Registration Protocols Extensions (regext)
Internet-Draft
Intended status: Standards Track
Expires: 21 January 2026

J. Singh
ARIN
A. Newton
ICANN

20 July 2025

Registration Data Access Protocol (RDAP) Extension for Resource Public Key Infrastructure (RPKI) Registration Data
draft-ietf-regext-rdap-rpki-02

Abstract

The Resource Public Key Infrastructure (RPKI) is used to secure inter-domain routing on the internet. This document defines a new Registration Data Access Protocol (RDAP) extension with identifier "rpki1", for accessing the RPKI registration data in the Internet Number Registry System (INRS) for the Route Origin Authorization (ROA), Autonomous System Provider Authorization (ASPA), and X.509 Resource Certificate RPKI profiles through RDAP. The INRS is composed of Regional Internet Registries (RIRs), National Internet Registries (NIRs), and Local Internet Registries (LIRs).

Table of Contents

1. Introduction

The network operators are increasingly deploying the Resource Public Key Infrastructure (RPKI, [RFC6480]) to secure inter-domain routing ([RFC4271]) on the internet. RPKI enables Internet Number Resource (INR) holders to cryptographically assert about their registered IP addresses and autonomous system numbers to prevent route hijacks and leaks. To that end, RPKI defines the following profiles:

* Route Origin Authorization (ROA, [RFC9582]) where a Classless Inter-Domain Routing (CIDR, [RFC1519]) address block holder cryptographically asserts about the origin autonomous system (AS, [RFC4271]) for routing that CIDR address block.
* Autonomous System Provider Authorization (ASPA, [I-D.ietf-sidrops-aspa-profile]) where an autonomous system number (ASN, [RFC5396]) holder cryptographically asserts about the provider ASes for that ASN.
* X.509 Resource Certificate ([RFC6487]) where the issuer grants the subject a right-of-use for the listed IP addresses and/or autonomous system numbers.

This document defines a new RDAP extension with identifier "rpki1", for accessing the RPKI registration data in the Internet Number Registry System (INRS) for the aforementioned RPKI profiles through RDAP. The INRS is composed of Regional Internet Registries (RIRs), National Internet Registries (NIRs), and Local Internet Registries (LIRs).

The motivation here is that such RDAP data could complement the existing RPKI diagnostic tools (e.g., [ROUTINATOR], [NIST-RPKI-MONITOR], etc.) when troubleshooting a route hijack or leak, by conveniently providing access to registration information from a registry's database beside what is inherently available from an RPKI profile object. There is registration metadata that is often needed for troubleshooting that does not appear in an RPKI profile object or its verified payload but could be looked up or searched using RDAP; such as:

* When did the initial version of a ROA get published?
* Was a ROA created in conjunction with an Internet Routing Registry (IRR, [RFC2622]) route?
* Which IRR routes are related with a ROA?
* Which IP networks are associated with a ROA?
* Which ROAs are associated with an origin AS?

* Which ASPAs are associated with a provider AS?
* Which X.509 resource certificates are associated with an organization?
* Which organization is registered as the authoritative source for an RPKI profile object?

Furthermore, correlating registered RPKI data with registered IP networks and autonomous system numbers would also give access to the latter's contact information through RDAP entity objects, which should aid troubleshooting.

In addition to troubleshooting, serving RPKI metadata over RDAP offers a convenience to network operators through a simple lookup mechanism. As is demonstrated in [RDAP-GUIDE], constructing custom RDAP scripts is relatively easy and beneficial to network operators for the purposes of reporting. Though not RDAP-based, systems such as [JDR] and [CLOUDFLARE] have shown the utility of an approach that allows users to explore the RPKI hierarchy in a visual fashion, without interacting with the signed objects directly.

For these purposes, this specification defines RDAP object classes, as well as lookup and search path segments, for the ROA, ASPA, and X.509 resource certificate registration data.

1.1. Requirements Language

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.

Indentation and whitespace in examples are provided only to illustrate element relationships, and are not a required feature of this specification.

"..." in examples is used as shorthand for elements defined outside of this document, as well as to abbreviate elements that are too long.

2. Extension

This document defines a new RDAP extension with identifier "rpki1", for accessing the RPKI registration data in the INRS for the ROA, ASPA, and X.509 Resource Certificate RPKI profiles through RDAP.

A server that supports the functionality specified in this document MUST include the "rpki1" string literal in the "rdapConformance" array (Section 4.1 of [RFC9083]) for any lookup or search response containing an RDAP object per the object class definition in Section 4.1, Section 5.1, or Section 6.1, as well as in the help response. Here is an elided example for this inclusion:

```
{
  "rdapConformance":
  [
    "rdap_level_0",
    "rpki1",
    ...
  ],
  ...
}
```

This extension adheres to the guidelines in [I-D.ietf-regext-rdap-extensions].

The "1" in "rpki1" denotes version 1 of this extension. New versions of this extension will use different extension identifiers.

2.1. What It Is Not

This RDAP extension MUST NOT be used to directly influence internet routing. Neither RDAP nor this extension define the necessary security properties or distribution mechanisms required to securely add, remove, or modify internet routes.

2.2. In The Future

In the future, if the RDAP data for the RPKI profiles supported in this document needs to evolve and/or additional RPKI profiles need to be made accessible through RDAP, a new RDAP extension must be defined, adhering to the guidelines in [I-D.ietf-regext-rdap-extensions].

3. Common Data Members

The RDAP object classes for RPKI (Section 4.1, Section 5.1, Section 6.1) can contain one or more of the following common members:

* "handle" -- a string representing the registry-unique identifier of an RPKI object registration
* "name" -- a string representing the identifier assigned to an RPKI object registration by the registration holder

* "digests" -- an array of objects representing hashes that entirely cover an RPKI object; such an object can contain the following members:
  - "digest" -- a hexadecimal string representing the hash that entirely covers an RPKI object
  - "digestAlgorithm" -- a string literal representing the algorithm used to generate the hash that entirely covers an RPKI object, with possible values of "SHA-256" and "SHA-512" ([RFC6234]) for this version of the specification
* "notValidBefore" -- a string that contains the time and date in Zulu (Z) format with UTC offset of 00:00 ([RFC3339]), representing the not-valid-before date of an X.509 resource certificate for an RPKI object (Section 4 of [RFC6487])
* "notValidAfter" -- a string that contains the time and date in Zulu (Z) format with UTC offset of 00:00 ([RFC3339]), representing the not-valid-after date of an X.509 resource certificate for an RPKI object (Section 4 of [RFC6487])
* "publicationUri" -- a URI string pointing to the location of an RPKI object within an RPKI repository; the URI scheme is "rsync", per Section 4 of [RFC6487]
* "notificationUri" -- an HTTPS URI string pointing to the location of the RPKI Repository Delta Protocol (RRDP) update notification file for an RPKI repository (Section 3 of [RFC8182])
* "entities" -- an array of entity objects (Section 5.1 of [RFC9083]), including the organization (entity) registered as the authoritative source for an RPKI object
* "rpkiType" -- a string literal representing various combinations of an RPKI repository and a Certification Authority (CA), with the following possible values:
  - "hosted" -- both the repository and CA are operated by a registry for an organization with allocated resources
  - "delegated" -- both the repository and CA are operated by an organization with resources allocated by a registry
  - "hybrid" -- the repository is operated by a registry for an organization with allocated resources whereas the CA is operated by the organization itself

The purpose of an object with "digest" and "digestAlgorithm" members is to enable an RDAP server to present a message digest (hash) for an entire RPKI object, thereby providing RDAP clients with an exact reference to the underlying RPKI object. This can help with analysis, research, and/or debugging.

