sidrops
Internet-Draft
Intended status: Standards Track
Expires: 25 October 2025

K. Sriram
NIST
N. Geng
Huawei
A. Herzberg
University of Connecticut

23 April 2025

Autonomous System Relationship Authorization (ASRA) as an Extension to ASPA for Enhanced AS Path Verification
draft-sriram-sidrops-asra-verification-02

Abstract

Autonomous System Provider Authorization (ASPA) record authorizes provider ASes of a customer AS (CAS). While ASPA-based AS_PATH verification can correctly detect and mitigate route leaks and some forged-origin or forged-path-segment hijacks, it fails to detect some malicious path manipulations for routes that are received from transit providers. This document utilizes a new RPKI object called Autonomous System Relationship Authorization (ASRA) that significantly enhances AS_PATH verification complementing ASPA. ASRA fills in a significant gap in the ASPA method by adding the capability to detect fake links in the AS_PATHs in BGP Updates propagated from providers to customers. ASRA achieves this by allowing an AS to register additional AS relationships, i.e., customers and lateral peers.

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 25 October 2025.

Table of Contents

1. Introduction

Autonomous System Provider Authorization (ASPA) record authorizes provider ASes of a customer (subject) AS [I-D.ietf-sidrops-aspa-profile]. While ASPA-based AS_PATH verification can correctly detect and mitigate route leaks and some forged-origin or forged-path-segment hijacks, it fails to detect some malicious path manipulations for routes that are received from transit providers (see Appendix B and Section 9 of [I-D.ietf-sidrops-aspa-verification]). This document utilizes a new RPKI object called Autonomous System Relationship Authorization (ASRA) that significantly enhances AS_PATH verification complementing ASPA. The Cryptographic Message Syntax (CMS) protected content type for the RPKI ASRA object is defined in [I-D.geng-sidrops-asra-profile]. ASRA fills in a significant gap in the ASPA method by adding the capability to detect fake links in the AS_PATHs in BGP Updates propagated from providers to customers. ASRA achieves this by allowing an AS to register additional AS relationships, i.e., customers and lateral peers.

ASPA already has the capability of detecting forged-origin or forged-path-segment hijacks (Section 2) when a verifying AS receives a BGP Update from a customer or lateral peer. ASRA adds the capability of detecting the same when a verifying AS receives a BGP Update from a provider. A forged-origin or forged-path-segment hijack involves a fake link (i.e., forged AS peering). The ASRA algorithm operates in conjunction with ASPA in such a way that it fully preserves the route leak detection capabilities of ASPA while adding the fake link detection capability.

Incremental benefit is accrued by early adopters. An AS that deploys ASPA and ASRA prevents an offending AS from faking a link to it if the receiving/verifying AS also deploys ASPA and ASRA. The fake link will be detected by the receiving AS even if no other AS in the received AS path has adopted ASPA or ASRA.

The reader is expected to be familiar with the following related documents: [I-D.ietf-sidrops-aspa-profile], [I-D.ietf-sidrops-aspa-verification], [I-D.ietf-sidrops-8210bis].

1.1. Terminology

The usage of terms follows Section 3 of [I-D.ietf-sidrops-aspa-verification].

1.2. 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.

2. AS Path Security Problems Addressed by ASRA

2.1. Fake-Link Attack: Provider Attacking a Customer

ASPA's properties of detection of forged-origin or forged-path-segment hijacks work only when the BGP Update is received from a customer or lateral peer (see Appendix B in [I-D.ietf-sidrops-aspa-verification]). The use of ASRA (together with ASPA) extends these properties to scenarios where the Update is received from a transit provider. This is achieved due to the added capability of detecting fake links in the AS path with the assistance of ASRAs. ASPA alone cannot detect fake links.

