SIDR
Internet-Draft
Intended status: Standards Track
Expires: February 14, 2017

D. Mandelberg
Unaffiliated
D. Ma
ZDNS

August 13, 2016

Simplified Local internet nUmber Resource Management with the RPKI
draft-ietf-sidr-slurm-02

Abstract

The Resource Public Key Infrastructure (RPKI) is a global authorization infrastructure that allows the holder of Internet Number Resources (INRs) to make verifiable statements about those resources. Network operators, e.g., Internet Service Providers (ISPs), can use the RPKI to validate BGP route origination assertions. In the future, ISPs also will be able to use the RPKI to validate the path of a BGP route. However, ISPs may want to establish a local view of the RPKI to control its own network while making use of RPKI data. The mechanisms described in this document provide a simple way to enable INR holders to establish a local, customized view of the RPKI, overriding global RPKI repository data as needed.

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 http://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 February 14, 2017.

Table of Contents

1. Introduction 3
1.1. Terminology 3
2. RPKI RPs with SLURM 4
3. SLURM Mechanisms 4
3.1. Validation Output Filtering 4
3.2. Locally Adding Assertions 5
3.3. Combining Mechanisms 5
4. Format of the SLURM File 5
5. SLURM File Configuration 8
5.1. SLURM File Atomicity 8
5.2. Multiple SLURM Files 8
6. IANA Considerations 9
7. Security considerations 9
8. Acknowledgements 10
9. References 10
9.1. Informative References 10
9.2. Normative References 11
Authors' Addresses 12

1. Introduction

The Resource Public Key Infrastructure (RPKI) is a global authorization infrastructure that allows the holder of Internet Number Resources (INRs) to make verifiable statements about those resources. For example, the holder of a block of IP(v4 or v6) addresses can issue a Route Origination Authorization (ROA) [RFC6482] to authorize an Autonomous System (AS) to originate routes for that block. Internet Service Providers (ISPs) can then use the RPKI to validate BGP routes. (Validation of the origin of a route is described in [RFC6483], and validation of the path of a route is described in [I-D.ietf-sidr-bgpsec-overview].)

However, an RPKI relying party may want to override some of the information expressed via putative TAs and the certificates downloaded from the RPKI repository system. For instances, [RFC6491] recommends the creation of ROAs that would invalidate public routes for reserved and unallocated address space, yet some ISPs might like to use BGP and the RPKI with private address space ([RFC1918], [RFC4193], [RFC6598]) or private AS numbers ([RFC1930], [RFC6996]). Local use of private address space and/or AS numbers is consistent with the RFCs cited above, but such use cannot be verified by the global RPKI. This motivates creation of mechanisms that enable a network operator to publish a variant of RPKI hierarchy (for its own use and that of its customers) at its discretion. Additionally, a network operator might wish to make use of a local override capability to protect routes from adverse actions [I-D.ietf-sidr-adverse-actions], until the results of such actions have been addressed. The mechanisms developed to provide this capability to network operators are hereby called Simplified Local internet nUmber Resource Management with the RPKI (SLURM).

SLURM allows an operator to create a local view of the global RPKI by generating sets of assertions. For Origin Validation [RFC6483], an assertion is a tuple of {IP prefix, prefix length, maximum length, AS number} as used by rpki-rtr version 0 [RFC6810] and version 1

[I-D.ietf-sidr-rpki-rtr-rfc6810-bis]. For BGPsec [I-D.ietf-sidr-bgpsec-overview], an assertion is a tuple of {AS number, subject key identifier, router public key} as used by rpki-rtr version. (For the remainder of this document, these assertions are called Origin Validation assertions and BGPsec assertions, respectively.)

