Internet Engineering Task Force (IETF)
Request for Comments: 8360
Category: Standards Track
ISSN: 2070-1721
G. Huston
G. Michaelson
APNIC
C. Martinez
LACNIC
T. Bruijnzeels
RIPE NCC
A. Newton
ARIN
D. Shaw
AFRINIC
April 2018

Resource Public Key Infrastructure (RPKI) Validation Reconsidered

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 Resource Public Key Infrastructure (RPKI), while retaining essential security features.

The procedure specified in RFC 6487 requires that Resource Certificates are rejected entirely if they are found to overclaim any resources not contained on the issuing certificate, whereas the validation process defined here allows an issuing Certification Authority (CA) to chose to communicate that such Resource Certificates should be accepted for the intersection of their resources and the issuing certificate.

It should be noted that the validation process defined here considers validation under a single trust anchor (TA) only. In particular, concerns regarding overclaims where multiple configured TAs claim overlapping resources are considered out of scope for this document.

This choice is signaled by a set of alternative Object Identifiers (OIDs) per "X.509 Extensions for IP Addresses and AS Identifiers" (RFC 3779) and "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)" (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 Route Origin Authorization (ROA) (RFC 6482) and BGPsec Router Certificate (BGPsec PKI Profiles -- publication requested) validation.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8360.

Copyright Notice

Table of Contents

1. Overview

This document specifies an alternative to the certificate validation procedure specified in RFC 6487. Where the procedure specified in RFC 6487 will require that Resource Certificates be rejected entirely if they are found to overclaim any resources not contained on the issuing certificate, the procedure defined here dictates that these Resource Certificates be accepted for the intersection of their resources and the issuing certificate only.

The outcome of both procedures is the same as long as no overclaims occur. Furthermore, the new procedure can never lead to the acceptance of resources that are not validly held on the path of issuing certificates.

However, the procedure defined here will limit the impact in case resources are no longer validly held on the path of issuing certificates to attestations, such as Route Origin Authorizations [RFC6482] that refer to these resources only.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 end entity (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 "overclaim" temporarily. A certificate is said to "overclaim" 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 reissued by TA to CA1, and the prefix 198.51.100.0/24 was removed. However, CA1 failed to reissue a new Certificate 3 to CA2. As a result, Certificate 3 is now overclaiming 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; thus, it would be desirable if ROA1 could still be viewed as valid. Technically, CA1 should reissue 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 a low probability problem today. However, the potential impact on routing security would be high if an overclaiming occurred near the apex of the RPKI hierarchy, as this would invalidate the entirety of the subtree 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 overclaimed resources. This revised validation algorithm is intended to avoid causing CA certificates to be treated as completely invalid as a result of overclaims. 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 resource extension [RFC3779] in the certificate.

4.2. Differences with Existing Standards

4.2.1. Certificate Policy (CP) for Use with Validation Reconsidered in the 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 }
```

Per this document, a new OID for an alternative "Certificate Policy (CP) for use with validation reconsidered in the Resource PKI (RPKI)" has been assigned 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) 3 }
```

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 X.509 Extensions for IP Addresses and AS Identifiers (RFC 3779)

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

4.2.2.1. OID for id-pe-ipAddrBlocks-v2

Per this document, an OID has been assigned for the extension id-pe-ipAddrBlocks-v2 (id-pe 28). 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 28 }
```

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 28 }

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

Per this document, an OID has been assigned for the extension id-pe-autonomousSysIds-v2 (id-pe 29). 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 29 }
```

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 29 }

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

Per this document, an OID has been assigned 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(90) }
```

The following is an amended specification to be used as an alternative to the specification in Appendix A of [RFC3779].

This normative appendix describes the extensions for IP address and AS identifier delegation 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(90) }

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 28 }

-- Validation Reconsidered IP Address Delegation Extension Syntax --
-- Syntax is imported from RFC 3779 --

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

id-pe-autonomousSysIds-v2  OBJECT IDENTIFIER ::= { id-pe 29 }

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

-- Syntax is imported from RFC 3779 --

END
```

4.2.3. Addendum to RFC 6268

Per this document, an OID has been assigned 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(91) }
```

[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 conforming to the 2008 version of ASN.1 to be used with the extensions defined in Sections 4.2.2.1 and 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(91) }

  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 contain 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 RFC 5280
       --

       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 28 }

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

       -- Syntax is imported from RFC 6268 --

       -- 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 29 }
```

