

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 19, 2018

G. Huston
G. Michaelson
APNIC
C. Martinez
LACNIC
T. Bruijnzeels
RIPE NCC
A. Newton
ARIN
D. Shaw
AFRINIC
November 15, 2017

RPKI Validation Reconsidered
draft-ietf-sidr-rpki-validation-reconsidered-09

Abstract

This document specifies an alternative to the certificate validation procedure specified in [RFC 6487](#) that reduces aspects of operational fragility in the management of certificates in the RPKI, while retaining essential security features.

Where the procedure specified in [RFC 6487](#) requires that Resource Certificates are rejecting entirely if they are found to over-claim any resources not contained on the issuing certificate, the validation process defined here allows an issuing Certificate Authority to chose to communicate that such Resource Certificates should be accepted for the intersection of their resources and the issuing certificate.

This choice is signalled by form of a set of alternative Object Identifiers (OIDs) of [RFC 3779](#) X.509 Extensions for IP Addresses and AS Identifiers, and certificate policy for the Resource Public Key Infrastructure ([RFC 6484](#)). It should be noted that in case these OIDs are not used for any certificate under a Trust Anchor, the validation procedure defined here has the same outcome as the procedure defined in [RFC 6487](#).

Furthermore this document provides an alternative to ROA ([RFC 6482](#)), and BGPsec Router Certificate (BGPsec PKI Profiles - publication requested) validation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on May 19, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Requirements notation	3
2.	Certificate Validation in the RPKI	3
3.	Operational Considerations	4
4.	An Amended RPKI Certification Validation Process	5
4.1.	Verified Resource Sets	6
4.2.	Differences with existing standards	6
4.2.1.	Certificate Policy (CP) for use with validation reconsidered in the Resource PKI (RPKI)	6
4.2.2.	An alternative to RFC3779 X.509 Extensions for IP Addresses and AS Identifiers	7
4.2.3.	Addendum to RFC6268	11
4.2.4.	An alternative to RFC6487 Profile for X.509 PKIX Resource Certificates	13
4.2.5.	An alternative ROA validation RFC6482	16

4.2.6. An alternative to BGPsec Router Certificate Validation	17
4.3. An example	17
5. Deployment Considerations	19
6. Security Considerations	19
7. IANA Considerations	19
8. Acknowledgements	20
9. References	20
9.1. Normative References	20
9.2. Informative References	21
Authors' Addresses	21

[1.](#) Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

[2.](#) Certificate Validation in the RPKI

As currently defined in [section 7.2 of \[RFC6487\]](#), validation of PKIX certificates that conform to the RPKI profile relies on the use of a path validation process where each certificate in the validation path is required to meet the certificate validation criteria.

These criteria require, in particular, that the Internet Number Resources (INRs) of each certificate in the validation path are "encompassed" by INRs on the issuing certificate. The first certificate in the path is required to be a trust anchor, and its resources are considered valid by definition.

For example, in the following sequence:

Certificate 1 (trust anchor):

Issuer TA,

Subject TA,

Resources 192.0.2.0/24, 198.51.100.0/24,
2001:db8::/32, AS64496-AS64500

Certificate 2:

Issuer TA,

Subject CA1,

Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

Certificate 3:

Issuer CA1,

Subject CA2,

Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

ROA 1:

Embedded Certificate 4 (EE certificate):

Issuer CA2,

Subject R1,

Resources 192.0.2.0/24

Prefix 192.0.2.0/24, Max Length 24, ASN 64496

All certificates in this scenario are considered valid since the INRs of each certificate are encompassed by those of the issuing certificate. ROA1 is valid because the specified prefix is encompassed by the embedded EE certificate, as required by [[RFC6482](#)].

3. Operational Considerations

The allocations recorded in the RPKI change as a result of resource transfers. For example, the CAs involved in transfer might choose to modify CA certificates in an order that causes some of these certificates to "over-claim" temporarily. A certificate is said to "over-claim" if it includes INRs not contained in the INRs of the CA that issued the certificate in question.