An example scenario is illustrated in Figure 1. Assume that all ASes shown in the Figure (the attacker AS(6) being a possible exception) register ASPA records and do ASPA-based AS_PATH verification. Where a link is marked C2P (Customer-to-Provider), it indicates that the AS shown below is a customer of the provider AS shown above. AS(1) originates the BGP route for prefix P which propagates to the other ASes. The AS_PATH received by AS(6) is path{5,4,3,2,1}. However, the misbehaving AS(6) shortens the path by faking link with AS(2) and propagates the route to AS(7) with a shortened path {6,2,1} to AS(7). AS(7) fails to detect the manipulated path based on verification using only ASPAs. It chooses this path over the other valid path via AS(8). However, if ASRA is deployed by AS(2), then AS(2)'s ASPA and ASRA can indicate that AS(6) is not connected to AS(2), and the faked link from AS(6) to AS(2) will be detected. If ASRA is deployed by AS(1), AS(2), and AS(4) also, then AS(6) is prevented from conducting the forged-origin or forged-path segment type of attack on its customer AS(7) (in this scenario). The details about the registration of ASRA and the algorithms for AS path verification using ASPAs and ASRAs are provided in Section 3 and Section 4, respectively.

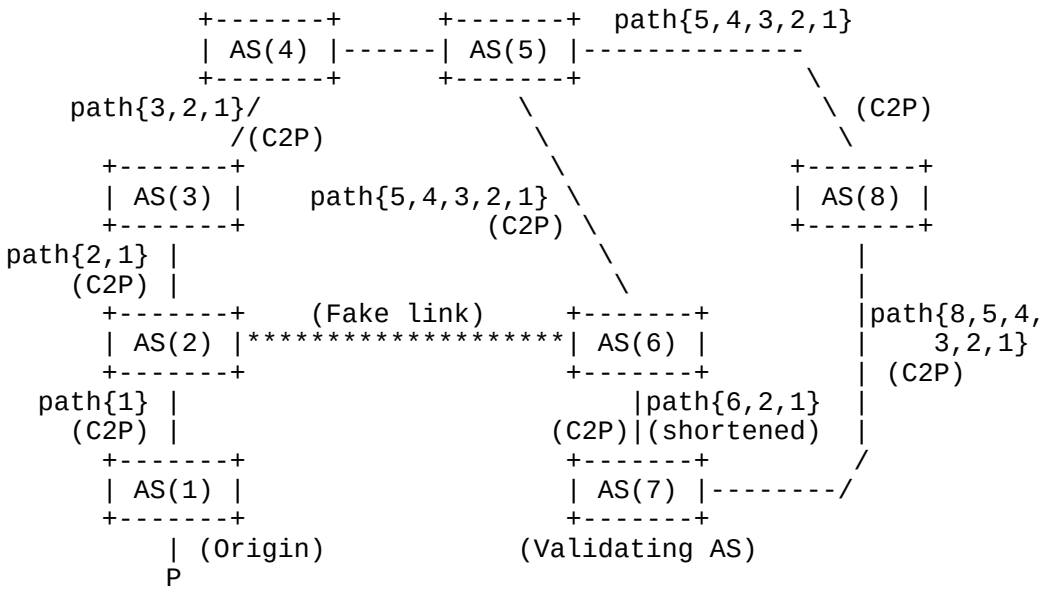

Figure 1: AS_PATH shortened by a misbehaving provider.

2.2. Fake-Link Attack: Customer Attacking its Non-Adopting Provider and Other Customer

Figure 2 illustrates a scenario in which one customer AS(6) of the non-adopting provider AS(7) attacks the provider which in turn propagates the attack (Update) to its other customer AS(5). In this example (Figure 2), the provider AS(7) has not adopted ASPA but all other ASes have. AS(5) is the receiver performing ASPA-based AS path verification. AS(6) conducts a fake-link (forged-origin) attack on AS(7) which accepts the route and propagates it to AS(5). AS(5) receives two routes (one each from AS(7) and AS(4)) and per-ASPA verification, the shorter route from AS(7) is Unknown while the longer route is Valid. But since both Valid and Unknown routes are eligible for path selection, AS(5) would select the shorter path from AS(7) and is thus deceived in effect by AS(6). If ASRA is deployed by AS(1) and AS(5), then AS(5) can detect and mitigate the fake-link (forged-origin) attack using ASRA and ASPA data (Section 4).

