
6.	Resource Certificate Validation	16
6.1.	Trust Anchors for Resource Certificates	16

6.2.	Resource Extension Validation	17
6.3.	Resource Certificate Path Validation	17
7.	Security Considerations	19
8.	IANA Considerations	19
9.	Normative References	19

Huston, et al.

Expires December 11, 2006

[Page 2]

Internet-Draft

Resource Certificate Profile

June 2006

Appendix A.	Example Resource Certificate	20
Appendix B.	Example Certificate Revocation List	21
Authors' Addresses		22
Intellectual Property and Copyright Statements		23

1. Introduction

This document defines a profile for X.509 certificates for use in the context of Resource Certificates. Resource Certificates are X.509 certificates that conform to this profile that convey the authority of a subject to be the entity that 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, such that when a number resource is allocated or assigned by a Registry to a receiving entity, then 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. Validation of a certificate can be undertaken by creating a valid issuer - subject chain from the trust anchor allocation authorities to the certificate.

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 use of IP addresses.

This document defines the fields that are used in a valid Resource Certificate that MUST be followed. Relying Parties SHOULD check that a Resource Certificate conforms to this profile as a necessary condition of 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.

Huston, et al.

Expires December 11, 2006

[Page 4]

Internet-Draft

Resource Certificate Profile

June 2006

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

This 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](#)]. It is noted that the RFC's description of this extension as a "right to use" is consistent with the assertion that the resources are "under the subject's current control."

There are three aspects of this extension that are noted here:

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 canonical form of describing a resource set,

with maximal spanning ranges and maximal spanning prefix masks as appropriate. All valid certificates in this certificate resource framework MUST use this 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 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 current controller of 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 valid X.509 / PKIX Resource Certificate contains the fields listed in the following sections. 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 (value is 2).

[3.2.](#) Serial number

The serial number value is a positive integer that is unique per Issuer. This field **MUST** be present in Resource Certificates.

[3.3.](#) Signature Algorithm

This field describes the algorithm used to compute the signature on this certificate. This profile uses SHA-256 with RSA. This field **MUST** be present and **MUST** use this value.

[3.4.](#) Issuer

This field identifies the entity that has signed and issued the certificate. The value of this field is an X.500 name. For a Root Trust Anchor this name is a self-selected name using only the Common Name (CN) X.500 name field. For a subordinate certificate this name **MUST** be the same name as the Subject name field on the 'parent' certificate. This field **MUST** be present.

[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 defined by the Issuer. All immediate subordinate certificates issued by this Subject **MUST** use an Issuer name that is identical to this Subject name.

This field **MUST** be present.

[3.6.](#) Valid From

The starting time at which point the certificate is valid. In this profile the "Valid From" time is no later than the time of certificate generation. As per [Section 4.1.2.5 of RFC 3280](#), 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](#)]. This field MUST be present.

[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 RFC 3280](#), 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](#)]. This field MUST be present.

[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 the Modulus must be no less than 1024 bits in length. This field MUST be present.

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

NOT be present.

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

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.

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 Subject Key Identifier is composed of the 160-bit SHA-1 hash of the value of the ASN.1 bit string of the subject public key (exponent and modulus), excluding the tag, length, and number of unused bits).

3.9.3. Authority Key Identifier

This field contains a hash of the Issuer's public key. The hash algorithm is SHA-1 (160) applied to the ASN.1 bit string of the Issuer public key (exponent and modulus), excluding the tag, length and number of unused bits) ([\[RFC3280\]](#), [Section 4.2.1.2](#)). This field MUST be present.

3.9.4. Key Usage

This describes the purpose of the certificate. This is a CRITICAL extension, and the field MUST be present.

The permissions permitted in this profile are Certificate signing and CRL signing if the Issuer permits the Subject to issue subordinate certificates.

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 a URI form of object identification. The preferred URI access mechanism is a single "rsync" URL that references a single inclusive CRL for each issuer.

This field MUST be present.

[3.9.6.](#) Authority Information Access

This field (AIA) identifies the location of all certificates that are issued by this Issuer. This profile uses a URI form of object identification. The preferred URI access mechanisms is "rsync".

This field MUST be present.

[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. 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. This profile uses a URI form of location identification. The preferred URI access mechanism is "rsync".

This field MUST be present.

[3.9.8.](#) Certificate Policies

This field 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.

The Resource Certificate Policy referenced by this OID MAY be referenced by a CPS Pointer qualifier.

This field MUST be present.

[3.9.9.](#) Subject Alternate Name

This is an OPTIONAL field, and may contain a Common Name as supplied by the subject in the Certificate Request. The Subject Alternative Name Field has no significance in terms of use of the certificate to validate assertions made by the Subject on in validation assertions made by subordinate entities that rely on a trust chain that includes the subject.