It may also happen that a child CA does not voluntarily request a shrunk resource certificate when resources are being transferred or reclaimed by the parent. Furthermore operational errors that may occur during management of RPKI databases also may create CA certificates that, temporarily, no longer encompass all of the INRs of subordinate certificates.

Consider the following sequence:

Certificate 1 (trust anchor):

Issuer TA,

Subject TA,

Resources 192.0.2.0/24, 198.51.100.0/24,
2001:db8::/32, AS64496-AS64500

Certificate 2:

Issuer TA,

Subject CA1,

Resources 192.0.2.0/24, 2001:db8::/32

Certificate 3 (invalid):

Issuer CA1,

Subject CA2,

Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

ROA 1 (invalid):

Embedded Certificate 4 (EE certificate, invalid):

Issuer CA2,

Subject R1,

Resources 192.0.2.0/24

Prefix 192.0.2.0/24, Max Length 24, ASN 64496

Here Certificate 2 from the previous example was re-issued by TA to CA1 and the prefix 198.51.100.0/24 was removed. However, CA1 failed to re-issue a new Certificate 3 to CA2. As a result Certificate 3 is now over-claiming and considered invalid; by recursion the embedded Certificate 4 used for ROA1 is also invalid. And ROA1 is invalid because the specified prefix contained in the ROA is no longer encompassed by a valid embedded EE certificate, as required by [\[RFC6482\]](#)

However, it should be noted that ROA1 does not make use of any of the address resources that were removed from CA1's certificate, and thus it would be desirable if ROA1 could still be viewed as valid. Technically CA1 should re-issue a Certificate 3 to CA2 without 198.51.100.0/24, and then ROA1 would be considered valid according to [\[RFC6482\]](#). But as long as CA1 does not take this action, ROA1 remains invalid. It would be preferable if ROA1 could be considered valid, since the assertion it makes was not affected by the reduced scope of CA1's certificate.

[4.](#) An Amended RPKI Certification Validation Process

4.1. Verified Resource Sets

The problem described above can be considered as a low probability problem today. However the potential impact on routing security would be high if an over-claiming occurred near the apex of the RPKI hierarchy, as this would invalidate the entirety of the sub-tree located below this point.

The changes specified here to the validation procedure in [\[RFC6487\]](#) do not change the probability of this problem, but they do limit the impact to just the over-claimed resources. This revised validation algorithm is intended to avoid causing CA certificates to be treated as completely invalid as a result of over-claims. However, these changes are designed to not degrade the security offered by the RPKI. Specifically, ROAs and router certificates will be treated as valid only if all of the resources contained in them are encompassed by all superior certificates along a path to a trust anchor.

The way this is achieved conceptually is by maintaining a Verified Resource Set (VRS) for each certificate that is separate from the INRs found in the [\[RFC3779\]](#) resource extension in the certificate.

4.2. Differences with existing standards

4.2.1. Certificate Policy (CP) for use with validation reconsidered in the Resource PKI (RPKI)

Note that [section 1.2 of \[RFC6484\]](#) defines the "Certificate Policy (CP) for the Resource PKI (RPKI)" with the following OID:

```
id-cp-ipAddr-asNumber OBJECT IDENTIFIER ::= { iso(1)
    identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) cp(14) 2 }
```

This document requests an assignment of a new OID for an alternative "Certificate Policy (CP) for use with validation reconsidered in the Resource PKI (RPKI)" as follows:

```
id-cp-ipAddr-asNumber-v2 OBJECT IDENTIFIER ::= { iso(1)
    identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) cp(14) TBD1 }
```

This alternative Certificate Policy is the same as the Certificate Policy described in [\[RFC6484\]](#), except that it is used to drive the decision in step 8 of the validation procedure described in [Section 4.2.4.4](#).