RRDP is intended as the long-term replacement for rsync in RPKI. For a CA that implements RRDP, the update notification file location is expected to be set in each X.509 resource certificate it issues (Section 3.2 of [RFC8182]). Consequently, the "notificationUri" data should help inform about the RPKI repository and/or CA operated downstream from a registry by an organization with resources allocated by that registry.

4. Route Origin Authorization

4.1. Object Class

The Route Origin Authorization (ROA) object class can contain the following members:

* "objectClassName" -- the string "rpki1_roa"
* "handle" -- see Section 3
* "name" -- see Section 3
* "digests" -- see Section 3
* "roaIps" -- an array of objects representing CIDR address blocks within a ROA; such an object can contain the following members:
  - "ip" -- a string representing an IPv4 or IPv6 CIDR address block with the "<CIDR prefix>/<CIDR length>" format (Section 4 of [RFC9582])
  - "maxLength" -- a number representing the maximum prefix length of the CIDR address block that the origin AS is authorized to advertise; up to 32 for IPv4 and up to 128 for IPv6 (Section 4 of [RFC9582])
* "originAutnum" -- an unsigned 32-bit integer representing the origin autonomous system number (Section 4 of [RFC9582])
* "notValidBefore" -- see Section 3
* "notValidAfter" -- see Section 3
* "publicationUri" -- see Section 3
* "notificationUri" -- see Section 3
* "entities" -- see Section 3
* "rpkiType" -- see Section 3
* "events" -- see Section 4.5 of [RFC9083]
* "links" -- "self" link, and "related" links for IP network and IRR (when defined) objects (Section 4.2 of [RFC9083])
* "remarks" -- see Section 4.3 of [RFC9083]

Here is an elided example of a ROA object:

```
{
  "objectClassName": "rpki1_roa",
  "handle": "XXXX",
  "name": "ROA-1",
  "digests":
  [
    {
      "digest": "01234567...89abcdef",
      "digestAlgorithm": "SHA-256",
    },
    ...
  ],
  "roaIps":
  [
    {
      "ip": "2001:db8::/48",
      "maxLength": 64
    },
    ...
  ],
  "originAutnum": 65536,
  "notValidBefore": "2024-04-27T23:59:59Z",
  "notValidAfter": "2025-04-27T23:59:59Z",
  "publicationUri": "rsync://example.net/path/to/XXXX.roa",
  "notificationUri": "https://example.net/path/to/notification.xml",
  "entities":
  [
    {
      "objectClassName": "entity",
      "handle": "XYZ-RIR",
      ...
    },
    ...
  ],
  "rpkiType": "hosted",
  "events":
  [
    {
      "eventAction": "registration",
      "eventDate": "2024-01-01T23:59:59Z"
    },
    ...
  ],
  "links":
  [
    {
      "value": "https://example.net/rdap/rpki1_roa/XXXX",
      "rel": "self",
```

```
        "href": "https://example.net/rdap/rpki1_roa/XXXX",
        "type": "application/rdap+json"
      },
      {
        "value": "https://example.net/rdap/rpki1_roa/XXXX",
        "rel": "related",
        "href": "https://example.net/rdap/ip/2001:db8::/48",
        "type": "application/rdap+json"
      },
      ...
    ],
    "remarks":
    [
      {
        "description": [ "ROA" ]
      }
    ]
  }
```

4.2. Lookup

The resource type path segment for exact or closest match lookup of a ROA object is "rpki1_roa".

The following lookup path segments are defined for a ROA object:

Syntax: rpki1_roa/<handle>

Syntax: rpki1_roa/<IP address>

Syntax: rpki1_roa/<CIDR prefix>/<CIDR length>

Syntax: rpki1_roa/<digest algorithm>/<digest>

A lookup query for ROA information by handle is specified using this form:

rpki1_roa/XXXX

XXXX is a string representing the "handle" property of a ROA, as described in Section 4.1. The following URL would be used to find information for a ROA that exactly matches the "8a848ab0729f0f4f0173ba2013bc5eb3" handle:

https://example.net/rdap/rpki1_roa/8a848ab0729f0f4f0173ba2013bc5eb3

A lookup query for ROA information by IP address is specified using this form:

rpki1_roa/YYYY

YYYY is a string representing an IPv4 or IPv6 address. The following URL would be used to find information for the most-specific ROA matching the "192.0.2.0" IP address:

https://example.net/rdap/rpki1_roa/192.0.2.0

Similarly, for the "2001:db8::" IP address:

https://example.net/rdap/rpki1_roa/2001%3Adb8%3A%3A

A lookup query for ROA information by CIDR is specified using this form:

rpki1_roa/YYYY/ZZZZ

YYYY/ZZZZ is a string representing the "ip" property of a CIDR address block within a ROA, as described in Section 4.1. The following URL would be used to find information for the most-specific ROA matching the "192.0.2.0/25" CIDR:

https://example.net/rdap/rpki1_roa/192.0.2.0/25

Similarly, for the "2001:db8::/64" CIDR:

https://example.net/rdap/rpki1_roa/2001%3Adb8%3A%3A/64

A lookup query for ROA information by digest is specified using this form:

rpki1_roa/BBBB/CCCC

BBBB is a string representing the "digestAlgorithm" property, and CCCC is a string representing the "digest" property, as described in Section 3. The following URL would be used to find information for a ROA matching the "7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069" SHA-256 digest:

https://example.net/rdap/rpki1_roa/SHA-256/7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069

In the "links" array of a ROA object, the context URI ("value" member) of each link should be the lookup URL by its handle, and if that’s not available, then the lookup URL by one of its IP addresses.

4.3. Search

The resource type path segment for searching ROA objects is "rpki1_roas".

The following search path segments are defined for ROA objects:

Syntax: rpki1_roas?name=<name search pattern>

Syntax: rpki1_roas?originAutnum=<autonomous system number>

Searches for ROA information by name are specified using this form:

rpki1_roas?name=XXXX

XXXX is a search pattern per Section 4.1 of [RFC9082], representing the "name" property of a ROA, as described in Section 4.1. The following URL would be used to find information for ROA names matching the "ROA-*" pattern:

https://example.net/rdap/rpki1_roas?name=ROA-*

Searches for ROA information by origin autonomous system number are specified using this form:

rpki1_roas?originAutnum=BBBB

BBBB is an autonomous system number representing the "originAutnum" property of a ROA, as described in Section 4.1. The following URL would be used to find information for ROAs with origin autonomous system number 65536:

https://example.net/rdap/rpki1_roas?originAutnum=65536

4.3.1. Search Results

The ROA search results are returned in the "rpki1_roaSearchResults" member, which is an array of ROA objects (Section 4.1).