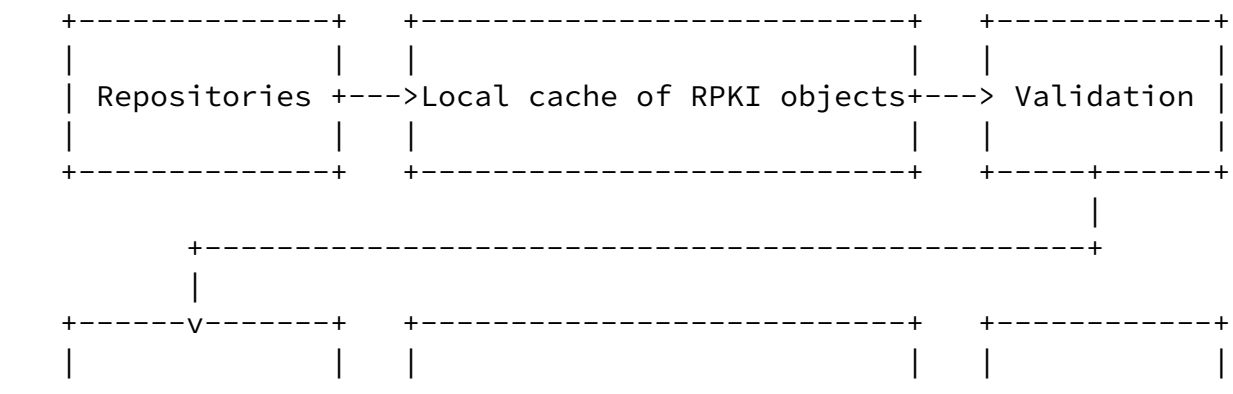
1.1. Terminology

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

2. RPKI RPs with SLURM

SLURM provides a simple way to enable INR holders to establish a local, customized view of the RPKI, by overriding RPKI repository data if needed. To that end, an RP with SLURM filters out (removes from consideration for routing decisions) any assertions in the RPKI that are overridden by local Origin Validation assertions and BGPsec assertions.

In general, the primary output of an RPKI relying party is the data it sends to routers over the rpki-rtr protocol. The rpki-rtr protocol enables routers to query a relying party for all assertions it knows about (Reset Query) or for an update of only the changes in assertions (Serial Query). The mechanisms specified in this document are to be applied to the result set for a Reset Query, and to both the old and new sets that are compared for a Serial Query. Relying party software MAY modify other forms of output in comparable ways, but that is outside the scope of this document.



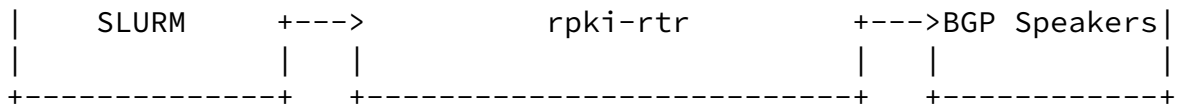


Figure 1: SLURM's Position in the Relying Party Stack

3. SLURM Mechanisms

3.1. Validation Output Filtering

To prevent the global RPKI from affecting routes with locally reserved INRs, a relying party is locally configured with a (possibly empty) list of IP prefixes and/or AS numbers that are used locally. (In general, these IP prefixes and AS numbers will be taken from reserved INR spaces.) Any Origin Validation assertions where the IP prefix is equal to or subsumed by a locally reserved IP prefix, are removed from the relying party's output. (Note that an Origin Validation assertion is not removed due to its AS number matching a

locally reserved AS number.) Any BGPsec assertion where the AS number is equal to a locally reserved AS number is removed from the relying party's output.

3.2. Locally Adding Assertions

Each relying party is locally configured with a (possibly empty) list of assertions. This list is added to the relying party's output.

3.3. Combining Mechanisms

In the envisioned typical use case, a relying party uses both output filtering and locally added assertions. In this case, the resulting assertions MUST be the same as if output filtering were performed before locally adding assertions. I.e., locally added assertions MUST NOT be removed by output filtering.

4. Format of the SLURM File

Relying party software SHOULD support the following configuration format for Validation Output Filtering and Locally Adding Assertions.

The format is defined using the Augmented Backus-Naur Form (ABNF) notation and core rules from [RFC5234] and the rules <IPv4address> and <IPv6address> from Appendix A of [RFC3986]. See Appendix A for an example SLURM file.

A SLURM file, <SLURMFile>, consists of a head and a body. The head identifies the file as a SLURM file, specifies the version of SLURM for which the file was written, and optionally contains other information described below. The body contains the configuration for Validation Output Filtering and Locally Adding Assertions.

```
SLURMFile = head body

head = firstLine *(commentLine / headLine)

body = *(commentLine / bodyLine)

firstLine = %x53.4c.55.52.4d SP "1.0" EOL ; "SLURM 1.0"

commentLine = *WSP [comment] EOL

headLine = *WSP headCommand [ 1*WSP [comment] ] EOL
```



```
bodyLine = *WSP bodyCommand [ 1*WSP [comment] ] EOL

comment = "#" *(VCHAR / WSP)

EOL = CRLF / LF
```

The head may specify a target. If present, the target string identifies the environment in which the SLURM file is intended to be used. The meaning of the target string, if present, is determined by the user. If a target is present, a relying party SHOULD verify that the target is an acceptable value, and reject the SLURM file if the target is not acceptable. For example, the relying party could be configured to accept SLURM files only if they do not specify a target, have a target value of "hostname=rpki.example.com", or have a target value of "as=65536". If more than one target line is present,

all targets must be acceptable to the RP.

```
headCommand = target

target =
   %x74.61.72.67.65.74 1*WSP ; "target"
   1*VCHAR
```