4.2.2. An alternative to [RFC3779](#) X.509 Extensions for IP Addresses and AS Identifiers

This document defines an alternative to [\[RFC3779\]](#). All specifications and procedures described in [\[RFC3779\]](#) apply, with the following notable exceptions.

4.2.2.1. OID for id-pe-ipAddrBlocks-v2

This document request an OID for the extension id-pe-ipAddrBlocks-v2 (id-pe TBD2). This OID MUST only be used in conjunction with the alternative Certificate Policy OID defined in [Section 4.2.1](#).

The following is an amended specification to be used as an alternative to the specification in [section 2.2.1 of \[RFC3779\]](#).

The OID for this extension is id-pe-ipAddrBlocks-v2.

id-pe-ipAddrBlocks-v2 OBJECT IDENTIFIER ::= { id-pe TBD2 }

where [\[RFC5280\]](#) defines:

id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }

4.2.2.2. Syntax for id-pe-ipAddrBlocks-v2

```

id-pe-ipAddrBlocks-v2      OBJECT IDENTIFIER ::= { id-pe TBD2 }

IPAddrBlocks               ::= SEQUENCE OF IPAddressFamily

IPAddressFamily             ::= SEQUENCE {      -- AFI & optional SAFI --
  addressFamily             OCTET STRING (SIZE (2..3)),
  ipAddressChoice           IPAddressChoice }

IPAddressChoice             ::= CHOICE {
  inherit                   NULL, -- inherit from issuer --
  addressesOrRanges         SEQUENCE OF IPAddressOrRange }

IPAddressOrRange            ::= CHOICE {
  addressPrefix             IPAddress,
  addressRange              IPAddressRange }

IPAddressRange              ::= SEQUENCE {
  min                       IPAddress,
  max                       IPAddress }

IPAddress                   ::= BIT STRING

```

Note that the descriptions of objects referenced in the syntax above are defined in sections [2.2.3.1](#) through [2.2.3.9](#) of [\[RFC3779\]](#).

[4.2.2.3](#). OID for id-pe-autonomousSysIds-v2

This document request an OID for the extension id-pe-autonomousSysIds-v2 (id-pe TBD3). This OID MUST only be used in conjunction with the alternative Certificate Policy OID defined in [Section 4.2.1](#).

The following is an amended specification to be used as an alternative to the specification in [section 3.2.1 of \[RFC3779\]](#).

The OID for this extension is id-pe-autonomousSysIds-v2.

```
id-pe-autonomousSysIds-v2  OBJECT IDENTIFIER ::= { id-pe TBD3 }
```

where [\[RFC5280\]](#) defines:

```

id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
                                   dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }

```

4.2.2.4. Syntax for id-pe-autonomousSysIds-v2

id-pe-autonomousSysIds-v2 OBJECT IDENTIFIER ::= { id-pe TBD3 }

ASIdentifiers ::= SEQUENCE {
asnum [0] EXPLICIT ASIdentifierChoice OPTIONAL,
rdi [1] EXPLICIT ASIdentifierChoice OPTIONAL}

ASIdentifierChoice ::= CHOICE {
inherit NULL, -- inherit from issuer --
asIdsOrRanges SEQUENCE OF ASIdOrRange }

ASIdOrRange ::= CHOICE {
id ASId,
range ASRange }

ASRange ::= SEQUENCE {
min ASId,
max ASId }

ASId ::= INTEGER

4.2.2.5. Amended IP Address Delegation Extension Certification Path Validation

Certificate path validation is performed as specified in [Section 4.2.4.4](#).

4.2.2.6. Amended Autonomous System Identifier Delegation Extension Certification Path Validation

Certificate path validation is performed as specified in [Section 4.2.4.4](#).