Here is an elided example of the search results when finding information for ROAs with origin autonomous system number 65536:

```
{
  "rdapConformance":
  [
    "rdap_level_0",
    "rpki1",
    ...
```

```
  ],
  ...
  "rpki1_roaSearchResults":
  [
    {
      "objectClassName": "rpki1_roa",
      "handle": "XXXX",
      "name": "ROA-1",
      "digests":
      [
        {
          "digest": "01234567...89abcdef",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "roaIps":
      [
        {
          "ip": "2001:db8::/48",
          "maxLength": 64
        },
        ...
      ],
      "originAutnum": 65536,
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/XXXX.roa",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
```

```
      [
        {
          "value": "https://example.net/rdap/rpki1_roa/XXXX",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_roa/XXXX",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_roa/XXXX",
          "rel": "related",
          "href": "https://example.net/rdap/ip/2001:db8::/48",
          "type": "application/rdap+json"
        },
        ...
      ]
    },
    ...
  ]
}
```

4.4. Reverse Search

Per Section 2 of [RFC9536], if a server receives a reverse search query with a searchable resource type of "ips" (Section 5 of [I-D.ietf-regext-rdap-rir-search]), a related resource type of "rpki1_roa", and a ROA property of "originAutnum" or "ip", then the reverse search will be performed on the IP network objects from its data store.

Section 9.2 and Section 9.3 include registration of entries for IP network searches in the RDAP Reverse Search and RDAP Reverse Search Mapping IANA registries when the related resource type is "rpki1_roa".

4.5. Relationship with IP Network Object Class

An IP network object can span multiple ROA objects, and vice-versa. Their relationship is affected by IP address transfers and splits in a registry. It would be useful to show all the ROA objects associated with an IP network object. To that end, this extension adds a new "rpki1_roas" member to the IP Network object class (Section 5.4 of [RFC9083]):

* "rpki1_roas" -- an array of ROA objects (Section 4.1) associated with an IP network object; if the array is too large, the server MAY truncate it, per Section 9 of [RFC9083]

Here is an elided example for an IP network object with ROAs:

```
{
  "objectClassName": "ip network",
  "handle": "ZZZZ-RIR",
  "startAddress": "2001:db8::",
  "endAddress": "2001:db8:ffff:ffff:ffff:ffff:ffff:ffff",
  "ipVersion": "v6",
  ...
  "rpki1_roas":
  [
    {
      "objectClassName": "rpki1_roa",
      "handle": "XXXX",
      "name": "ROA-1",
      "digests":
      [
        {
          "digest": "01234567...89abcdef",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "roaIps":
      [
        {
          "ip": "2001:db8::/48",
          "maxLength": 64
        },
        ...
      ],
      "originAutnum": 65536,
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/XXXX.roa",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
```

```
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
      [
        {
          "value": "https://example.net/rdap/rpki1_roa/XXXX",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_roa/XXXX",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_roa/XXXX",
          "rel": "related",
          "href": "https://example.net/rdap/ip/2001:db8::/48",
          "type": "application/rdap+json"
        },
        ...
      ]
    },
    {
      "objectClassName": "rpki1_roa",
      "handle": "YYYY",
      "name": "ROA-2",
      "digests":
      [
        {
          "digest": "12345678...9abcdef0",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "roaIps":
      [
        {
          "ip": "2001:db8:1::/48",
          "maxLength": 64
        },
        ...
      ],
      "originAutnum": 65537,
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/YYYY.roa",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
```

```
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
      [
        {
          "value": "https://example.net/rdap/rpki1_roa/YYYY",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_roa/YYYY",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_roa/YYYY",
          "rel": "related",
          "href": "https://example.net/rdap/ip/2001:db8:1::/48",
          "type": "application/rdap+json"
        },
        ...
      ]
    },
    ...
  ]
}
```

5. Autonomous System Provider Authorization

5.1. Object Class

The Autonomous System Provider Authorization (ASPA) object class can contain the following members:

* "objectClassName" -- the string "rpki1_aspa"
* "handle" -- see Section 3
* "name" -- see Section 3
* "digests" -- see Section 3

* "customerAutnum" -- an unsigned 32-bit integer representing an autonomous system number of the registration holder (called customer per ASPA terminology) (Section 3 of [I-D.ietf-sidrops-aspa-profile])
* "providerAutnums" -- an array of unsigned 32-bit integers, each representing the autonomous system number of an AS that is authorized as a provider (Section 3 of [I-D.ietf-sidrops-aspa-profile])
* "notValidBefore" -- see Section 3
* "notValidAfter" -- see Section 3
* "publicationUri" -- see Section 3
* "notificationUri" -- see Section 3
* "entities" -- see Section 3
* "rpkiType" -- see Section 3
* "events" -- see Section 4.5 of [RFC9083]
* "links" -- "self" link, and "related" links for autonomous system number and IRR (when defined) objects (Section 4.2 of [RFC9083])
* "remarks" -- see Section 4.3 of [RFC9083]

Here is an elided example of an ASPA object:

```
{
  "objectClassName": "rpki1_aspa",
  "handle": "XXXX",
  "name": "ASPA-1",
  "digests":
  [
    {
      "digest": "23456789...abcdef01",
      "digestAlgorithm": "SHA-256",
    },
    ...
  ],
  "customerAutnum": 65536,
  "providerAutnums":
  [
    65542,
    ...
  ],
  "notValidBefore": "2024-04-27T23:59:59Z",
  "notValidAfter": "2025-04-27T23:59:59Z",
  "publicationUri": "rsync://example.net/path/to/XXXX.aspa",
  "notificationUri": "https://example.net/path/to/notification.xml",
  "entities":
  [
    {
      "objectClassName": "entity",
      "handle": "XYZ-RIR",
```

```
        ...
      },
      ...
    ],
    "rpkiType": "hosted",
    "events":
    [
      {
        "eventAction": "registration",
        "eventDate": "2024-01-01T23:59:59Z"
      },
      ...
    ],
    "links":
    [
      {
        "value": "https://example.net/rdap/rpki1_aspa/XXXX",
        "rel": "self",
        "href": "https://example.net/rdap/rpki1_aspa/XXXX",
        "type": "application/rdap+json"
      },
      {
        "value": "https://example.net/rdap/rpki1_aspa/XXXX",
        "rel": "related",
        "href": "https://example.net/rdap/autnum/65536",
        "type": "application/rdap+json"
      },
      ...
    ],
    "remarks":
    [
      {
        "description": [ "ASPA" ]
      }
    ]
  }
```

5.2. Lookup

The resource type path segment for exact match lookup of an ASPA object is "rpki1_aspa".

