

Workgroup: Network Working Group
Internet-Draft:
draft-ietf-sidrps-aspa-verification-11
Published: 24 October 2022
Intended Status: Standards Track
Expires: 27 April 2023

A	A. Azimov	E. Bogomazov	R. Bush	K. Patel
	uYandex	Qrator Labs	IIJ & Arccus	Arccus
	t			
	h			
	o			
	r			
	s			
	:			
	J. Snijders	K. Sriram		
	Fastly	USA NIST		

BGP AS_PATH Verification Based on Resource Public Key Infrastructure (RPKI) Autonomous System Provider Authorization (ASPA) Objects

Abstract

This document defines the semantics of an Autonomous System Provider Authorization object in the Resource Public Key Infrastructure to verify the Border Gateway Protocol (BGP) AS_PATH attribute of advertised routes. This type of AS_PATH verification is primarily intended for detection and mitigation of route leaks. It also to some degree provides protection against forged-origin prefix hijacks.

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 27 April 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Anomaly Propagation](#)
- [3. Autonomous System Provider Authorization](#)
- [4. Customer-Provider Verification Procedure](#)
- [5. AS_PATH Verification](#)
 - [5.1. Definition of Indices](#)
 - [5.1.1. RS-Client of a Non-Transparent RS](#)
 - [5.2. Algorithm for Upstream Paths](#)
 - [5.3. Algorithm for Downstream Paths](#)
 - [5.4. ASPA Registration Recommendations](#)
 - [5.5. AS_PATH Verification Recommendation](#)
- [6. Mitigation](#)
- [7. Operational Considerations](#)
 - [7.1. Mutual Transit \(Complex Relations\)](#)
 - [7.2. AS Confederations](#)
- [8. Comparison to Other Technologies](#)
 - [8.1. BGPsec](#)
 - [8.2. Peerlock](#)
- [9. IANA Considerations](#)
- [10. Security Considerations](#)
- [11. Acknowledgments](#)
- [12. References](#)
 - [12.1. Normative References](#)
 - [12.2. Informative References](#)
- [Authors' Addresses](#)

1. Introduction

The Border Gateway Protocol (BGP) originally was designed without mechanisms to validate whether the contents of attributes in BGP UPDATES conform to wishes of the involved Internet Number resource holders. As a consequence BGP hijacks and BGP route leaks [[RFC7908](#)] exist. Some existing BGP extensions are able to partially solve these problems; for example, RPKI-based route origin validation (RPKI-ROV) [[RFC6483](#)] [[RFC6811](#)] [[RFC9319](#)] can be used to detect and filter accidental mis-originations, and [[RFC9234](#)] or [[I-D.ietf-grow-route-leak-detection-mitigation](#)] can be used to detect and mitigate accidental route leaks.

This specification focuses on solving a number of real-world operational problems: the automatic detection of route leaks and

improbable BGP paths (including forged-origin BGP hijacks). To achieve this, new AS_PATH verification procedures are described to automatically detect invalid AS_PATHs in announcements that are received from customers, lateral peers (defined in [RFC7908]), transit providers, Route Servers (RSes), and RS-clients. These procedures use a shared database of cryptographically signed customer-to-provider relationships using a new Resource Public Key Infrastructure (RPKI) Signed Object: Autonomous System Provider Authorization (ASPA) [I-D.ietf-sidrops-aspa-profile]. This incrementally deployable technique provides benefits to early adopters in context of limited deployment.

2. Anomaly Propagation

Both route leaks and hijacks have similar effects on ISP operations - they redirect traffic which can result in denial of service (DoS), eavesdropping, increased latency, and packet loss. But the level of risk depends significantly on the extent of propagation of the anomalies. For example, a hijack that is propagated only to customers may cause bottlenecking within a particular ISP's customer cone, but if the anomaly propagates through lateral (i.e., non-transit) peers and transit providers, or reaches global distribution through transit-free networks, then the ill effects will likely be experienced across continents.