The body contains zero or more configuration lines for Validation Output Filtering and Locally Adding Assertions. Each <del> command specifies an INR to use for Validation Output Filtering. Each <add> command specifies an assertion to use for Locally Adding Assertions.

```
bodyCommand = add / del

add =
   %x61.64.64 1*WSP ; "add"
   addItem

del =
   %x64.65.6c 1*WSP ; "del"
   delItem

addItem = addItemPrefixAS / addItemASKey

; Add a mapping from a prefix and max length to an AS number.
addItemPrefixAS =
   %x6f.72.69.67.69.6e.61.74.69.6f.6e 1*WSP ; "origination"
   IPprefixMaxLen 1*WSP
   ASnum
```



```
; Add a mapping from an AS number to a router public key.
addItemASKey =
   %x62.67.70.73.65.63 1*WSP ; "bgpsec"
   ASnum 1*WSP
   RouterSKI 1*WSP
   RouterPubKey

delItem = delItemPrefix / delItemAS
```

```
; Filter prefix-AS mappings, using the given prefix
delItemPrefix =
   %x6f.72.69.67.69.6e.61.74.69.6f.6e 1*WSP ; "origination"
   IPprefix

; Filter AS-key mappings for the given AS
delItemAS =
   %x62.67.70.73.65.63 1*WSP ; "bgpsec"
   ASnum

IPprefix = IPv4prefix / IPv6prefix

IPprefixMaxLen = IPv4prefixMaxLen / IPv6prefixMaxLen

IPv4prefix = IPv4address "/" 1*2DIGIT
IPv6prefix = IPv6address "/" 1*3DIGIT

; In the following two rules, if the maximum length component
is
; missing, it is treated as equal to the prefix length.
IPv4prefixMaxLen = IPv4prefix ["-" 1*2DIGIT]
IPv6prefixMaxLen = IPv6prefix ["-" 1*3DIGIT]

ASnum = 1*DIGIT

; This is the Base64 [RFC4648] encoding of a router
certificate's
; Subject Key Identifer, as described in
; [I-D.ietf-sidr-bgpsec-pki-profiles] and [RFC6487].  This is
the
; value of the ASN.1 OCTET STRING without the ASN.1 tag or
length
; fields.

RouterSKI = Base64
```



```
; This is the Base64 [RFC4648] encoding of a router public
```

```
key's
; subjectPublicKeyInfo value, as described in
; [I-D.ietf-sidr-bgpsec-algs].  This is the full ASN.1 DER
encoding
; of the subjectPublicKeyInfo, including the ASN.1 tag and
length
; values of the subjectPublicKeyInfo SEQUENCE.
RouterPubKey = Base64

Base64 = 1*(ALPHA / DIGIT / "+" / "/") 0*2"="
```

5. SLURM File Configuration

5.1. SLURM File Atomicity

To ensure local consistency, the effect of SLURM MUST be atomic. That is, the output of the relying party must be either the same as if SLURM file were not used, or it must reflect the entire SLURM configuration. For an example of why this is required, consider the case of two local routes for the same prefix but different origin AS numbers. Both routes are configured with Locally Adding Assertions. If neither addition occurs, then both routes could be in the unknown state [RFC6483]. If both additions occur then both routes would be in the valid state. However, if one addition occurs and the other does not, then one could be invalid while the other is valid.

5.2. Multiple SLURM Files

An implementation MAY support the concurrent use of multiple SLURM files. In this case, the resulting inputs to Validation Output Filtering and Locally Adding Assertions are the respective unions of the inputs from each file. The envisioned typical use case for multiple files is when the files have distinct scopes. For instance, operators of two distinct networks may resort to one RP system to frame routing decisions. As such, they probably deliver SLURM files to this RP respectively. Before an RP configures SLURM files from different source it MUST make sure there is no internal conflict among the INR assertions in these SLURM files. To do so, the RP SHOULD check the entries of SLURM file with regard to overlaps of the INR assertions and report errors to the sources that created these SLURM files in question.

If a problem is detected with the INR assertions in these SLURM files, the RP MUST NOT use them, and SHOULD issue a warning as error report in the following cases:

1. There may be conflicting changes to Origin Validation assertions if there exists an IP address X and distinct SLURM files Y,Z such that X is contained by any prefix in any <addItemPrefixAS> or <delItemPrefix> in file Y and X is contained by any prefix in any <addItemPrefixAS> or <delItemPrefix> in file Z.

2. There may be conflicting changes to BGPsec assertions if there exists an AS number X and distinct SLURM files Y,Z such that X is used in any <addItemASKey> or <delItemAS> in file Y and X is used in any <addItemASKey> or <delItemAS> in file Z.