4.2.2.7. Amended ASN.1 module

This document requests an OID for id-mod-ip-addr-and-as-ident-v2, as follows:

```
IPAddrAndASCertExtn-v2 { iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7) mod(0)
  id-mod-ip-addr-and-as-ident-v2(TBD4) }
```

The following is an amended specification to be used as an alternative to the specification in section [appendix A of \[RFC3779\]](#).

This normative appendix describes the IP address and AS identifiers extensions used by conforming PKI components in ASN.1 syntax.

```
IPAddrAndASCertExtn-v2 { iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7) mod(0)
  id-mod-ip-addr-and-as-ident-v2(TBD4) }
```

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

IMPORTS

-- PKIX specific OIDs and arcs --

```
id-pe FROM PKIX1Explicit88 { iso(1) identified-organization(3)
  dod(6) internet(1) security(5) mechanisms(5) pkix(7)
  id-mod(0) id-pkix1-explicit(18) }
```

-- IP Address Block and AS Identifiers Syntax --

```
IPAddrBlocks, ASIdentifiers FROM IPAddrAndASCertExtn { iso(1)
  identified-organization(3) dod(6) internet(1) security(5)
  mechanisms(5) pkix(7) mod(0) id-mod-ip-addr-and-as-ident(30) }
;
```

-- Validation Reconsidered IP Address Delegation Extension OID --

```
id-pe-ipAddrBlocks-v2 OBJECT IDENTIFIER ::= { id-pe TBD2 }
```

-- Validation Reconsidered IP Address Delegation Extension Syntax --
-- Syntax is imported from [[RFC3779](#)] --

-- Validation Reconsidered Autonomous System Identifier --
-- Delegation Extension OID --

```
id-pe-autonomousSysIds-v2 OBJECT IDENTIFIER ::= { id-pe TBD3 }
```

-- Validation Reconsidered Autonomous System Identifier --
-- Delegation Extension Syntax --

-- Syntax is imported from [[RFC3779](#)] --

END

4.2.3. Addendum to [RFC6268](#)

This document requests an OID for id-mod-ip-addr-and-as-ident-2v2 as follows:

```
IPAddrAndASCertExtn-2010v2 { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) mod(0)
    id-mod-ip-addr-and-as-ident-2v2(TBD5) }
```

[RFC6268] is an informational RFC that updates some auxiliary ASN.1 modules to conform to the 2008 version of ASN.1; the 1988 ASN.1 modules in [Section 4.2.2.7](#) remain the normative version.

The following is an additional module confirming to the 2008 version of ASN.1 to be used with the extensions defined in [Section 4.2.2.1](#) and [Section 4.2.2.3](#).

```
IPAddrAndASCertExtn-2010v2 { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) mod(0)
    id-mod-ip-addr-and-as-ident-2v2(TBD5) }
```

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

```
EXPORTS ALL;
IMPORTS
```

```
-- PKIX specific OIDs and arcs --
```

```
id-pe
FROM PKIX1Explicit-2009
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkix1-explicit-02(51)}
```

```
EXTENSION
FROM PKIX-CommonTypes-2009
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkixCommon-02(57)}
```

```
-- IP Address Block and AS Identifiers Syntax --
```

```
IPAddrBlocks, ASIdentifiers
FROM IPAddrAndASCertExtn-2010
{ iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7) mod(0)
```



```
        id-mod-ip-addr-and-as-ident-2(72) }
;

--
-- Extensions contains the set of extensions defined in this
-- module
--
-- These are intended to be placed in public key certificates
-- and thus should be added to the CertExtensions extension
-- set in PKIXImplicit-2009 defined for [RFC5280]
--

Extensions EXTENSION ::= {
    ext-pe-ipAddrBlocks-v2 | ext-pe-autonomousSysIds-v2
}

-- Validation Reconsidered IP Address Delegation Extension OID --

ext-pe-ipAddrBlocks-v2 EXTENSION ::= {
    SYNTAX IPAddrBlocks
    IDENTIFIED BY id-pe-ipAddrBlocks-v2
}

id-pe-ipAddrBlocks-v2 OBJECT IDENTIFIER ::= { id-pe TBD2 }

-- Validation Reconsidered IP Address Delegation --
--      Extension Syntax                               --

-- Syntax is imported from [RFC6268] --

-- Validation Reconsidered Autonomous System Identifier --
--      Delegation Extension OID                               --

ext-pe-autonomousSysIds-v2 EXTENSION ::= {
    SYNTAX ASIdentifiers
    IDENTIFIED BY id-pe-autonomousSysIds-v2
}

id-pe-autonomousSysIds OBJECT IDENTIFIER ::= { id-pe TBD3 }

-- Validation Reconsidered Autonomous System Identifier --
--      Delegation Extension Syntax                               --

-- Syntax is imported from [RFC6268] --

END
```