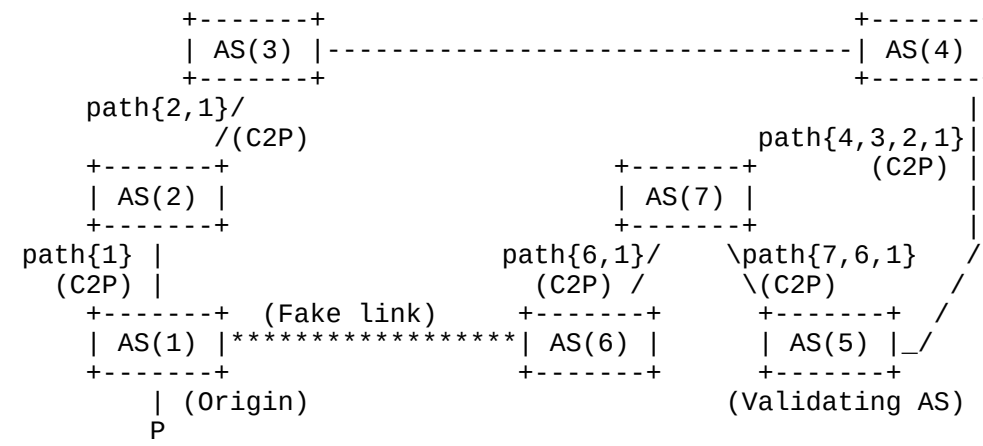

Figure 2: Customer attacking its non-adopting provider and another customer.

3. ASRA Registration Recommendations

The term "Compliant AS" or "compliant BGP router" in this document refers to one that is compliant with the specifications in this document. A compliant AS that has a valid ASRA record MUST also have a valid ASPA record. A valid ASRA record(s) for a signer (subject) AS that does not have a valid ASPA record MUST be ignored (considered unusable) for AS path verification purposes.

There are three subcategories of ASRAs defined: ASRA1, ASRA2, and ASRA3 [I-D.geng-sidrops-asra-profile]. They are distinguished by a subcategory field by setting its value to 1, 2, or 3, respectively. ASRA1 and ASRA2 are used to register the lists of customers and lateral peers, respectively. Alternatively, if the subject AS does not wish to separately disclose customers and lateral peers, it MAY choose to register an ASRA3 to register the combined list of customers and lateral peers. An ASRA-compliant AS MUST either register ASRA3 alone or register both ASRA1 and ASRA2. To signal that there are no neighbors to report in a subcategory, AS 0 MUST be included in the corresponding ASRA subcategory in the payload field.

If it is found that an AS has X.509 valid ASRA3 and simultaneously has X.509 valid ASRA1 and/or ASRA2, then only the ASRA3 MUST be considered for AS path verification and the ASRA subcategories ASRA1 and ASRA2 MUST be ignored.

It is highly RECOMMENDED that an AS (compliant signer AS) register and maintain either a single ASRA3 object or a single object of each subcategory ASRA1 and ASRA2. Such a practice helps prevent race

conditions during ASRA updates. If multiple X.509 valid ASRAs of a subcategory exist for given subject AS, the ASes listed in all such ASRAs will be combined (by the relying party) into one list of neighbors of the subcategory in consideration. This combined list will be used for AS path verification purposes.

All neighbors that are customers or lateral peers of the signer AS MUST be included in an ASRA(s) of an appropriate subcategory following above-mentioned recommendations.

A pair of compliant ASes in a mutual transit relationship are required to include each other in their respective ASPA (per [I-D.ietf-sidrops-aspa-verification]). They MUST NOT further include each other in ASRA1, ASRA2, or ASRA3. A compliant AS that has a complex relationship with a neighbor AS where one of the relationships is Provider is required to include the neighbor AS in its ASPA (per [I-D.ietf-sidrops-aspa-verification]). (Note: By the term "relationship is foo" it is meant here that the neighbor is foo.) The AS MUST NOT further include the other AS in ASRA1, ASRA2, or ASRA3. A compliant AS that has a complex relationship with a neighbor AS where none of the relationships are Provider implies that its relationships with the neighbor AS are customer and lateral peer. In such a case, the AS MUST include the neighbor AS in its ASRA3 if doing ASRA3, otherwise in its ASRA1 as well as ASRA2.

The Route Server (RS) to RS-client relationship is similar to the provider-to-customer relationship. So, a compliant non-transparent RS AS MUST either (1) list all its RS-clients as customers in ASRA3, or (2) list all its RS-clients as customers in ASRA1 and register an ASRA2 with only AS 0 listed in the set of lateral peers.