The following lookup path segments are defined for an ASPA object:

Syntax: rpki1_aspa/<handle>

Syntax: rpki1_aspa/<customer autonomous system number>

Syntax: rpki1_aspa/<digest algorithm>/<digest>

A lookup query for ASPA information by handle is specified using this form:

rpki1_aspa/XXXX

XXXX is a string representing the "handle" property of an ASPA, as described in Section 5.1. The following URL would be used to find information for an ASPA that exactly matches the "47ab80ed8693f25d0187d93a07db4484" handle:

https://example.net/rdap/rpki1_aspa/47ab80ed8693f25d0187d93a07db4484

A lookup query for ASPA information by customer autonomous system number is specified using this form:

rpki1_aspa/YYYY

YYYY is an autonomous system number representing the "customerAutnum" property of an ASPA, as described in Section 5.1. The following URL would be used to find information for an ASPA with customer autonomous system number 65536:

https://example.net/rdap/rpki1_aspa/65536

A lookup query for ASPA information by digest is specified using this form:

rpki1_aspa/BBBB/CCCC

BBBB is a string representing the "digestAlgorithm" property, and CCCC is a string representing the "digest" property, as described in Section 3. The following URL would be used to find information for an ASPA matching the "f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d90697" SHA-256 digest:

https://example.net/rdap/rpki1_aspa/SHA-256/f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d90697

In the "links" array of an ASPA object, the context URI ("value" member) of each link should be the lookup URL by its handle, and if that’s not available, then the lookup URL by its customer autonomous system number.

5.3. Search

The resource type path segment for searching ASPA objects is "rpki1_aspas".

The following search path segments are defined for ASPA objects:

Syntax: rpki1_aspas?name=<name search pattern>

Syntax: rpki1_aspas?providerAutnum=<provider autonomous system number>

Searches for ASPA information by name are specified using this form:

rpki1_aspas?name=XXXX

XXXX is a search pattern per Section 4.1 of [RFC9082], representing the "name" property of an ASPA, as described in Section 5.1. The following URL would be used to find information for ASPA names matching the "ASPA-*" pattern:

https://example.net/rdap/rpki1_aspas?name=ASPA-*

Searches for ASPA information by provider autonomous system number are specified using this form:

rpki1_aspas?providerAutnum=YYYY

YYYY is an autonomous system number within the "providerAutnums" property of an ASPA, as described in Section 5.1. The following URL would be used to find information for ASPAs with provider autonomous system number 65542:

https://example.net/rdap/rpki1_aspas?providerAutnum=65542

5.3.1. Search Results

The ASPA search results are returned in the "rpki1_aspaSearchResults" member, which is an array of ASPA objects (Section 5.1).

Here is an elided example of the search results when finding information for ASPAs with provider autonomous system number 65542:

```
{
  "rdapConformance":
  [
    "rdap_level_0",
    "rpki1",
    ...
  ],
  ...
  "rpki1_aspaSearchResults":
  [
    {
      "objectClassName": "rpki1_aspa",
      "handle": "XXXX",
      "name": "ASPA-1",
      "digests":
      [
        {
          "digest": "23456789...abcdef01",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "customerAutnum": 65536,
      "providerAutnums":
      [
        65542,
        ...
      ],
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/XXXX.aspa",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
```

```
        ...
      ],
      "links":
      [
        {
          "value": "https://example.net/rdap/rpki1_aspa/XXXX",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_aspa/XXXX",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_aspa/XXXX",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65536",
          "type": "application/rdap+json"
        },
        ...
      ],
      ...
    },
    ...
  ]
}
```

5.4. Reverse Search

Per Section 2 of [RFC9536], if a server receives a reverse search query with a searchable resource type of "autnums" (Section 5 of [I-D.ietf-regext-rdap-rir-search]), a related resource type of "rpki1_aspa", and an ASPA property of "customerAutnum" or "providerAutnum", then the reverse search will be performed on the autonomous system number objects from its data store.

Section 9.2 and Section 9.3 include registration of entries for autonomous system number searches in the RDAP Reverse Search and RDAP Reverse Search Mapping IANA registries when the related resource type is "rpki1_aspa".

5.5. Relationship with Autonomous System Number Object Class

An autonomous system number object for an ASN range can span multiple ASPA objects. However, an ASPA object can only be linked to a single autonomous system number object. It would be useful to show all the ASPA objects associated with an autonomous system number object. To that end, this extension adds a new "rpki1_aspas" member to the Autonomous System Number object class (Section 5.5 of [RFC9083]):

* "rpki1_aspas" -- an array of ASPA objects (Section 5.1) with "customerAutnum" values from within the autonomous system number range of an autonomous system number object; if the array is too large, the server MAY truncate it, per Section 9 of [RFC9083]

Here is an elided example for an autonomous system number object with ASPAs:

```
{
  "objectClassName": "autnum",
  "handle": "ZZZZ-RIR",
  "startAutnum": 65536,
  "endAutnum": 65541,
  ...
  "rpki1_aspas":
  [
    {
      "objectClassName": "rpki1_aspa",
      "handle": "XXXX",
      "name": "ASPA-1",
      "digests":
      [
        {
          "digest": "23456789...abcdef01",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "customerAutnum": 65536,
      "providerAutnums":
      [
        65542,
        ...
      ],
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/XXXX.aspa",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
```

```
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
      [
        {
          "value": "https://example.net/rdap/rpki1_aspa/XXXX",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_aspa/XXXX",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_aspa/XXXX",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65536",
          "type": "application/rdap+json"
        },
        ...
      ],
      ...
    },
    {
      "objectClassName": "rpki1_aspa",
      "handle": "YYYY",
      "name": "ASPA-2",
      "digests":
      [
        {
          "digest": "3456789a...bcdef012",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "customerAutnum": 65537,
      "providerAutnums":
      [
        65543,
        ...
      ],
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/YYYY.aspa",
      "notificationUri": "https://example.net/path/to/notification.xml",
```

```
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
      [
        {
          "value": "https://example.net/rdap/rpki1_aspa/YYYY",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_aspa/YYYY",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_aspa/YYYY",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65537",
          "type": "application/rdap+json"
        },
        ...
      ],
      ...
    },
    ...
  ]
}
```

6. X.509 Resource Certificate

6.1. Object Class

The X.509 resource certificate object class can contain the following members:

* "objectClassName" -- the string "rpki1_x509ResourceCert"

* "handle" -- see Section 3
* "digests" -- see Section 3
* "serialNumber" -- a string representing the unique identifier for the certificate (Section 4.2 of [RFC6487])
* "issuer" -- a string representing the CA that issued the certificate (Section 4.4 of [RFC6487])
* "signatureAlgorithm" -- a string representing the algorithm used by the CA to sign the certificate (Section 4.3 of [RFC6487])
* "subject" -- a string representing the identity of the subject the certificate is issued to (Section 4.5 of [RFC6487])
* "subjectPublicKeyInfo" -- an object representing the subject's public key information (Section 4.7 of [RFC6487]), with the following members:
  - "publicKeyAlgorithm" -- a string representing the algorithm for the public key
  - "publicKey" -- a string representation of the public key
* "subjectKeyIdentifier" -- a string, typically Base64-encoded, representing the unique identifier for the subject's public key (Section 4.8.2 of [RFC6487])
* "ips" -- an array of strings, each representing an IPv4 or IPv6 CIDR address block with the "<CIDR prefix>/<CIDR length>" format (Section 4.8.10 of [RFC6487])
* "autnums" -- an array of unsigned 32-bit integers, each representing an autonomous system number (Section 4.8.11 of [RFC6487])
* "notValidBefore" -- see Section 3
* "notValidAfter" -- see Section 3
* "publicationUri" -- see Section 3
* "notificationUri" -- see Section 3
* "entities" -- see Section 3
* "rpkiType" -- see Section 3
* "events" -- see Section 4.5 of [RFC9083]
* "links" -- "self" link, "related" links for IP network and/or autonomous system number objects (Section 4.2 of [RFC9083]), and "rdap-help" link (see Section 7)
* "remarks" -- see Section 4.3 of [RFC9083]

