SIDROPS
Internet-Draft
Updates: 8416 (if approved)
Intended status: Standards Track
Expires: 23 November 2025

J. Snijders

B. Cartwright-Cox
Port 179 Ltd

22 May 2025

Simplified Local Internet Number Resource Management (SLURM) with RPKI Autonomous System Provider Authorizations (ASPA)

draft-ietf-sidrops-aspa-slurm-03

Abstract

ISPs may want to establish a local view of exceptions to the Resource Public Key Infrastructure (RPKI) data in the form of local filters or additional attestations. This document defines an addendum to RFC 8416 by specifying a format for local filters and local assertions for Autonomous System Provider Authorizations (ASPA) for use with the RPKI.

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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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

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

This Internet-Draft will expire on 23 November 2025.

Table of Contents

1. Introduction 2
2. SLURM v2 File Overview 2
3. Validation Output Filters for ASPA 3
3.1. Validated ASPA Filters 3
3.2. Locally Added ASPA Assertions 4
4. Example of a SLURM file with ASPA Filters and Assertions . . 5
5. Security Considerations 7
6. IANA Considerations 7
7. Acknowledgements 7
8. Normative References 7
Appendix A. Implementation status - RFC EDITOR: REMOVE BEFORE PUBLICATION 8
Authors' Addresses 8

1. Introduction

ISPs may want to establish a local view of exceptions to the Resource Public Key Infrastructure (RPKI) data in the form of local filters or additional attestations. This document defines an addendum to RFC 8416 by specifying a format for local filters and local assertions for Autonomous System Provider Authorizations (ASPA) for use with the RPKI.

See [RFC8416] for an overview of the SLURM mechanism, specifically Section 3 and Section 4.

2. SLURM v2 File Overview

A SLURM file consists of a single JSON [RFC8259] object containing the following members:

* A "slurmVersion" member that MUST be set to 2, encoded as a number

* A "validationOutputFilters" member whose value is an object. The object MUST contain exactly three members:

  - A "prefixFilters" member, see Section 3.3.1 [RFC8416]

  - A "bgpsecFilters" member, see section 3.3.2 [RFC8416]

  - A "aspaFilters" member, see Section 3.1

* A "locallyAddedAssertions" member whose value is an object. The object MUST contain exactly three members:

  - A "prefixAssertions" member, see Section 3.4.1 [RFC8416]

  - A "bgpsecAssertions" member, see Section 3.4.2 [RFC8416]

  - A "aspaAssertions" member, see Section 3.2

The following JSON structure with JSON members represents a SLURM file that has no filters or assertions:

```
{
  "slurmVersion": 2,
  "validationOutputFilters": {
    "aspaFilters": [],
    "bgpsecFilters": [],
    "prefixFilters": []
  },
  "locallyAddedAssertions": {
    "aspaAssertions": [],
    "bgpsecAssertions": [],
    "prefixAssertions": []
  }
}
```

3. Validation Output Filters for ASPA

3.1. Validated ASPA Filters

The Relying Party (RP) can configure zero or more Validated ASPA Filters ("ASPA Filters" for short). Each ASPA Filter contains a single ’customerAsn’ and optionally a single ’comment’.

* The ’customerAsn’ field contains the AS number of the Customer Autonomous System that is the authorizing entity.

* It is RECOMMENDED that an explanatory comment be included with each ASPA Filter so that it can be shown to users of the RP software.

Any Validated ASPA Payload (VAP) [I-D.ietf-sidrops-aspa-profile] that matches any configured ASPA Filter MUST be removed from the RP's output.

A VAP is considered to match with an ASPA Filter if the following condition applies:

1. The VAP is considered to match if the VAP Customer ASN is equal to the ASPA Filter Customer ASN.

The following example JSON structure represents a "aspaFilters" member with one object as described above:

```
"aspaFilter": [
  {
    "customerAsn": 64496,
    "comment": "Filter out ASPA Payloads which specify AS 64496 as the Customer Asn"
  }
]
```

3.2. Locally Added ASPA Assertions

Each RP is locally configured with a (possibly empty) array of ASPA Assertions. Each ASPA Assertion MUST contain a 'customerAsn' member containing the Customer ASN and a 'providerAsns' array of numbers, reflecting the set of Provider ASNs. It is RECOMMENDED that an explanatory comment be included that may be shown to users of the RP software.

The above is expressed as a value of the "aspaAssertions" member, as an array of zero or more objects. Each object MUST contain one each of all of the following members:

* A "customerAsn" member whose value is a number.