4.2.4. An alternative to [RFC6487](#) Profile for X.509 PKIX Resource Certificates

This document defines an alternative Profile for X.509 PKIX Resource Certificates. This profile follows all definitions and procedures described in [\[RFC6487\]](#) with the following notable exceptions.

4.2.4.1. Amended Certificate Policies

The following is an amended specification to be used in this profile, in place of [section 4.8.9 of \[RFC6487\]](#).

This extension MUST be present and MUST be marked critical. It MUST include exactly one policy of type id-cp-ipAddr-asNumber-v2, as specified in the updated RPKI CP in [Section 4.2.1](#).

4.2.4.2. Amended IP Resources

The following is an amended specification to be used in this profile, in place of [section 4.8.10 of \[RFC6487\]](#).

Either the IP Resources extension, or the AS Resources extension, or both, MUST be present in all RPKI certificates, and if present, MUST be marked critical.

This extension contains the list of IP address resources as per [Section 4.2.2.1](#). The value may specify the "inherit" element for a particular Address Family Identifier (AFI) value. In the context of resource certificates describing public number resources for use in the public Internet, the Subsequent AFI (SAFI) value MUST NOT be used.

This extension MUST either specify a non-empty set of IP address records, or use the "inherit" setting to indicate that the IP address resource set of this certificate is inherited from that of the certificate's issuer.

4.2.4.3. Amended AS Resources

The following is an amended specification to be used in this profile, in place of [section 4.8.11 of \[RFC6487\]](#).

Either the AS Resources extension, or the IP Resources extension, or both, MUST be present in all RPKI certificates, and if present, MUST be marked critical.

This extension contains the list of AS number resources as per [Section 4.2.2.3](#), or it may specify the "inherit" element. Routing

Domain Identifier (RDI) values are NOT supported in this profile and MUST NOT be used.

This extension MUST either specify a non-empty set of AS number records, or use the "inherit" setting to indicate that the AS number resource set of this certificate is inherited from that of the certificate's issuer.

4.2.4.4. Amended Resource Certificate Path Validation

The following is an amended specification for path validation to be used in place of [section 7.2 of \[RFC6487\]](#) allowing for the validation of both certificates following the profile defined in [\[RFC6487\]](#), as well as certificates following the profile described above.

The following algorithm is employed to validate CA and EE resources certificates. It is modelled on the path validation algorithm from [\[RFC5280\]](#), but modified to make use of the IP Address Delegation and AS Identifier Delegation Extensions from [\[RFC3779\]](#).

There are two inputs to the validation algorithm:

1. a trust anchor
2. a certificate to be validated

The algorithm is initialized with two new variables for use in the RPKI: Validated Resource Set-IP (VRS-IP) and Validated Resource Set-AS (VRS-AS). These sets are used to track the set of INRs (IP address space and AS Numbers) that are considered valid for each CA certificate. The VRS-IP and VRS-AS sets are initially set to the IP Address Delegation and AS Identifier Delegation values, respectively, from the trust anchor used to perform validation.