The following types of certificates can be represented using this object class:

* a CA certificate (Section 2.2 of [RFC6480]) that a registry issues to an organization (the subject) for its allocated IP addresses and/or autonomous system numbers, authorizing the organization CA to issue end-entity certificates (Section 2.3 of [RFC6480])

* a BGPSec router certificate ([RFC8209]) where an ASN(s) holder cryptographically asserts that a router (the subject) holding the corresponding private key is authorized to emit secure route advertisements on behalf of the AS(es) specified in the certificate

Here is an elided example of an X.509 resource certificate object for a CA certificate:


```
{
  "objectClassName": "rpki1_x509ResourceCert",
  "handle": "ABCD",
  "digests":
  [
    {
      "digest": "456789ab...cdef0123",
      "digestAlgorithm": "SHA-256",
    },
    ...
  ],
  "serialNumber": "1234",
  "issuer": "CN=RIR-CA",
  "signatureAlgorithm": "ecdsa-with-SHA256",
  "subject": "CN=ISP-CA",
  "subjectPublicKeyInfo":
  {
    "publicKeyAlgorithm": "id-ecPublicKey",
    "publicKey": "..."
  },
  "subjectKeyIdentifier": "hOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=",
  "ips":
  [
    "192.0.2.0/24",
    "2001:db8::/48"
  ],
  "autnums":
  [
    65536,
    65537
  ],
  "notValidBefore": "2024-04-27T23:59:59Z",
  "notValidAfter": "2025-04-27T23:59:59Z",
  "publicationUri": "rsync://example.net/path/to/ABCD.cer",
  "notificationUri": "https://example.net/path/to/notification.xml",
  "entities":
  [
    {
      "objectClassName": "entity",
```

```
      "handle": "XYZ-RIR",
      ...
    },
    ...
  ],
  "rpkiType": "hosted",
  "events":
  [
    {
      "eventAction": "registration",
      "eventDate": "2024-01-01T23:59:59Z"
    },
    ...
  ],
  "links":
  [
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
      "rel": "self",
      "href": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
      "rel": "related",
      "href": "https://example.net/rdap/ip/192.0.2.0/24",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
      "rel": "related",
      "href": "https://example.net/rdap/ip/2001:db8::/48",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
      "rel": "related",
      "href": "https://example.net/rdap/autnum/65536",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
      "rel": "related",
      "href": "https://example.net/rdap/autnum/65537",
      "type": "application/rdap+json"
    },
    ...
  ],
```

```
  "remarks":
  [
    {
      "description": [ "CA certificate" ]
    }
  ]
}
```

Here is an elided example of an X.509 resource certificate object for a BGPSec router certificate:

```
{
  "objectClassName": "rpki1_x509ResourceCert",
  "handle": "EFGH",
  "digests":
  [
    {
      "digest": "56789abc...def01234",
      "digestAlgorithm": "SHA-256",
    },
    ...
  ],
  "serialNumber": "5678",
  "issuer": "CN=ISP-CA",
  "signatureAlgorithm": "ecdsa-with-SHA256",
  "subject": "CN=ISP-BGPSEC-ROUTER",
  "subjectPublicKeyInfo":
  {
    "publicKeyAlgorithm": "id-ecPublicKey",
    "publicKey": "..."
  },
  "subjectKeyIdentifier": "iOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=",
  "autnums":
  [
    65536,
    65537
  ],
  "notValidBefore": "2024-04-27T23:59:59Z",
  "notValidAfter": "2025-04-27T23:59:59Z",
  "publicationUri": "rsync://example.net/path/to/EFGH.cer",
  "notificationUri": "https://example.net/path/to/notification.xml",
  "entities":
  [
    {
      "objectClassName": "entity",
      "handle": "XYZ-RIR",
      ...
    },
```

```
    ...
  ],
  "rpkiType": "hosted",
  "events":
  [
    {
      "eventAction": "registration",
      "eventDate": "2024-01-01T23:59:59Z"
    },
    ...
  ],
  "links":
  [
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
      "rel": "self",
      "href": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
      "rel": "related",
      "href": "https://example.net/rdap/autnum/65536",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
      "rel": "related",
      "href": "https://example.net/rdap/autnum/65537",
      "type": "application/rdap+json"
    },
    ...
  ],
  "remarks":
  [
    {
      "description": [ "BGPSec router certificate" ]
    }
  ]
}
```

6.2. Lookup

The resource type path segment for exact match lookup of an X.509 resource certificate object is "rpki1_x509ResourceCert".

The following lookup path segments are defined for an X.509 resource certificate object:

Syntax: rpki1_x509ResourceCert/<handle>

Syntax: rpki1_x509ResourceCert/<digest algorithm>/<digest>

A lookup query for X.509 resource certificate information by handle is specified using this form:

rpki1_x509ResourceCert/XXXX

XXXX is a string representing the "handle" property of an X.509 resource certificate, as described in Section 6.1. The following URL would be used to find information for an X.509 resource certificate that exactly matches the "ABCD" handle:

https://example.net/rdap/rpki1_x509ResourceCert/ABCD

A lookup query for X.509 resource certificate information by digest is specified using this form:

rpki1_x509ResourceCert/BBBB/CCCC

BBBB is a string representing the "digestAlgorithm" property, and CCCC is a string representing the "digest" property, as described in Section 3. The following URL would be used to find information for an X.509 resource certificate matching the "83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d90697f" SHA-256 digest:

https://example.net/rdap/rpki1_x509ResourceCert/SHA-256/83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d90697f

6.3. Search

The resource type path segment for searching X.509 resource certificate objects is "rpki1_x509ResourceCerts".

The following search path segments are defined for X.509 resource certificate objects:

Syntax: rpki1_x509ResourceCerts?handle=<handle search pattern>

Syntax: rpki1_x509ResourceCerts?issuer=<issuer search pattern>

Syntax: rpki1_x509ResourceCerts?subject=<subject search pattern>

Syntax: rpki1_x509ResourceCerts?subjectKeyIdentifier=<subject key identifier>

Syntax: rpki1_x509ResourceCerts?ip=<IP address>

Syntax: rpki1_x509ResourceCerts?cidr=<CIDR>

Syntax: rpki1_x509ResourceCerts?autnum=<autonomous system number>

Searches for X.509 resource certificate information by handle are specified using this form:

rpki1_x509ResourceCerts?handle=XXXX

XXXX is a search pattern per Section 4.1 of [RFC9082], representing the "handle" property of an X.509 resource certificate object, as described in Section 6.1. The following URL would be used to find information for X.509 resource certificate objects with handle matching the "EFG*" pattern:

https://example.net/rdap/rpki1_x509ResourceCerts?handle=EFG*

Searches for X.509 resource certificate information by certificate issuer are specified using this form:

rpki1_x509ResourceCerts?issuer=YYYY

YYYY is a search pattern per Section 4.1 of [RFC9082], representing the "issuer" property of an X.509 resource certificate object, as described in Section 6.1. The following URL would be used to find information for X.509 resource certificate objects with issuer matching the "CN=ISP-*" pattern:

https://example.net/rdap/rpki1_x509ResourceCerts?issuer=CN%3DISP-*

Searches for X.509 resource certificate information by certificate subject are specified using this form:

rpki1_x509ResourceCerts?subject=ZZZZ

ZZZZ is a search pattern per Section 4.1 of [RFC9082], representing the "subject" property of an X.509 resource certificate object, as described in Section 6.1. The following URL would be used to find information for X.509 resource certificate objects with subject matching the "CN=ISP-BGPSEC-ROUTE*" pattern:

https://example.net/rdap/rpki1_x509ResourceCerts?subject=CN%3DISP-BGPSEC-ROUTE*

Searches for X.509 resource certificate information by subject key identifier are specified using this form:

rpki1_x509ResourceCerts?subjectKeyIdentifier=BBBB

BBBB is a string representing the "subjectKeyIdentifier" property of an X.509 resource certificate object, as described in Section 6.1. The following URL would be used to find an X.509 resource certificate object with subject key identifier matching the "iOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=" string:

https://example.net/rdap/rpki1_x509ResourceCerts?subjectKeyIdentifier=iOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=

Searches for X.509 resource certificate information by an IP address are specified using this form:

rpki1_x509ResourceCerts?ip=CCCC

CCCC is a string representing an IPv4 or IPv6 address. The following URL would be used to find information for X.509 resource certificate objects with the "ips" member encompassing the "192.0.2.0" IP address:

https://example.net/rdap/rpki1_x509ResourceCerts?ip=192.0.2.0

Similarly, for the "2001:db8::" IP address:

https://example.net/rdap/rpki1_x509ResourceCerts?ip=2001%3Adb8%3A%3A

Searches for X.509 resource certificate information by a CIDR are specified using this form:

rpki1_x509ResourceCerts?cidr=CCCC/DDDD

CCCC/DDDD is a string representing an IPv4 or IPv6 CIDR, with CCCC as the CIDR prefix and DDDD as the CIDR length. The following URL would be used to find information for X.509 resource certificate objects with the "ips" member encompassing the "192.0.2.0/25" CIDR:

https://example.net/rdap/rpki1_x509ResourceCerts?cidr=192.0.2.0%2F25

Similarly, for the "2001:db8::/64" CIDR:

https://example.net/rdap/rpki1_x509ResourceCerts?cidr=2001%3Adb8%3A%3A%2F64

Searches for X.509 resource certificate information by an autonomous system number are specified using this form:

rpki1_x509ResourceCerts?autnum=EEEE

EEEE is an autonomous system number within the "autnums" property of an X.509 resource certificate object, as described in Section 6.1. The following URL would be used to find information for X.509 resource certificate objects with the "autnums" member including autonomous system number 65536:

https://example.net/rdap/rpki1_x509ResourceCerts?autnum=65536

6.3.1. Search Results

The X.509 resource certificate search results are returned in the "rpki1_x509ResourceCertSearchResults" member, which is an array of X.509 resource certificate objects (Section 6.1).

Here is an elided example of the search results when finding information for X.509 resource certificate objects with issuer matching the "CN=ISP-*" pattern:

```
{
  "rdapConformance":
  [
    "rdap_level_0",
    "rpki1",
    ...
  ],
  ...
  "rpki1_x509ResourceCertSearchResults":
  [
    {
      "objectClassName": "rpki1_x509ResourceCert",
      "handle": "EFGH",
      "digests":
      [
        {
          "digest": "56789abc...def01234",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "serialNumber": "5678",
      "issuer": "CN=ISP-CA",
      "signatureAlgorithm": "ecdsa-with-SHA256",
      "subject": "CN=ISP-BGPSEC-ROUTER",
      "subjectPublicKeyInfo":
      {
        "publicKeyAlgorithm": "id-ecPublicKey",
        "publicKey": "..."
      },
```

```
      "subjectKeyIdentifier": "iOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=",
      "autnums":
      [
        65536,
        65537
      ],
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/ABCD.cer",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
      [
        {
          "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65536",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65537",
          "type": "application/rdap+json"
        },
```

```
        ...
      ],
      ...
    },
    ...
  ]
}
```

6.4. Reverse Search

Per Section 2 of [RFC9536], if a server receives a reverse search query with a searchable resource type of "ips" (Section 5 of [I-D.ietf-regext-rdap-rir-search]), a related resource type of "rpki1_x509ResourceCert", and an X.509 Resource Certificate property of "handle", then the reverse search will be performed on the IP network objects from its data store.

Similarly, if a server receives a reverse search query with a searchable resource type of "autnums", a related resource type of "rpki1_x509ResourceCert", and an X.509 Resource Certificate property of "handle", then the reverse search will be performed on the autonomous system number objects.

Section 9.2 and Section 9.3 include registration of entries for IP network and autonomous system number searches in the RDAP Reverse Search and RDAP Reverse Search Mapping IANA registries when the related resource type is "rpki1_x509ResourceCert".

6.5. Relationship with Other Object Classes

It would be useful to show all the X.509 resource certificates associated with an object of another RDAP class; in particular, with an IP network object, an autonomous system number object, or an entity (organization) object. To that end, this extension adds a new "rpki1_x509ResourceCerts" member to the IP Network (Section 5.4 of [RFC9083]), Autonomous System Number (Section 5.5 of [RFC9083]), and Entity (Section 5.1 of [RFC9083]) object classes:

* "rpki1_x509ResourceCerts" -- an array of X.509 resource certificate objects (Section 6.1) for the IP address range in an IP network object, the autonomous system number range in an autonomous system number object, or an entity (organization) object; if the array is too large, the server MAY truncate it, per Section 9 of [RFC9083]