Transparent RS AS case: Typically, an IX RS publishes a list of all RS clients it has so that each RS client can choose which other clients to peer with. The peering relationships are set up by using BGP Community tags or through policies configured at the RS AS. In the case of a transparent RS AS, the peering between any pair of clients is effectively lateral peering (note that the RS AS is absent in the AS_PATH). A compliant RS client of a transparent RS AS MUST include in the ASRA all the AS numbers of other RS clients that it has selected to peer with at the RS. If a compliant RS client has selected to receive all routes from a transparent RS, then the RS client MUST include in the ASRA the full published list of RS clients of the transparent RS.

Authors’ note: The possibility of defining an ASRA type using which a transparent RS AS can register all its RS clients will be considered in case it adds value. It may be useful at least for cross-checking the peering relationships registered by RS clients.

4. Algorithms for Enhancement of AS Path Verification Using ASRA

In this section, two algorithms are described which enhance AS path verification by augmenting ASPA-based verification [I-D.ietf-sidrops-aspa-verification] with ASRA data. The basic principles behind each algorithm are explained. (The intention is that the SIDROPS WG discussions will help decide which algorithm to select.)

Let the sequence {AS(N), AS(N-1),..., AS(2), AS(1)} represent the AS_PATH in terms of unique ASNs, where AS(1) is the origin AS and AS(N) is the most recently added AS and neighbor of the receiving/ verifying AS. The terms AS path and AS_PATH are interchangeably used in this document. N is the AS path length in unique ASes. Let AS(N+1) represent the receiving AS that is verifying the entire received AS path. For a given AS hop, say AS(i) to AS(i+1), AS(i) is the sender and AS(i+1) is the receiver. For each such AS hop in the AS path, the algorithms seek to check if the hop is a fake link, i.e., AS(i+1) forging a connection to AS(i).

In the descriptions that follow, a valid ASPA or ASRA is one that is X.509 valid.

4.1. Algorithm A (Less Strict)

For a given AS hop AS(i) to AS(i+1), algorithm A gives precedence to the ASPA created by the receiver AS(i+1) over the ASRA created by the sender AS(i), and hence it is less strict (compared to Algorithm B (Section 4.2)). This algorithm can be used under the assumption that AS(i+1) is very unlikely to create a false ASPA record (i.e., falsely including AS(i) as a provider) because it is a digitally signed object and hence repudiation is hard. However, this algorithm does not guard against the creation of a false ASPA record and under such conditions the stricter Algorithm B (Section 4.2) must be used.

4.1.1. Fake Link Determination (Alg. A)

The following is the procedure (per Algorithm A) for determining if the AS(i) to AS(i+1) hop in the AS path is a fake link.

- If AS(i) has valid ASPA(s) and they do not include AS(i+1) as a Provider,
- AND if AS(i) has valid ASRA(s) and they do not include AS(i+1) as a customer or lateral peer,
- AND {EITHER AS(i+1) has no valid ASPA OR {AS(i+1) has valid ASPA(s) and they do not include AS(i) as a Provider},
- then set Fake-Link(AS(i), AS(i+1)) = Detected,
- Else, set Fake-Link(AS(i), AS(i+1)) = Not Detected.

4.1.2. Enhancement to AS Path Verification Using ASRA (Alg. A)

4.1.2.1. Algorithm for Upstream Paths

Remains unchanged and the same as described in Section 7.2 of [I-D.ietf-sidrops-aspa-verification].

4.1.2.2. Algorithm for Downstream Paths (Alg. A)

The parameters min_up_ramp and min_down_ramp represent ramp lengths (in # ASes), and are computed using only ASPAs (see Section 7 of [I-D.ietf-sidrops-aspa-verification] and Figure 3 below). Successive ASPAs affirm the up-ramp from AS(1) to AS(K), where K = min_up_ramp. The up-ramp stops at AS(K) because AS(K) does not have a valid ASPA or its valid ASPA(s) do not include AS(K+1) as a provider. The down-ramp from AS(L) to AS(N) is also affirmed by successive ASPAs, where L = N - min_down_ramp + 1. The top of the down-ramp is at AS(L) because AS(L) does not have a valid ASPA or its valid ASPA(s) do not include AS(L-1) as a provider.