This path validation algorithm verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

- a. for all 'x' in {1, ..., n-1}, the subject of certificate 'x' is the issuer of certificate ('x' + 1);
- b. certificate '1' is issued by a trust anchor;
- c. certificate 'n' is the certificate to be validated; and
- d. for all 'x' in {1, ..., n}, certificate 'x' is valid.

Certificate validation requires verifying that all of the following conditions hold, in addition to the certification path validation criteria specified in [Section 6 of \[RFC5280\]](#).

1. The signature of certificate x ($x > 1$) is verified using the public key of the issuer's certificate ($x-1$), using the signature algorithm specified for that public key (in certificate $x-1$).
2. The current time lies within the interval defined by the NotBefore and NotAfter values in the Validity field of certificate x .
3. The Version, Issuer, and Subject fields of certificate x satisfy the constraints established in [Section 4.1-4.7](#) of this specification.
4. If certificate x uses the Certificate Policy defined in [section 4.8.9 of \[RFC6487\]](#), then the certificate MUST contain all extensions defined in [section 4.8 of \[RFC6487\]](#) that must be present. The value(s) for each of these extensions MUST satisfy the constraints established for each extension in the respective sections. Any extension not thus identified MUST NOT appear in certificate x .
5. If certificate x uses the Certificate Policy defined in [Section 4.2.4.1](#), then all extensions defined in [section 4.8 of \[RFC6487\]](#), except sections [4.8.9](#), [4.8.10](#) and [4.8.10](#) MUST be present. The certificate MUST contain an extension as defined in [Section 4.2.4.2](#) or [Section 4.2.4.3](#), or both. The value(s) for each of these extensions MUST satisfy the constraints established for each extension in the respective sections. Any extension not thus identified MUST NOT appear in certificate x .
6. Certificate x MUST NOT have been revoked, i.e., it MUST NOT appear on a CRL issued by the CA represented by certificate $x-1$.
7. Compute the VRS-IP and VRS-AS set values as indicated below:
 - * If the IP Address Delegation extension is present in certificate x and $x=1$, set the VRS-IP to the resources found in this extension.
 - * If the IP Address Delegation extension is present in certificate x and $x > 1$, set the VRS-IP to the intersection of the resources between this extension and the value of the VRS-IP computed for certificate $x-1$.

- * If the IP Address Delegation extension is absent in certificate x, set the VRS-IP to NULL.
 - * If the IP Address Delegation extension is present in certificate x and $x=1$, set the VRS-IP to the resources found in this extension.
 - * If the AS Identifier Delegation extension is present in certificate x and $x>1$, set the VRS-AS to the intersection of the resources between this extension and the value of the VRS-AS computed for certificate x-1
 - * If the AS Identifier Delegation extension is absent in certificate x, set the VRS-AS to NULL.
8. If there is any difference in resources in the VRS-IP and the IP Address Delegation extension on certificate x, or the VRS-AS and the AS Identifier Delegation extension on certificate x, then:
- * If certificate x uses the Certificate Policy defined in [Section 4.2.4.1](#) a warning listing the over-claiming resources for certificate x SHOULD be issued.
 - * If certificate x uses the Certificate Policy defined in [section 4.8.9 of \[RFC6487\]](#), then certificate x MUST be rejected.

These rules allow a CA certificate to contain resources that are not present in (all of) the certificates along the path from the trust anchor to the CA certificate. If none of the resources in the CA certificate are present in all certificates along the path, no subordinate certificates could be valid. However, the certificate is not immediately rejected as this may be a transient condition. Not immediately rejecting the certificate does not result in a security problem because the associated VRS sets accurately reflect the resources validly associated with the certificate in question.

[4.2.5.](#) An alternative ROA validation [RFC6482](#)

[Section 4 of \[RFC6482\]](#) currently has the following text on the validation of resources on a ROA:

- o The IP address delegation extension [\[RFC3779\]](#) is present in the end-entity (EE) certificate (contained within the ROA), and each IP address prefix(es) in the ROA is contained within the set of IP addresses specified by the EE certificate's IP address delegation extension.