* A "providerAsns" member whose value is an array of numbers.

* An optional "comment" member whose value is a string.

In addition to the constraints described by the formal ASN.1 definition, the contents of the providerAsns field MUST satisfy the following constraints:

* The customerAsn value MUST NOT appear in any ASN in the providerAsns field.

* The elements of providerAsns MUST be ordered in ascending numerical order.

* Each value of ASN MUST be unique (with respect to the other elements of providerAsns).

The following example JSON structure represents a "aspaAssertions" member with one object as described above:

```
"aspaAssertions": [
  {
    "customerAsn": 64496,
    "providerAsns": [64497, 64498],
    "comment": "Locally assert 64497 are 64498 are providers to 64496"
  }
]
```

Note that an "aspaAssertions" member matches the syntax of the ASPA PDU described in Section 5.12 of [I-D.ietf-sidrops-8210bis]. Relying Parties MUST add any "aspaAssertions" member thus found to the set of ASPA PDUs, excluding duplicates, when using version 2 of the RPKI-Router protocol [I-D.ietf-sidrops-8210bis]. An "aspaAssertions" does not act as an implicit filter.

4. Example of a SLURM file with ASPA Filters and Assertions

```
{
  "slurmVersion": 2,
  "validationOutputFilters": {
    "prefixFilters": [
      {
        "prefix": "192.0.2.0/24",
        "comment": "All VRPs encompassed by prefix"
      },
      {
        "asn": 64496,
        "comment": "All VRPs matching ASN"
      },
      {
        "prefix": "198.51.100.0/24",
        "asn": 64497,
        "comment": "All VRPs encompassed by prefix, matching ASN"
      }
    ],
```

```
    "bgpsecFilters": [
      {
        "asn": 64496,
        "comment": "All keys for ASN"
      },
      {
        "SKI": "voibVdC3Nzl9dcSfSFuFj6mK0R8",
        "comment": "Key matching Router SKI"
      },
      {
        "asn": 64497,
        "SKI": "UQ9IXSminbe1FfnEePjtPLeqfSM",
        "comment": "Key for ASN 64497 matching Router SKI"
      }
    ],
    "aspaFilters": [
      {
        "customerAsn": 64496,
        "comment": "ASPAs matching Customer ASN 64496"
      }
    ]
  },
  "locallyAddedAssertions": {
    "prefixAssertions": [
      {
        "asn": 64496,
        "prefix": "198.51.100.0/24",
        "comment": "My other important route"
      },
      {
        "asn": 64496,
        "prefix": "2001:db8::/32",
        "maxPrefixLength": 48,
        "comment": "My other important de-aggregated routes"
      }
    ],
    "bgpsecAssertions": [
      {
        "asn": 64496,
        "comment" : "My known key for my important ASN",
        "SKI": "XUJQ4tgdREjYop786R0p/wdeyeI",
        "routerPublicKey": "MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEgFcjQ/g//LAQerAH2Mpp+Guco
DAGBbhIqD33wNPsXxnAGb+mtZ7XQrVO9DQ6UlAShtig5+QfEKpTtFgiqfiAFQ"
      }
    ],
    "aspaAssertions": [
      {
        "customerAsn": 64496,
        "providerAsns": [64497, 64498],
```

```
        "comment": "Locally assert 64497 and 64498 are providers for 64496"
      }
    ]
  }
}
```

5. Security Considerations

For Security Considerations see Section 6 of [RFC8416].

6. IANA Considerations

This document has no IANA actions.

7. Acknowledgements

The authors would like to thank Tim Bruijnzeels Mike Hollyman, Koen van Hove for their helpful review and contributions to this document.

8. Normative References

[I-D.ietf-sidrops-8210bis]
Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 2", Work in Progress, Internet-Draft, draft-ietf-sidrops-8210bis-20, 22 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-8210bis-20>.

[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>.

[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>.

[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>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[RFC8416] Ma, D., Mandelberg, D., and T. Bruijnzeels, "Simplified Local Internet Number Resource Management with the RPKI (SLURM)", RFC 8416, DOI 10.17487/RFC8416, August 2018, <https://www.rfc-editor.org/info/rfc8416>.

Appendix A. Implementation status - RFC EDITOR: REMOVE BEFORE PUBLICATION

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in RFC 7942. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to RFC 7942, "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

* ... to be filled in!

Authors' Addresses

Job Snijders
Amsterdam
Netherlands
Email: job@sobornost.net

Ben Cartwright-Cox
Port 179 Ltd
London
United Kingdom
Email: ben@benjojo.co.uk