Here is an elided example for an entity (organization) object with X.509 resource certificates:

```
{
  "objectClassName" : "entity",
  "handle":"XYZ-RIR",
  ...
  "rpki1_x509ResourceCerts":
  [
    {
      "objectClassName": "rpki1_x509ResourceCert",
      "handle": "ABCD",
      "digests":
      [
        {
          "digest": "456789ab...cdef0123",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "serialNumber": "1234",
      "issuer": "CN=RIR-CA",
      "signatureAlgorithm": "ecdsa-with-SHA256",
      "subject": "CN=ISP-CA",
      "subjectPublicKeyInfo":
      {
        "publicKeyAlgorithm": "id-ecPublicKey",
        "publicKey": "..."
      },
      "subjectKeyIdentifier": "hOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=",
      "ips":
      [
        "192.0.2.0/24",
        "2001:db8::/48"
      ],
      "autnums":
      [
        65536,
        65537
      ],
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/ABCD.cer",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
```

```
      ...
    ],
    "rpkiType": "hosted",
    "events":
    [
      {
        "eventAction": "registration",
        "eventDate": "2024-01-01T23:59:59Z"
      },
      ...
    ],
    "links":
    [
      {
        "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
        "rel": "self",
        "href": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
        "type": "application/rdap+json"
      },
      {
        "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
        "rel": "related",
        "href": "https://example.net/rdap/ip/192.0.2.0/24",
        "type": "application/rdap+json"
      },
      {
        "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
        "rel": "related",
        "href": "https://example.net/rdap/ip/2001:db8::/48",
        "type": "application/rdap+json"
      },
      {
        "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
        "rel": "related",
        "href": "https://example.net/rdap/autnum/65536",
        "type": "application/rdap+json"
      },
      {
        "value": "https://example.net/rdap/rpki1_x509ResourceCert/ABCD",
        "rel": "related",
        "href": "https://example.net/rdap/autnum/65537",
        "type": "application/rdap+json"
      },
      ...
    ],
    ...
  },
  {
```

```
      "objectClassName": "rpki1_x509ResourceCert",
      "handle": "EFGH",
      "digests":
      [
        {
          "digest": "56789abc...def01234",
          "digestAlgorithm": "SHA-256",
        },
        ...
      ],
      "serialNumber": "5678",
      "issuer": "CN=ISP-CA",
      "signatureAlgorithm": "ecdsa-with-SHA256",
      "subject": "CN=ISP-BGPSEC-ROUTER",
      "subjectPublicKeyInfo":
      {
        "publicKeyAlgorithm": "id-ecPublicKey",
        "publicKey": "..."
      },
      "subjectKeyIdentifier": "iOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=",
      "autnums":
      [
        65536,
        65537
      ],
      "notValidBefore": "2024-04-27T23:59:59Z",
      "notValidAfter": "2025-04-27T23:59:59Z",
      "publicationUri": "rsync://example.net/path/to/EFGH.cer",
      "notificationUri": "https://example.net/path/to/notification.xml",
      "entities":
      [
        {
          "objectClassName": "entity",
          "handle": "XYZ-RIR",
          ...
        },
        ...
      ],
      "rpkiType": "hosted",
      "events":
      [
        {
          "eventAction": "registration",
          "eventDate": "2024-01-01T23:59:59Z"
        },
        ...
      ],
      "links":
```

```
      [
        {
          "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "rel": "self",
          "href": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65536",
          "type": "application/rdap+json"
        },
        {
          "value": "https://example.net/rdap/rpki1_x509ResourceCert/EFGH",
          "rel": "related",
          "href": "https://example.net/rdap/autnum/65537",
          "type": "application/rdap+json"
        },
        ...
      ],
      ...
    },
    ...
  ]
}
```

7. RDAP for Delegated and Hybrid RPKI

For delegated and hybrid RPKI (see "rpkiTypes" in Section 3), a registry may ask an organization with allocated resources to provide the base URL for its RDAP service. If the RDAP base URL is provided, then in the X.509 resource certificate object (Section 6.1) for that organization’s CA certificate, the registry MUST include a link object (Section 4.2 of [RFC9083]) with the "rel" member set to "rdap-help" and the "href" member set to the help URL (Section 3.1.6 of [RFC9082]) for that RDAP service by appending the "help" path segment to the provided base URL. RDAP clients can then parse the base RDAP URL from the "href" value of such a link object and use the "ips" and "autnums" values from the X.509 resource certificate object to form ROA and ASPA lookup queries for that organization’s RDAP service.

"rdap-help" is a new link relation type for RDAP help data (see Section 9.4), enabling an RDAP client to distinguish the help URL from other related URLs.

Here is an elided example of an X.509 resource certificate object for a delegated CA certificate with an "rdap-help" link object:

```
{
  "objectClassName": "rpki1_x509ResourceCert",
  "handle": "IJKL",
  "digests":
  [
    {
      "digest": "6789abcd...ef012345",
      "digestAlgorithm": "SHA-256",
    },
    ...
  ],
  "serialNumber": "9012",
  "issuer": "CN=RIR-CA",
  "signatureAlgorithm": "ecdsa-with-SHA256",
  "subject": "CN=ISP-DELEGATED-CA",
  "subjectPublicKeyInfo":
  {
    "publicKeyAlgorithm": "id-ecPublicKey",
    "publicKey": "..."
  },
  "subjectKeyIdentifier": "iOcGgxqXDa7mYv78fR+sGBKMtWJqItSLfaIYJDKYi8A=",
  "ips":
  [
    "2001:db8:2::/48"
  ],
  "autnums":
  [
    65538
  ],
  "notValidBefore": "2024-04-27T23:59:59Z",
  "notValidAfter": "2025-04-27T23:59:59Z",
  "publicationUri": "rsync://example.net/path/to/IJKL.cer",
  "notificationUri": "https://example.com/path/to/notification.xml",
  "entities":
  [
    {
      "objectClassName": "entity",
      "handle": "ABC-RIR",
      ...
    },
    ...
  ],
  "rpkiType": "delegated",
  "events":
  [
    {
      "eventAction": "registration",
      "eventDate": "2024-01-01T23:59:59Z"
```

```
    },
    ...
  ],
  "links":
  [
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/IJKL",
      "rel": "self",
      "href": "https://example.net/rdap/rpki1_x509ResourceCert/IJKL",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/IJKL",
      "rel": "related",
      "href": "https://example.net/rdap/ip/2001:db8:2::/48",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/IJKL",
      "rel": "related",
      "href": "https://example.net/rdap/autnum/65538",
      "type": "application/rdap+json"
    },
    {
      "value": "https://example.net/rdap/rpki1_x509ResourceCert/IJKL",
      "rel": "rdap-help",
      "href": "https://example.com/rdap/help",
      "type": "application/rdap+json"
    },
    ...
  ],
  "remarks":
  [
    {
      "description": [ "Delegated CA certificate" ]
    }
  ]
}
```


In this example, note how the authority component (domain) in the "value" URL differs from that in the "href" URL for the "rdap-help" link object, with the former for the registry’s RDAP service and the latter for that organization’s RDAP service.

8. Security Considerations

This document does not introduce any new security considerations past those already discussed in the RDAP protocol specifications ([RFC7481], [RFC9560]).

Section 2.1 explains why this RDAP extension MUST NOT be used to directly influence internet routing.

9. IANA Considerations

9.1. RDAP Extensions Registry

IANA is requested to register the following values in the RDAP Extensions Registry at [RDAP-EXTENSIONS]:

* Extension identifier: rpki1
* Registry operator: Any
* Published specification: This document.
* Contact: IETF iesg@ietf.org (mailto:iesg@ietf.org)
* Intended usage: This extension describes version 1 of a method to access the RPKI registration data through RDAP.

9.2. RDAP Reverse Search Registry

IANA is requested to register the following entries in the RDAP Reverse Search Registry at [RDAP-REVERSE-SEARCH]:

IP network search by the origin autonomous system number of a ROA:

* Searchable Resource Type: ips
* Related Resource Type: rpki1_roa
* Property: originAutnum
* Description: The server supports the IP network search by the origin autonomous system number of an associated RPKI ROA.
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

IP network search by a CIDR address block of a ROA:

* Searchable Resource Type: ips
* Related Resource Type: rpki1_roa
* Property: ip
* Description: The server supports the IP network search by a CIDR address block of an associated RPKI ROA.
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org

* Reference: This document.

