Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 20, 2017

T. King
D. Kopp
DE-CIX
A. Lambrianidis
AMS-IX
A. Fenioux
France-IX

January 16, 2017

# Signaling Prefix Origin Validation Results from a Route-Server to Peers
draft-ietf-sidrops-route-server-rpki-light-01

## Abstract

This document defines the usage of the BGP Prefix Origin Validation State Extended Community [I-D.ietf-sidr-origin-validation-signaling] to signal prefix origin validation results from a route-server to its peers. Upon reception of prefix origin validation results peers can use this information in their local routing decision process.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without normative meaning.

## Status of This Memo

## Copyright Notice

## Table of Contents

## 1. Introduction

RPKI-based prefix origin validation [RFC6480] can be a significant operational burden for BGP peers to implement and adopt. In order to boost acceptance and usage of prefix origin validation and ultimately increase the security of the Internet routing system, IXPs may provide RPKI-based prefix origin validation at the route-server [I-D.ietf-idr-ix-bgp-route-server]. The result of this prefix origin validation is signaled to peers by using the BGP Prefix Origin Validation State Extended Community as introduced in [I-D.ietf-sidr-origin-validation-signaling].

Peers receiving the prefix origin validation result from the route-server(s) can use this information in their local routing decision

process for acceptance, rejection, preference, or other traffic engineering purposes of a particular route.

## 2. Signaling Prefix Origin Validation Results from a Route-Server to Peers

The BGP Prefix Origin Validation State Extended Community (as defined in [I-D.ietf-sidr-origin-validation-signaling]) is utilized for signaling prefix origin validation result from a route-server to peers.

[I-D.ietf-sidr-origin-validation-signaling] proposes an encoding of the prefix origin validation result [RFC6811] as follows:

| Value | Meaning |
|---|---|
| 0 | Valid |
| 1 | Not found |
| 2 | Invalid |

Table 1

This encoding is re-used. Route-servers providing RPKI-based prefix origin validation set the validation state according to the prefix origin validation result (see [RFC6811]).

## 3. Operational Recommendations

### 3.1. Local Routing Decision Process

A peer receiving prefix origin validation results from the route-server MAY use the information in its own local routing decision process. The local routing decision process SHOULD apply to the rules as described in section 5 [RFC6811].

A peer receiving a prefix origin validation result from the route-server MAY redistribute this information within its own AS.

### 3.2. Route-Server Receiving the BGP Prefix Origin Validation State Extended Community

An IXP route-server receiving routes from its peers containing the BGP Prefix Origin Validation State Extended Community MUST remove the extended community before the route is re-distributed to its peers. This is required regardless of whether the route-server is executing prefix origin validation or not.

Failure to do so would allow opportunistic peers to advertise routes tagged with arbitrary prefix origin validation results via a route-server, influencing maliciously the decision process of other route-server peers.

### 3.3. Information about Validity of a BGP Prefix Origin Not Available at a Route-Server

In case information about the validity of a BGP prefix origin is not available at the route-server (e.g., error in the ROA cache, CPU overload) the route-server MUST NOT add the BGP Prefix Origin Validation State Extended Community to the route.

### 3.4. Error Handling at Peers

A route sent by a route-server SHOULD only contain none or one BGP Prefix Origin Validation State Extended Community.

A peer receiving a route from a route-server containing more than one BGP Prefix Origin Validation State Extended Community SHOULD only consider the largest value (as described in Table 1) in the validation result field and disregard the other values.  Values larger than two in the validation result field MUST be disregarded.

## 4. IANA Considerations

None.

## 5. Security Considerations

All security considerations described in RFC RFC6811 [RFC6811] fully apply to this document.

Additionally, threat agents polluting ROA cache server(s) run by IXPs can cause significant operational impact, since multiple route-server clients could be affected.  Peers should be vigilant as to the integrity and authenticity of the origin validation results, as they are provided by a third party, namely the IXP hosting both the route-server as well as any ROA cache server(s).

Therefore, a route-server could be misused to spread malicious prefix origin validation results.  However, peers already trust route-server for the collection and redistribution of BGP routing information to other peers.

Similar issues may arise due to inadvertent corruption of the ROA cache database.

To facilitate trust and help with peers establishing appropriate controls in mitigating the risks mentioned above, IXPs SHOULD provide out-of-band means for peers to ensure that the ROA validation process has not been compromised or corrupted.

To countermeasure DDoS attacks, it is common practice to make use of blackholing services (see RFC 7999 [RFC7999]). Peers are using blackholing to drop traffic, typically by announcing a more specific prefix, which is under attack. If no ROA entry exists for the more specific prefix, its validation status would be "Invalid". This might be undesirable, in which case it would be recommended for targeted peers to either create the appropriate ROA entry as necessary, or use adopted classification for such more specific prefixes.

The introduction of a mechanisms described in this document does not pose a new class of attack vectors to the relationship between route-servers and peers.

## 6. References

### 6.1. Normative References

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

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <http://www.rfc-editor.org/info/rfc4360>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <http://www.rfc-editor.org/info/rfc6811>.

[RFC7999] King, T., Dietzel, C., Snijders, J., Doering, G., and G. Hankins, "BLACKHOLE Community", RFC 7999, DOI 10.17487/RFC7999, October 2016, <http://www.rfc-editor.org/info/rfc7999>.

### 6.2. Informative References

[I-D.ietf-idr-ix-bgp-route-server]
Jasinska, E., Hilliard, N., Raszuk, R., and N. Bakker, "Internet Exchange BGP Route Server", draft-ietf-idr-ix-bgp-route-server-12 (work in progress), June 2016.

[I-D.ietf-sidr-origin-validation-signaling]
Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R. Bush, "BGP Prefix Origin Validation State Extended Community", draft-ietf-sidr-origin-validation-signaling-07 (work in progress), November 2015.

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

## Authors' Addresses

Thomas King
DE-CIX Management GmbH
Lichtstrasse 43i
Cologne  50825
DE

Email: thomas.king@de-cix.net

Daniel Kopp
DE-CIX Management GmbH
Lichtstrasse 43i
Cologne  50825
DE

Email: daniel.kopp@de-cix.net

Aristidis Lambrianidis
Amsterdam Internet Exchange
Frederiksplein 42
Amsterdam  1017 XN
NL

Email: aristidis.lambrianidis@ams-ix.net

Arnaud Fenioux
France-IX
88 Avenue Des Ternes
Paris  75017
FR

Email: afenioux@franceix.net