The ability to constrain propagation of BGP anomalies to transit providers and lateral peers - without requiring support from the source of the anomaly (which is critical if the source has malicious intent) - should significantly improve the security of global inter-domain routing system.

3. Autonomous System Provider Authorization

As described in [RFC6480], the RPKI is based on a hierarchy of resource certificates that are aligned to the Internet Number Resource allocation structure. Resource certificates are X.509 certificates that conform to the PKIX profile [RFC5280], carrying the extensions for IP addresses and AS identifiers [RFC3779]. A resource certificate is a binding by an issuer of IP address blocks and Autonomous System (AS) numbers to the subject of a certificate, identified by the unique association of the subject's private key with the public key contained in the resource certificate. The RPKI is structured so that each current resource certificate matches a current resource allocation or assignment.

ASPA is a digitally signed object that binds, for a selected AFI, a Set of Provider AS numbers to a Customer AS number (in terms of BGP announcements, not business relationship), and are signed by the holder of the Customer AS. An ASPA attests that a Customer AS holder (CAS) has authorized a Set of Provider ASes (SPAS) to propagate the Customer's IPv4 or IPv6 announcements onward, i.e., to the Provider's upstream providers, lateral peers, or customers. The ASPA object profile is described in [I-D.ietf-sidrops-aspa-profile]. In this document, the notation (AS1, AFI, [AS2,...]) is used to represent the ASPA object for AS1 in the selected AFI. In this example, AS2 and any other ASes listed in the square brackets represent the transit provider ASes.

4. Customer-Provider Verification Procedure

This section describes a procedure for checking if an ordered pair of AS numbers (ASNs), e.g., (AS1, AS2), has the property that AS2 is an attested provider of AS1 per ASPA. This procedure is used in ASPA-based AS_PATH validation as described in [Section 5](#). The procedure takes (AS1, AS2, AFI) as input parameters and returns one of three possible results, which are "Valid", "Invalid", and "Unknown".

A relying party (RP) must have access to a local cache of the complete set of cryptographically valid ASPAs when performing the customer-provider verification procedure.

The following algorithm describes the customer-provider verification procedure for a selected AFI:

1. Retrieve all cryptographically valid ASPAs with the selected AFI that have a customer value of AS1. The union of SPAS from these ASPAs forms the set of authorized providers.
2. If the set of authorized providers is empty, then the procedure exits with an outcome of "Unknown".
3. If AS2 is included in the set of authorized providers, then the procedure exits with an outcome of "Valid".
4. Otherwise, the procedure exits with an outcome of "Invalid".

Since an AS may have different sets of providers for different AFI, accordingly, it may have different SPAS in the corresponding ASPAs. Therefore, the above procedure with the input (AS1, AS2, AFI) may have different outputs for different AFI values.

5. AS_PATH Verification

The procedures described in this document are applicable only to four-octet AS number compatible BGP speakers [[RFC6793](#)]. If such a BGP speaker receives both AS_PATH and AS4_PATH attributes in an UPDATE, then the procedures are applied on the reconstructed AS path (Section 4.2.3 of [[RFC6793](#)]). So, the term AS_PATH is used in this document to refer to the usual AS_PATH [[RFC4271](#)] as well as the reconstructed AS path (the latter in instances when reconstruction is performed).

If an attacker creates a route leak intentionally, they may try to strip their AS from the AS_PATH. To partly guard against that, a check is necessary to match the most recently added AS in the AS_PATH to the BGP neighbor's ASN. This check is expected to be performed as specified in Section 6.3 of [[RFC4271](#)]. If the check fails, then the AS_PATH is considered a Malformed AS_PATH and the UPDATE is considered to be in error (Section 6.3 of [[RFC4271](#)]). It is expected that the case of transparent RS is appropriately taken care of (e.g., by suspending the check). Note that the check fails also when the AS_PATH is empty (zero length) and that is appropriate. These checks are mentioned here because they are commonly a part of commercial BGP implementations and support the AS path validation procedures in this document.