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

-- Syntax is imported from RFC 6268 --

END
```

4.2.4. An Alternative to the 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 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 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], which allows 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 resource certificates. It is modeled on the path validation algorithm from [RFC5280] but is 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: Verified Resource Set-IP (VRS-IP) and Verified 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 Sections 4.1 to 4.7 of RFC 6487.

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 4.8.11 MUST be present. The certificate MUST contain an extension as defined in Sections 4.2.4.2 or 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 Certificate Revocation List (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 overclaiming 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

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

> 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.

> 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 [RFC8209] 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 [RFC8209], the following constraint MUST be met:

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

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

5. Validation Examples

In this section, we will demonstrate the outcome of RPKI validation performed using the algorithm and procedures described in Sections 4.2.4.4, 4.2.5, and 4.2.6, under three deployment scenarios:

- An RPKI tree consisting of certificates using the old OIDs only
- An RPKI tree consisting of certificates using the new OIDs only
- An RPKI tree consisting of a mix of certificates using either the old or the new OIDs

In this context, we refer to a certificate as using the 'old' OIDs, if the certificate uses a combination of the OIDs defined in Section 1.2 of [RFC6484], Section 2.2.1 of [RFC3779], and/or Section 3.2.1 of [RFC3779]. We refer to a certificate as using the 'new' OIDS, if the certificate uses a combination of OIDs defined in Sections 4.2.4.1, 4.2.2.1, and/or Section 4.2.2.3.

5.1. Example 1 -- An RPKI Tree Using the Old OIDs Only

Consider the following example:

```
  Certificate 1 (trust anchor):
   Issuer: TA,
   Subject: TA,
   OIDs: OLD,
   Resources: 0/0, ::0, AS0-4294967295 (all resources)

    Verified Resource Set: 0/0, ::0, AS0-4294967295 (all resources)
    Warnings: none

  Certificate 2:
   Issuer: TA,
   Subject: CA1,
   OIDs: OLD,
   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 (invalid):
 Issuer: CA1,
 Subject: CA2,
 OIDs: OLD,
 Resources: 192.0.2.0/24, 198.51.100.0/24, AS64496

  Verified Resource Set: 192.0.2.0/24, AS64496

  Certificate 3 is considered invalid because resources
  contains 198.51.100.0/24, which is not found in the
  Verified Resource Set.

ROA 1 (invalid):
 Embedded Certificate 4 (EE certificate invalid):
  Issuer: CA2,
  Subject: R1,
  OIDs: OLD,
  Resources: 192.0.2.0/24
    Prefix 192.0.2.0/24, Max Length 24, ASN 64496

  ROA1 is considered invalid because Certificate 3 is invalid.

ROA 2 (invalid):
 Embedded Certificate 5 (EE certificate invalid):
  Issuer: CA2,
  Subject: R2,
  OIDs: OLD,
  Resources: 198.51.100.0/24
   Prefix 198.51.100.0/24, Max Length 24, ASN 64496

  ROA2 is considered invalid because Certificate 3 is invalid.

BGPsec Certificate 1 (invalid):
 Issuer: CA2,
 Subject: ROUTER-64496,
 OIDs: NEW,
 Resources: AS64496

  BGPsec Certificate 1 is invalid because Certificate 3 is invalid.

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

  BGPsec Certificate 2 is invalid because Certificate 3 is invalid.
```

5.2. Example 2 -- An RPKI Tree Using the New OIDs Only

Consider the following example under the amended approach:

```
Certificate 1 (trust anchor):
 Issuer: TA,
 Subject: TA,
 OIDs: NEW,
 Resources: 0/0, ::0, AS0-4294967295 (all resources)

  Verified Resource Set: 0/0, ::0, AS0-4294967295 (all resources)
  Warnings: none

Certificate 2:
 Issuer: TA,
 Subject: CA1,
 OIDs: NEW,
 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,
 OIDs: NEW,
 Resources: 192.0.2.0/24, 198.51.100.0/24, AS64496

  Verified Resource Set: 192.0.2.0/24, AS64496
  Warnings: overclaim for 198.51.100.0/24

ROA 1 (valid):
 Embedded Certificate 4 (EE certificate):
  Issuer: CA2,
  Subject: R1,
  OIDs: NEW,
  Resources: 192.0.2.0/24
   Prefix 192.0.2.0/24, Max Length 24, ASN 64496

   Verified Resource Set: 192.0.2.0/24
   Warnings: none

  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,
  OIDs: NEW,
  Resources: 198.51.100.0/24
    Prefix 198.51.100.0/24, Max Length 24, ASN 64496

    Verified Resource Set: none (empty set)
    Warnings: 198.51.100.0/24

  ROA2 is considered invalid because the ROA prefix 198.51.100.0/24
  is not contained in the Verified Resource Set.

BGPsec Certificate 1 (valid):
 Issuer: CA2,
 Subject: ROUTER-64496,
 OIDs: NEW,
 Resources: AS64496

  Verified Resource Set: AS64496
  Warnings: none

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

   Verified Resource Set: AS64496

  BGPsec Certificate 2 is invalid because not all of its resources
  are contained in the Verified Resource Set.