Autonomous system number search by the customer autonomous system number of an ASPA:

* Searchable Resource Type: autnums
* Related Resource Type: rpki1_aspa
* Property: customerAutnum
* Description: The server supports the autonomous system number search by the customer autonomous system number of an associated RPKI ASPA.
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

Autonomous system number search by a provider autonomous system number of an ASPA:

* Searchable Resource Type: autnums
* Related Resource Type: rpki1_aspa
* Property: providerAutnum
* Description: The server supports the autonomous system number search by a provider autonomous system number of an associated RPKI ASPA.
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

IP network search by the handle of an X.509 resource certificate:

* Searchable Resource Type: ips
* Related Resource Type: rpki1_x509ResourceCert
* Property: handle
* Description: The server supports the IP network search by the handle of an associated RPKI X.509 resource certificate.
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

Autonomous system number search by the handle of an X.509 resource certificate:

* Searchable Resource Type: autnums
* Related Resource Type: rpki1_x509ResourceCert
* Property: handle
* Description: The server supports the autonomous system number search by the handle of an associated RPKI X.509 resource certificate.

* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

9.3. RDAP Reverse Search Mapping Registry

IANA is requested to register the following entries in the RDAP Reverse Search Mapping Registry at [RDAP-REVERSE-SEARCH-MAPPING]:

IP network search by the origin autonomous system number of a ROA:

* Searchable Resource Type: ips
* Related Resource Type: rpki1_roa
* Property: originAutnum
* Property Path: $.originAutnum
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

IP network search by a CIDR address block of a ROA:

* Searchable Resource Type: ips
* Related Resource Type: rpki1_roa
* Property: ip
* Property Path: $.roaIps[*].ip
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

Autonomous system number search by the customer autonomous system number of an ASPA:

* Searchable Resource Type: autnums
* Related Resource Type: rpki1_aspa
* Property: autnum
* Property Path: $.customerAutnum
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

Autonomous system number search by a provider autonomous system number of an ASPA:

* Searchable Resource Type: autnums
* Related Resource Type: rpki1_aspa
* Property: providerAutnum
* Property Path: $.providerAutnums[*]
* Registrant Name: IETF

* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

IP network search by the handle of an X.509 resource certificate:

* Searchable Resource Type: ips
* Related Resource Type: rpki1_x509ResourceCert
* Property: handle
* Property Path: $.handle
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

Autonomous system number search by the handle of an X.509 resource certificate:

* Searchable Resource Type: autnums
* Related Resource Type: rpki1_x509ResourceCert
* Property: handle
* Property Path: $.handle
* Registrant Name: IETF
* Registrant Contact Information: iesg@ietf.org
* Reference: This document.

9.4. Link Relations Registry

IANA is requested to register the following value in the Link Relations Registry at [LINK-RELATIONS]:

* Relation Name: rdap-help
* Description: Refers to a resource with RDAP help information related to the link context.
* Reference: This document.

10. Acknowledgements

Job Snijders, Ties de Kock, Mark Kosters, Tim Bruijnzeels, Bart Bakker, Frank Hill, Tobias Fiebig, Q Misell, and R端diger Volk from the RPKI community provided valuable feedback for this document.

11. Change History

(Remove this section before publication.)

11.1. Changes from 00 to 01

* Adhering to the guidelines in [I-D.ietf-regext-rdap-extensions].

* Highlighted other RDAP search scenarios that could help with RPKI troubleshooting.
* Be more explicit about what this extension is not. (Feedback from Tobias Fiebig during IETF 122 SIDROPS presentation.)
* How/when to evolve this extension in the future.
* Renamed the "autnum" member as "customerAutnum" in the ASPA RDAP object class to better match the "CustomerASID" field from the ASPA RPKI profile.

11.2. Changes from 01 to 02

* Generate a message digest that covers an entire RPKI object. (Feedback from Job Snijders during IETF 122 SIDROPS presentation.)
* Expound on RDAP for delegated and hybrid RPKI. (Feedback from Q Misell and R端diger Volk during IETF 122 SIDROPS presentation.)

12. References

12.1. Normative References

[I-D.ietf-regext-rdap-extensions]
Newton, A., Singh, J., and T. Harrison, "RDAP Extensions", Work in Progress, Internet-Draft, draft-ietf-regext-rdap-extensions-07, 2 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-regext-rdap-extensions-07>.

[I-D.ietf-regext-rdap-rir-search]
Harrison, T. and J. Singh, "Registration Data Access Protocol (RDAP) Regional Internet Registry (RIR) Search", Work in Progress, Internet-Draft, draft-ietf-regext-rdap-rir-search-19, 4 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-regext-rdap-rir-search-19>.

[I-D.ietf-sidrops-aspa-profile]
Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-19, 6 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-19>.

[RFC1519] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, DOI 10.17487/RFC1519, September 1993, <https://www.rfc-editor.org/info/rfc1519>.

[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>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[RFC5396] Huston, G. and G. Michaelson, "Textual Representation of Autonomous System (AS) Numbers", RFC 5396, DOI 10.17487/RFC5396, December 2008, <https://www.rfc-editor.org/info/rfc5396>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[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>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[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>.

[RFC9082] Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/info/rfc9082>.

[RFC9083] Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/info/rfc9083>.

[RFC9536] Loffredo, M. and M. Martinelli, "Registration Data Access Protocol (RDAP) Reverse Search", RFC 9536, DOI 10.17487/RFC9536, April 2024, <https://www.rfc-editor.org/info/rfc9536>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

12.2. Informative References

[CLOUDFLARE] Cloudflare, "RPKI Portal", <https://rpki.cloudflare.com/>.

[JDR] NLNet Labs, "JDR", <https://blog.nlnetlabs.nl/introducing-jdr/>.

[LINK-RELATIONS] IANA, "Link Relations", <https://www.iana.org/assignments/link-relations/>.

[NIST-RPKI-MONITOR] NIST, "NIST RPKI Monitor", <https://rpki-monitor.antd.nist.gov/>.

[RDAP-EXTENSIONS] IANA, "RDAP Extensions", <https://www.iana.org/assignments/rdap-extensions/>.

[RDAP-GUIDE] Newton, A., "RDAP Guide", <https://rdap.rcode3.com/misc/uses.html>.

[RDAP-REVERSE-SEARCH] IANA, "RDAP Reverse Search", <https://www.iana.org/assignments/rdap-reverse-search/>.

[RDAP-REVERSE-SEARCH-MAPPING] IANA, "RDAP Reverse Search Mapping", <https://www.iana.org/assignments/rdap-reverse-search-mapping/>.

[RFC2622] Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., and M. Terpstra, "Routing Policy Specification Language (RPSL)", RFC 2622, DOI 10.17487/RFC2622, June 1999, <https://www.rfc-editor.org/info/rfc2622>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC7481] Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", STD 95, RFC 7481, DOI 10.17487/RFC7481, March 2015, <https://www.rfc-editor.org/info/rfc7481>.

[RFC9560] Hollenbeck, S., "Federated Authentication for the Registration Data Access Protocol (RDAP) Using OpenID Connect", RFC 9560, DOI 10.17487/RFC9560, April 2024, <https://www.rfc-editor.org/info/rfc9560>.

[ROUTINATOR] NLNet Labs, "Routinator", <https://www.nlnetlabs.nl/projects/routing/routinator/>.

Authors' Addresses

Jasdip Singh
ARIN
Email: jasdips@arin.net

Andy Newton
ICANN
Email: andy@hxr.us