5.1. Definition of Indices

The AS_PATH attribute identifies the autonomous systems through which an UPDATE message has passed. It may contain two types of components: AS_SEQUENCES and AS_SETs, as defined in [[RFC4271](#)]. (Note: The consideration of AS Confederations is discussed in [Section 7.2.](#))

If the AS_PATH contains an AS_SET in any position, then it is marked by the verification algorithm as Invalid. If the AS_PATH does not contain an AS_SET but only AS_SEQUENCE(s), then it is represented for simplicity in the verification algorithm as a sequence of unique AS numbers: AS(1), AS(2), ..., AS(I-1), AS(I), AS(I+1), ..., AS(N), where AS(1) is the rightmost (i.e., origin) AS and AS(N) is the leftmost, i.e., the neighbor of the validating AS. N is the AS_PATH length in terms of the number of unique ASNs. (Note: see [Section 5.1.1](#) for the consideration of a special case.)

An Invalid Pair Index is determined as a minimal I such that the customer-provider validation procedure ([Section 4](#)) with parameters (AS(I), AS(I+1), AFI) returns Invalid. If there is no such minimal I, then the Invalid Pair Index value is set equal to N.

The Reverse Invalid Pair Index is determined as the Invalid Pair Index calculated for the reversed version of the sequence AS(1), AS(2), ..., AS(I-1), AS(I), AS(I+1), ..., AS(N).

An Unknown Pair Index is determined as a minimal I such that the customer-provider validation procedure ([Section 4](#)) with parameters (AS(I), AS(I+1), AFI) returns Unknown. If there is no such minimal I or the minimal I value is greater than the Invalid Pair Index, then the Unknown Pair Index value is set equal to the Invalid Pair Index.

The Reverse Unknown Pair Index is determined as the Unknown Pair Index calculated for the reversed version of the sequence AS(1), AS(2), ..., AS(I-1), AS(I), AS(I+1), ..., AS(N).

The procedures described in [Section 5.2](#) and [Section 5.3](#) make use of the four Indices defined above.

5.1.1. RS-Client of a Non-Transparent RS

A special consideration is given to the case when the validating AS is an RS-client of a non-transparent Route Server (RS). In this case, when the indices described [Section 5.1](#) are computed, the ASN of the RS is removed from the AS_PATH only for the purpose generating the sequence AS(1), AS(2), ..., AS(I-1), AS(I), AS(I+1), ..., AS(N) that was defined in [Section 5.1](#). Thus, AS(N) would equal the AS number of the AS added just before the RS. Also, N would be one less than the AS_PATH length.

Note that when an UPDATE is received from an IX RS, it is equivalent to coming from a lateral peer regardless of whether the RS is transparent or not. Hence, the Upstream path validation procedure ([Section 5.2](#)) can be applied at the receiving RS-client in both cases (i.e., transparent and non-transparent RS) provided that the non-transparent RS AS is removed from the AS_PATH as described above (preceding paragraph).

5.2. Algorithm for Upstream Paths

The upstream verification algorithm described here is applied when a route is received from a customer or a lateral peer, or by an RS-client at an IX RS. Each hop AS(I) to AS(I+1) in the unique ASN sequence AS(1), AS(2),... , AS(N) must be Valid per the customer-provider validation procedure ([Section 4](#)) for the AS_PATH to be Valid. If at least one of those hops is Invalid, then the AS_PATH would be Invalid. If the AS_PATH verification outcome is neither Valid nor Invalid, then it would be evaluated as Unknown.

The upstream path verification procedure is specified as follows:

1. If the AS_PATH has an AS_SET, then the procedure halts with the outcome "Invalid".
2. If the Invalid Pair Index is less than N, then the procedure halts with the outcome "Invalid".
3. If the Unknown Pair Index is less than N, then the procedure halts with the outcome "Unknown".
4. Else, the procedure halts with the outcome "Valid".