6. IANA Considerations

None

7. Security considerations

The mechanisms described in this document provide a network operator with additional ways to control make use of RPKI data while preserving autonomy in address space and ASN management. These mechanisms are applied only locally; they do not influence how other network operators interpret RPKI data. Nonetheless, care should be taken in how these mechanisms are employed. Note that it also is possible to use SLURM to (locally) manipulate assertions about non-private INRs, e.g., allocated address space that is globally routed. For example, a SLURM file may be used to override RPKI data that a network operator believes has been corrupted by an adverse action. Network operators who elect to use SLURM in this fashion should use extreme caution.

The goal of the mechanisms described in this document is to enable an RP to create its own view of the RPKI, which is intrinsically a security function. An RP using a SLURM file is trusting the assertions made in that file. Errors in the SLURM file used by an RP can undermine the security offered by the RPKI, to that RP. It could declare as invalid ROAs that would otherwise be valid, and vice versa. As a result, an RP must carefully consider the security implications of the SLURM file being used, especially if the file is provided by a third party.

Additionally, each RP using SLURM MUST ensure the authenticity and

integrity of any SLURM file that it uses. Initially, the SLURM file may be pre-configured out of band, but if the RP updates its SLURM

file over the network, it MUST verify the authenticity and integrity of the updated SLURM file.

8. Acknowledgements

The authors would like to thank Stephen Kent for his guidance and detailed reviews of this document. Thanks go to Wei Wang for the idea behind the target command, to Richard Hansen for his careful reviews and Hui Zou for her editorial assistance.

9. References

9.1. Informative References

[I-D.ietf-sidr-bgpsec-overview]
Lepinski, M. and S. Turner, "An Overview of BGPsec", draft-ietf-sidr-bgpsec-overview-08 (work in progress), June 2016.

[I-D.ietf-sidr-lta-use-cases]
Bush, R., "Use Cases for Localized Versions of the RPKI", draft-ietf-sidr-lta-use-cases-07 (work in progress), July 2016.

[I-D.ietf-sidr-rpki-rtr-rfc6810-bis]
Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", draft-ietf-sidr-rpki-rtr-rfc6810-bis-07 (work in progress), March 2016.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <http://www.rfc-editor.org/info/rfc1918>.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)",

BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <http://www.rfc-editor.org/info/rfc1930>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <http://www.rfc-editor.org/info/rfc4193>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/

RFC6482, February 2012, <http://www.rfc-editor.org/info/rfc6482>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <http://www.rfc-editor.org/info/rfc6483>.

[RFC6491] Manderson, T., Vegoda, L., and S. Kent, "Resource Public Key Infrastructure (RPKI) Objects Issued by IANA", RFC 6491, DOI 10.17487/RFC6491, February 2012, <http://www.rfc-editor.org/info/rfc6491>.

[RFC6598] Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe, C., and M. Azinger, "IANA-Reserved IPv4 Prefix for Shared Address Space", BCP 153, RFC 6598, DOI 10.17487/RFC6598, April 2012, <http://www.rfc-editor.org/info/rfc6598>.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, DOI 10.17487/RFC6810, January 2013, <http://www.rfc-editor.org/info/rfc6810>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <http://www.rfc-editor.org/info/rfc6890>.

[RFC6996] Mitchell, J., "Autonomous System (AS) Reservation for Private Use", BCP 6, RFC 6996, DOI 10.17487/RFC6996, July 2013, <http://www.rfc-editor.org/info/rfc6996>.

[RFC7682] McPherson, D., Amante, S., Osterweil, E., Blunk, L., and D. Mitchell, "Considerations for Internet Routing Registries (IRRs) and Routing Policy Configuration", RFC 7682, DOI 10.17487/RFC7682, December 2015, <http://www.rfc-editor.org/info/rfc7682>.

9.2. Normative References

[I-D.ietf-sidr-bgpsec-algs]
Turner, S., "BGPsec Algorithms, Key Formats, & Signature Formats", draft-ietf-sidr-bgpsec-algs-15 (work in progress), April 2016.

[I-D.ietf-sidr-bgpsec-pki-profiles]
Reynolds, M., Turner, S., and S. Kent, "A Profile for

BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests", draft-ietf-sidr-bgpsec-pki-profiles-18 (work in progress), July 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <http://www.rfc-editor.org/info/rfc4648>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for

X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <http://www.rfc-editor.org/info/rfc6487>.

Authors' Addresses

David Mandelberg
Unaffiliated

Email: david@mandelberg.org

Di Ma
ZDNS
4 South 4th St. Zhongguancun
Haidian, Beijing 100190
China

Email: madi@zdns.cn