If the end-entity certificate uses the Certificate Policy defined in [Section 4.2.4.1](#), then the following approach must be used instead.

- o The amended IP address delegation extension described in [Section 4.2.4.2](#) is present in the end-entity (EE) certificate (contained within the ROA), and each IP address prefix(es) in the ROA is contained within the VRS-IP set that is specified as an outcome of EE certificate validation described in [Section 4.2.4.4](#).

Note that this ensures that ROAs can be valid only, if all IP address prefixes in the ROA are encompassed by the VRS-IP of all certificates along the path to the trust anchor used to verify it.

Operators MAY issue separate ROAs for each IP address prefix, so that the loss of one or more IP address prefixes from the VRS-IP of any certificate along the path to the trust anchor would not invalidate authorizations for other IP address prefixes.

[4.2.6.](#) An alternative to BGPsec Router Certificate Validation

If a BGPsec Router Certificate ([[I-D.ietf-sidr-bgpsec-pki-profiles](#)]) uses the Certificate Policy defined in [Section 4.2.4.1](#), then in addition to the BGPsec Router Certificate Validation defined in section 3.3 of [[I-D.ietf-sidr-bgpsec-pki-profiles](#)], the following constraint MUST be met:

- o The VRS-AS of BGPsec Router Certificates MUST encompass all ASNs in the AS Resource Identifier Delegation extension.

Operators MAY issue separate BGPsec Router Certificates for different ASNs, so that the loss of on ASN from the VRS-AS of any certificate along the path to the trust anchor would not invalidate router keys for other ASNs.

[4.3.](#) An example

Consider the following example under the amended approach:

Certificate 1 (trust anchor):

Issuer TA,
Subject TA,
Resources 192.0.2.0/24, 198.51.100.0/24,
2001:db8::/32, AS64496-AS64500

Verified Resource Set: 192.0.2.0/24, 198.51.100.0/24,
2001:db8::/32, AS64496-AS64500

Warnings: none

Certificate 2:

Issuer TA,
Subject CA1,
Resources 192.0.2.0/24, 2001:db8::/32, AS64496

Verified Resource Set: 192.0.2.0/24,
2001:db8::/32, AS64496

Warnings: none

Certificate 3:

Issuer CA1,
Subject CA2,
Resources 192.0.2.0/24, 198.51.100.0/24, AS64496

Verified Resource Set: 192.0.2.0/24, AS64496
Warnings: over-claim for 198.51.100.0/24

ROA 1 (valid):

Embedded Certificate 4 (EE certificate):
Issuer CA2,
Subject R1,
Resources 192.0.2.0/24

Verified resources: 192.0.2.0/24
Warnings: none

Prefix 192.0.2.0/24, Max Length 24, ASN 64496

ROA1 is considered valid because the prefix matches the Verified Resource Set on the embedded EE certificate.

ROA 2 (invalid):

Embedded Certificate 5 (EE certificate invalid):
Issuer CA2,
Subject R2,
Resources 198.51.100.0/24

EE certificate is invalid due to over-claim for 198.51.100.0/24

Prefix 198.51.100.0/24, Max Length 24, ASN 64496

ROA2 is considered invalid because the embedded EE certificate is considered invalid.

BGPsec Certificate 1 (valid):

Issuer CA2
Subject ROUTER-64496
Resources AS64496

Verified resources: AS64496
Warnings: none

BGPsec Certificate 2 (invalid):
Issuer CA2
Subject ALL-ROUTERS
Resources AS64496-AS64497

EE certificate is invalid due to over-claim for AS64497

This problem can be mitigated by issuing separate certificates for each AS number.

5. Deployment Considerations

Because this document introduces new OIDs and an alternative the Profile for X.509 PKIX Resource Certificates described in [\[RFC6487\]](#), the use of such certificates in the global RPKI will lead to the rejection of such certificates by Relying Party tools that do not (yet) implement the alternative profile described in this document.