5.3. Algorithm for Downstream Paths

The downstream verification algorithm described here is applied when a route is received from a transit provider.

Consider an UPDATE with the unique AS sequence AS(1), AS(2),... , AS(N) as defined in [Section 5.1](#). When the UPDATE is received from a provider, it may have both an upstream ramp (on the left) and a downstream ramp (on the right), where the downstream ramp follows the upstream ramp (both ramps are ASPA valid hop-by-hop). The upstream ramp starts at AS(1) and each AS hop in it has the property that AS(i+1) is a provider of AS(i) per ASPA. The downstream ramp ends at AS(N) and each AS hop in it has the property that AS(i-1) is a provider of AS(i) per ASPA. The upstream ramp stops (reaches its apex) when the ASPA validation to check customer-to-provider relationship of the AS-pair corresponding to the next AS hop gives Invalid or Unknown result. The apex of the downstream ramp is determined similarly but by doing the checks backwards starting with the hop from AS(N-1) to AS(N).

If there is an upstream ramp but no downstream ramp or vice versa, then clearly the UPDATE is valid (i.e., not a route leak). However, if both ramps exist, then the UPDATE is Valid if and only if either one or zero AS hops exist between the apexes of the two ramps, i.e., there is no AS between the apexes (see [[sriram1](#)] for formal proof). If there are one or more ASes between the apexes of the upstream and downstream ramps, then the UPDATE is a route leak (Invalid) or the presence of a leak cannot be known using available ASPAs (Unknown) [[sriram1](#)].

The determination of a route leak (Invalid) UPDATE can be done with the use of the Invalid Pair Index and Reverse Invalid Pair Index. The rule for Invalid determination is as follows: if the sum of Invalid Pair Index and Reverse Invalid Pair Index is less than N,

then route was leaked [[sriram1](#)] or the AS_PATH attribute was malformed.

The downstream path verification procedure is specified as follows:

1. If the AS_PATH has an AS_SET, then the procedure halts with the outcome "Invalid".
2. If the sum of the Invalid Pair Index and the Reverse Invalid Pair Index is less than N, then the procedure halts with the outcome "Invalid".
3. If the sum of the Unknown Pair Index and the Reverse Unknown Pair Index is less than N, then the procedure halts with the outcome "Unknown".
4. Else, the procedure halts with the outcome "Valid".

5.4. ASPA Registration Recommendations

An ASPA is a positive attestation that an AS holder has authorized its providers to redistribute received routes to the provider's providers and lateral peers. This does not preclude the provider AS from redistribution to its other customers. An AS number resource holder in its role as Customer, MUST register each of its transit provider ASes in its ASPA record. Operators SHOULD endeavour to register all providers in a single ASPA object at any time.

Registration of an ASPA (AS, AFI, [0]) and no other ASPAs is meant to be a statement by the registering AS that it has no transit providers. An RS AS MUST register an AS 0 ASPA and MUST NOT register any other ASPAs. Normally, so-called "Tier-1" ASes do not have transit providers. However, if a Tier-1 AS is present at an IX RS as an RS-client, then it MUST register an ASPA showing the RS AS as a provider.

An ASPA (AS, AFI, [0]) SHOULD be the only ASPA registered by an AS that intends declare that it is provider-free in the selected AFI. If AS 0 coexists with other provider ASes in the same ASPA (or other ASPA records in the same AFI), then the presence of the AS 0 has no effect on the AS_PATH verification procedures. The validation procedures simply consider the other (distinct from AS 0) providers as the authorized providers of the AS in consideration.

5.5. AS_PATH Verification Recommendation

A compliant AS MUST apply the upstream and downstream AS path validation algorithms ([Section 5.2](#) and [Section 5.3](#), respectively) in principle producing outcomes as specified though the implementation details may differ.