[3.9.10.](#) IP Resources

This field contains the list of IP address resources as per [\[RFC3779\]](#). Either IP Resources or AS Resources fields, or both, MUST be present in all Resource Certificates.

This is a CRITICAL field.

[3.9.11.](#) AS Resources

This field contains the list of AS number resources as per [[RFC3779](#)]. Either IP Resources or AS Resources fields, or both, MUST be present in all Resource Certificates.

This is a CRITICAL field.

[4.](#) Resource Certificate Revocation List Profile

Resource Certificate Authorities (CA) MUST issue a Certificate Revocation List (CRL). The CRL issuer is the CA, and no indirect CRLs are supported in the scope of this profile. The scope of the CRL in this profile 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.

This profile does not encompass the issuing of Delta CRLs, nor does the profile encompass the issuance of multiple CRLs by a single CA.

The following fields are REQUIRED in a conforming CRL. No other CRL fields are supported in this profile. 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 supercedes 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). This field MUST be present.

[4.2.](#) Issuer Name

The value of this field is the X.500 name of the issuing CA who is also the signer of the CRL, and is identical to the Issuer name in the Resource Certificates. This field MUST be present.

[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. This field MUST be present.

[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. This field MUST be present.

[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 the following fields are used in this profile. No CRL extensions are supported in this profile.

[4.6.1.](#) Serial Number

The Issuer's serial number of the revoked certificate. This field MUST be present.

[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. This field MUST be present.

[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.

[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. The syntax for this CRL extension is defined in [section 4.2.1.1 of \[RFC3280\]](#).

Conforming CRL issuers MUST use the key identifier method (defined in [section 5.2.1 of \[RFC3280\]](#)), and MUST include this extension in all CRLs issued.

Huston, et al.

Expires December 11, 2006

[Page 11]

Internet-Draft

Resource Certificate Profile

June 2006

[4.7.2.](#) CRL Number

The CRL number is a non-critical CRL extension which conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer. This extension allows users to easily determine when a particular CRL supersedes another CRL. The higher CRL Number value supercedes all other CRLs issued by the CA within the scope of this profile. CRL issuers conforming to this profile MUST include this extension in all CRLs.

[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.

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

[There are no profile-based qualifications are noted 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

[[RFC4211](#)] indicates that this MUST be 2, if supplied. As Resource Certificates are Version 3 certificates, this field MUST be omitted in this profile.

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 assign a ValidityFrom date based on the certificate issue date and a ValidityTo date based on the CA's business rule. If this field is not omitted then at least one of notBefore and notAfter MUST be specified.

notBefore

This field will be mapped to the ValidityFrom certificate field. If this field is later than the CA's business rule for certificate issuance, then the request MAY NOT be honored.

notAfter

This field will be mapped to the ValidityTo certificate field.

Values of notAfter prior to the current time MUST be considered as an invalid Certificate Request. If this field is later than the CA's business rule for certificate issuance then issued certificate MAY use a ValidityTo date as determined by the CA's business rule for certificate issuance.

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 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).

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 URI of the form of a single "rsync" URL that references a single inclusive CRL that will be 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 CRLDistributionPoint URL within the repository hierarchy administered by the CA.

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 an SIA URL within the repository hierarchy administered by the CA.

Certificate Policies

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

SubjectAlternateName

This field MAY be present, and the CA SHOULD 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.

[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 andASNumber resources that match the subject's right-of-use of these resources with the class of resources specified by the Resource Class control value.

6. Resource Certificate Validation

This section describes the Resource Certificate validation model. 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 $\{1, \dots, n-1\}$, the subject of certificate x is the issuer of certificate $x+1$;
2. certificate 1 is issued by the trust anchor;
3. certificate n is the certificate to be validated; and
4. for all x in $\{1, \dots, n\}$, 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 the 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 a valid certificate will terminate in 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 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.

Validation of a certificate's resource extension in the context of an ordered certification path of {1, ..., n}, each of the contiguous resource sets of IP addresses and AS Numbers described in certificate x 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 ($\{1,2,\dots,n\}$ where '1' is a trust anchor, and 'n' is the target certificate) verifying that all of the

Huston, et al.

Expires December 11, 2006

[Page 17]

Internet-Draft

Resource Certificate Profile

June 2006

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. Normative References

- [RFC0791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), September 1981.
- [RFC2050] Hubbard, K., Kesters, 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.

Huston, et al. Expires December 11, 2006 [Page 19]

Internet-Draft Resource Certificate Profile June 2006

- [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

Huston, et al.

Expires December 11, 2006

[Page 20]

Internet-Draft

Resource Certificate Profile

June 2006

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 Issuers - 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.

Huston, et al.

Expires December 11, 2006

[Page 21]

Internet-Draft

Resource Certificate Profile

June 2006

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 algorithm
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: guh@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

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

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).