For this reason it is important that such tools are updated before Certificate Authorities start to use this specification.

However, because the choice of algorithm is well-defined for each certificate and/or RPKI signed object, there is no strict requirement for all Certificate Authorities to migrate to this new algorithm within a specific time period. The choice to opt-in to this can be made by each CA independently. CAs MAY also choose to use the new algorithm for new certificates or objects only, without pro-actively re-issuing existing objects - for example because the latter would require an active authorisation by a user of the system.

6. Security Considerations

The authors believe that the revised validation algorithm introduces no new security vulnerabilities into the RPKI, because it cannot lead to any ROA and/or Router Certificates to be accepted if they contain resources that are not held by the issuer.

7. IANA Considerations

IANA is to add the following to the SMI Security for PKIX Certificate Policies registry:

Decimal	Description	References
TBD1	id-cp-ipAddr-asNumber-v2	[section 4.2.1]

IANA is to add the following to the SMI Security for PKIX Certificate Extension registry:

Decimal	Description	References
TBD2	id-pe-ipAddrBlocks-v2	[section 4.2.2.1]
TBD3	id-pe-autonomousSysIds-v2	[section 4.2.2.3]

IANA is to add the following to the SMI Security for PKIX Module Identifier registry:

Decimal	Description	References
TBD4	id-mod-ip-addr-and-as-ident-v2	[section 4.2.2.7]
TBD5	id-mod-ip-addr-and-as-ident-2v2	[section 4.2.3]

8. Acknowledgements

The authors would like to thank Stephen Kent for reviewing and contributing to this document. We would like to thank Rob Austein for suggesting that separate OIDs should be used to make the behaviour of Relying Party tools deterministic, and we would like to thank Russ Hously, Sean Turner and Tom Petch for their contributions on OID and ASN.1 updates. Finally we would like to thank Tom Harrison for a general review of this document.

9. References

9.1. Normative References

- [I-D.ietf-sidr-bgpsec-pki-profiles]
Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", [draft-ietf-sidr-bgpsec-pki-profiles-21](#) (work in progress), January 2017.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", [RFC 3779](#), DOI 10.17487/RFC3779, June 2004, <<https://www.rfc-editor.org/info/rfc3779>>.

- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 5280](#), DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", [RFC 6482](#), DOI 10.17487/RFC6482, February 2012, <<https://www.rfc-editor.org/info/rfc6482>>.
- [RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", [BCP 173](#), [RFC 6484](#), DOI 10.17487/RFC6484, February 2012, <<https://www.rfc-editor.org/info/rfc6484>>.
- [RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", [RFC 6487](#), DOI 10.17487/RFC6487, February 2012, <<https://www.rfc-editor.org/info/rfc6487>>.

9.2. Informative References

- [RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", [RFC 6268](#), DOI 10.17487/RFC6268, July 2011, <<https://www.rfc-editor.org/info/rfc6268>>.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
Australia

Phone: +61 7 3858 3100
Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
Australia

Phone: +61 7 3858 3100
Email: ggm@apnic.net

Carlos M. Martinez
Latin American and Caribbean IP Address Regional Registry
Rambla Mexico 6125
Montevideo 11400
Uruguay

Phone: +598 2604 2222
Email: carlos@lacnic.net

Tim Bruijnzeels
RIPE Network Coordination Centre
Singel 258
Amsterdam 1016 AB
The Netherlands

Email: tim@ripe.net

Andrew Lee Newton
American Registry for Internet Numbers
3635 Concorde Parkway
Chantilly, VA 20151
USA

Email: andy@arin.net

Daniel Shaw
African Network Information Centre (AFRINIC)
11th Floor, Standard Chartered Tower
Cybercity, Ebene
Mauritius

Phone: +230 403 51 00
Email: daniel@afrinic.net