The procedures described in this document are applicable only for the address families AFI 1 (IPv4) and AFI 2 (IPv6) with SAFI 1 (unicast) in both cases [[IANA-AF](#)]. The procedures MUST NOT be applied to other address families by default.

6. Mitigation

If the output of the AS_PATH verification procedure is "Invalid", then the route MUST be rejected.

The above AS_PATH verification procedures ([Section 5.2](#) and [Section 5.3](#)) are able to check routes received from customers, lateral peers, transit providers, RSeS, and RS-clients. The ASPA-based path verification mechanism combined with BGP Roles [[RFC9234](#)] and ROA-based Origin Validation [[RFC6811](#)] can provide a fully automated solution to detect and filter hijacks and route leaks, including malicious ones (e.g., forged-origin hijacks).

7. Operational Considerations

7.1. Mutual Transit (Complex Relations)

There are peering relationships which cannot be described as strictly simple peer-to-peer (i.e., lateral peers) or customer-to-provider. An example is when both parties (ASes) treat each other as a customer, i.e., the customer-to-provider relationship applies in each direction. That is called a sibling relationship, and in such case, an ASPA (AS1, AFI, [AS2, ...]) must be created by AS1 and another ASPA (AS2, AFI, [AS1, ...]) must be created by AS2.

7.2. AS Confederations

The ASes on the boundary of an AS Confederation MUST register ASPAs using the Confederation's global ASN and the procedures for ASPA-based AS path validation in this document are NOT RECOMMENDED for use on eBGP links internal to the Confederation.

8. Comparison to Other Technologies

8.1. BGPsec

While the described upgrades to BGP are quite useful, they still rely on an unsigned transitive BGP attributes, e.g., AS_PATH, which can be manipulated by on-path attackers. BGPsec [[RFC8205](#)] was designed to solve the problem of AS_PATH validation using cryptographic signatures contained in BGP UPDATE messages. While BGPsec offers protection against unauthorized path modifications, BGPsec by design does not protect against route leaks.

BGPsec and ASPA are complementary technologies.

8.2. Peerlock

The Peerlock mechanism [[Peerlock](#)] [[Flexsealing](#)] has a similar objective as the ASPA-based route leak protection mechanism described in this document. It is commonly deployed by large Internet carriers to protect each other from route leaks. Peerlock depends on a laborious manual process in which operators coordinate the distribution of unstructured Provider Authorizations through out-of-band means in a many-to-many fashion. On the other hand, ASPA's use of the RPKI allows for automated, scalable, and ubiquitous deployment, making the protection mechanism available to a wider range of network operators.

The ASPA mechanism implemented in router code versus Peerlock's AS_PATH regular expressions also provides a way to detect anomalies propagated from transit providers and IX route servers. ASPA is intended to be a complete solution and replacement for existing Peerlock deployments.

9. IANA Considerations

This document includes no request to IANA.

10. Security Considerations

The proposed mechanism is compatible only with BGP implementations that can process 32-bit ASNs in the AS_PATH. This limitation should not have a real effect on operations since legacy BGP routers are rare and it is highly unlikely that they support integration with the RPKI.

ASPA issuers should be aware of the implications of the ASPA-based AS path validation. A downstream AS can apply the verification mechanism and possibly invalidate and reject all routes passed to upstream providers other than the provider ASes listed in the ASPA record. It is the responsibility of each compliant AS to maintain a correct set of providers in its ASPA record(s).

It is highly recommended that a compliant AS should maintain a single ASPA object that covers all its providers. Such a practice will help prevent race conditions during ASPA updates that might affect prefix propagation. The software that provides hosting for ASPA records SHOULD support enforcement of this practice. During a transition process between different certificate authority (CA) registries, the ASPA records SHOULD be kept identical in all registries.

While the ASPA-based mechanism is able to generally detect both mistakes and malicious activity affecting routes received from customers, RS-clients, or lateral peers, it might fail to detect some malicious path modifications for routes that are received from upstream providers.