  Note that this problem can be mitigated by issuing separate
  certificates for each AS number.
```

5.3. Example 3 -- An RPKI Tree Using a Mix of Old and New OIDs

In the following example, new OIDs are used only for CA certificates where the issuing CA anticipates that an overclaim could occur and has a desire to limit the impact of this to just the overclaimed resources in question:

```
Certificate 1 (trust anchor):
 Issuer: TA,
 Subject: TA,
 OIDs: OLD,
 Resources: 0/0, ::0, AS0-4294967295 (all resources)

  Verified Resource Set: 0/0, ::0, AS0-4294967295 (all resources)
  Warnings: none

  Note that a trust anchor certificate cannot be found to
  overclaim.  So, using the new OIDs here would not change
  anything with regards to the validity of this certificate.

Certificate 2:
 Issuer: TA,
 Subject: CA1,
 OIDs: OLD,
 Resources: 192.0.2.0/24, 2001:db8::/32, AS64496

  Verified Resource Set: 192.0.2.0/24,
                         2001:db8::/32, AS64496
  Warnings: none

  Note that since the TA certificate claims all resources, it
  is impossible to issue a certificate below it that could be
  found to be overclaiming.  Therefore, there is no benefit
  in using the new OIDs for Certificate 2.

Certificate 3:
 Issuer: CA1,
 Subject: CA2,
 OIDs: NEW,
 Resources: 192.0.2.0/24, 198.51.100.0/24, AS64496

  Verified Resource Set: 192.0.2.0/24, AS64496
  Warnings: overclaim for 198.51.100.0/24

  Note that CA1 anticipated that it might invalid Certificate 3
  issued to CA2, if its own resources on Certificate 2 were
  modified and old OIDs were used on Certificate 3.
```

```
ROA 1 (valid):
 Embedded Certificate 4 (EE certificate):
  Issuer: CA2,
  Subject: R1,
  OIDs: OLD,
  Resources: 192.0.2.0/24
   Prefix 192.0.2.0/24, Max Length 24, ASN 64496

   Verified Resource Set: 192.0.2.0/24
   Warnings: none

  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,
  OIDs: OLD,
  Resources: 198.51.100.0/24
    Prefix 198.51.100.0/24, Max Length 24, ASN 64496

    Verified Resource Set: none (empty set)

  ROA2 is considered invalid because resources on its EE
  certificate contains 198.51.100.0/24, which is not contained
  in its Verified Resource Set.

  Note that if new OIDs were used here (as in example 2), ROA 2
  would be considered invalid because the prefix is not
  contained in the Verified Resource Set.

  So, if there is no difference in the validity outcome, one could
  argue that using old OIDs here is clearest, because any
  overclaim of ROA prefixes MUST result in it being considered
  invalid (as described in Section 4.2.5).

BGPsec Certificate 1 (valid):
 Issuer: CA2,
 Subject: ROUTER-64496,
 OIDs: OLD,
 Resources: AS64496

  Verified Resource Set: AS64496
  Warnings: none
```

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

   Verified Resource Set: AS64496
```

BGPsec Certificate 2 is considered invalid because resources contains AS64497, which is not contained in its Verified Resource Set.

Note that if new OIDs were used here (as in example 2), BGPsec Certificate 2 would be considered invalid because the prefix is not contained in the Verified Resource Set.

So, if there is no difference in the validity outcome, one could argue that using old OIDs here is the clearest, because any overclaim on this certificate MUST result in it being considered invalid (as described in Section 4.2.6).

Also note that, as in example 2, this problem can be mitigated by issuing separate certificates for each AS number.

6. Deployment Considerations

This document defines an alternative RPKI validation algorithm, but it does not dictate how this algorithm will be deployed. This should be discussed as a separate effort. That said, the following observations may help this discussion.

Because this document introduces new OIDs and an alternative to 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 Certification Authorities start to use this specification.

However, because the OIDs are defined in each RPKI certificate, there is no strict requirement for all Certification Authorities, or even for all the certificates they issue, to migrate to the new OIDs at the same time. The example in Section 5.3 illustrates a possible deployment where the new OIDs are used only in CA certificates where an accidental overclaim may occur.

7. 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.

8. IANA Considerations

IANA has added the following to the "SMI Security for PKIX Certificate Policies" registry:

Decimal	Description	References
3	id-cp-ipAddr-asNumber-v2	Section 4.2.1

IANA has added the following to the "SMI Security for PKIX Certificate Extension" registry:

Decimal	Description	References
28	id-pe-ipAddrBlocks-v2	Section 4.2.2.1
29	id-pe-autonomousSysIds-v2	Section 4.2.2.3

IANA has added the following to the "SMI Security for PKIX Module Identifier" registry:

Decimal	Description	References
90	id-mod-ip-addr-and-as-ident-v2	Section 4.2.2.7
91	id-mod-ip-addr-and-as-ident-2v2	Section 4.2.3

9. References

9.1. Normative References

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8209] Reynolds, M., Turner, S., and S. Kent, "A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", RFC 8209, DOI 10.17487/RFC8209, September 2017, <https://www.rfc-editor.org/info/rfc8209>.

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>.

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 behavior of Relying Party tools deterministic, and we would like to thank Russ Housley, 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.

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 Internet Address 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
United States of America

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