Since an upstream provider becomes a trusted point, in theory it might be able to propagate without detection some instances of hijacked prefixes of its customers or routes with malformed or manipulated AS_PATHs. While it may happen in theory, it does not seem to be a realistic scenario. Normally a customer and its transit provider have a signed agreement and such a policy violation should have legal consequences or customer can just drop the relationship with such a provider and remove the corresponding ASPA record.

11. Acknowledgments

The authors wish to thank the authors of [[RFC6483](#)] since its text was used as an example while writing [Section 3](#) in this document. Thanks are also due to Jakob Heitz, Ben Maddison, Jeff Haas, and Nick Hilliard for comments and discussion about the algorithms. The authors wish to thank Iljitsch van Beijnum for providing a suggestion about downstream paths.

12. References

12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [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>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [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>>.
- [RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, DOI 10.17487/RFC6793, December 2012, <<https://www.rfc-editor.org/info/rfc6793>>.
- [RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <<https://www.rfc-editor.org/info/rfc6811>>.
- [RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <<https://www.rfc-editor.org/info/rfc7908>>.
- [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>>.

12.2. Informative References

- [Flexsealing] McDaniel, T., Smith, J., and M. Schuchard, "Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis", November 2020, <<https://arxiv.org/pdf/2006.06576.pdf>>.
- [I-D.ietf-grow-route-leak-detection-mitigation] Sriram, K. and A. Azimov, "Methods for Detection and Mitigation of BGP Route Leaks", Work in Progress, Internet-Draft, draft-ietf-grow-route-leak-detection-mitigation-07, 26 April

2022, <<https://www.ietf.org/archive/id/draft-ietf-grow-route-leak-detection-mitigation-07.txt>>.

[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-10, 12 August 2022, <<https://www.ietf.org/archive/id/draft-ietf-sidrops-aspa-profile-10.txt>>.

[IANA-AF] IANA, "Address Family Numbers", <<https://www.iana.org/assignments/address-family-numbers/address-family-numbers.xhtml>>.

[Peerlock] Snijders, J., "Peerlock", June 2016, <https://www.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <<https://www.rfc-editor.org/info/rfc3779>>.

[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, <<https://www.rfc-editor.org/info/rfc6483>>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <<https://www.rfc-editor.org/info/rfc8205>>.

[RFC9234] Azimov, A., Bogomazov, E., Bush, R., Patel, K., and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages", RFC 9234, DOI 10.17487/RFC9234, May 2022, <<https://www.rfc-editor.org/info/rfc9234>>.

[RFC9319] Gilad, Y., Goldberg, S., Sriram, K., Snijders, J., and B. Maddison, "The Use of maxLength in the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 9319, DOI 10.17487/RFC9319, October 2022, <<https://www.rfc-editor.org/info/rfc9319>>.

[sriram1] Sriram, K. and J. Heitz, "On the Accuracy of Algorithms for ASPA Based Route Leak Detection", IETF SIDROPS Meeting, Proceedings of the IETF 110, March 2021, <<https://datatracker.ietf.org/meeting/110/materials/slides-110-sidrops-sriram-aspa-alg-accuracy-01>>.

Authors' Addresses

Alexander Azimov
Yandex
Ulitsa Lva Tolstogo 16
Moscow

119021
Russian Federation

Email: a.e.azimov@gmail.com

Eugene Bogomazov
Qrator Labs
1-y Magistralnyy tupik 5A
Moscow
123290
Russian Federation

Email: eb@qrator.net

Randy Bush
Internet Initiative Japan & Arrcus, Inc.
5147 Crystal Springs
Bainbridge Island, Washington 98110
United States of America

Email: randy@psg.com

Keyur Patel
Arrcus
2077 Gateway Place
Suite #400
San Jose, CA 95119
United States of America

Email: keyur@arrcus.com

Job Snijders
Fastly
Amsterdam
Netherlands

Email: job@fastly.com

Kotikalapudi Sriram
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: ksriram@nist.gov