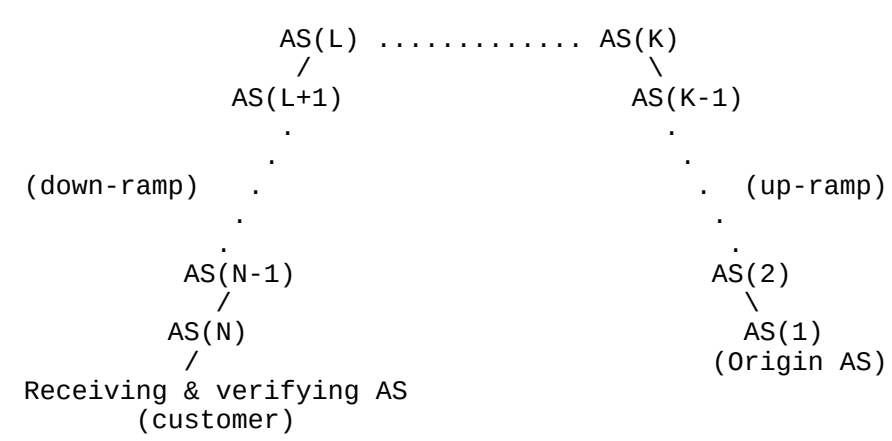

Figure 3: Illustration of min-up-ramp and min-down-ramp

First, run the verification algorithm for downstream paths as described in Section 7.3 of [I-D.ietf-sidrops-aspa-verification]. The obtained outcome is one of these: Valid, Invalid, Unknown. Now enhance the outcome using the following algorithm where ASRA data is applied. For the Fake-Link(AS(i), AS(i+1)) function, use the one described in Section 4.1.1.

1. If the outcome is Invalid, it remains unchanged and the procedure halts.
2. Else, if min_up_ramp = N or {min_up_ramp + min_down_ramp} > N, then the outcome remains unchanged (Valid)and the procedure halts.
3. Else, let i = min_up_ramp.
4. If Fake-Link(AS(i), AS(i+1)) = Detected, then change the outcome to Invalid and the procedure halts.
5. Else, if i = N - min_down_ramp, then the procedure halts (outcome remains unchanged).
6. Else, increment i to i+1. Go to Step #4.

4.2. Algorithm B (Strict)

Algorithm B does not give precedence to the ASPA created by the receiver AS(i+1) over the ASRA created by the sender AS(i), and hence it is strict (compared to Algorithm A). This algorithm is used to counter the possibility that AS(i+1) could maliciously create a false ASPA record (i.e., falsely including AS(i) as a provider) even though repudiation is hard.

4.2.1. Fake Link Determination (Alg. B)

The following is the procedure (per Algorithm B) for determining if the AS(i) to AS(i+1) hop in the AS path is a fake link.

- If AS(i) has valid ASPA(s) and they do not include AS(i+1) as a Provider,
- AND if AS(i) has valid ASRA(s) and they do not include AS(i+1) as a customer or lateral peer,
- then set Fake-Link(AS(i), AS(i+1)) = Detected,
- Else, set Fake-Link(AS(i), AS(i+1)) = Not Detected.

4.2.2. Enhancement to AS Path Verification Using ASRA (Alg. B)

4.2.2.1. Algorithm for Upstream Paths

Remains unchanged and the same as described in Section 7.2 of [I-D.ietf-sidrops-aspa-verification].

4.2.2.2. Algorithm for Downstream Paths (Alg. B)

Here the min_up_ramp parameter is the same as discussed in Section 4.1.2.2. First, run the verification algorithm for downstream paths as described in Section 7.3 of [I-D.ietf-sidrops-aspa-verification]. The obtained outcome is one of these: Valid, Invalid, Unknown. Now enhance the outcome using the following algorithm where ASRA data is applied. For the Fake-Link(AS(i), AS(i+1)) function, use the one described in

Section 4.2.1.

1. If the outcome is Invalid, it remains unchanged and the procedure halts.
2. Else, if min_up_ramp = N, then also the outcome remains unchanged (Valid) and the procedure halts.
3. Else, let i = min_up_ramp.
4. If Fake-Link(AS(i), AS(i+1)) = Detected, then change the outcome to Invalid and the procedure halts.
5. Else, if i = N - 1, then the procedure halts (outcome remains unchanged).
6. Else, increment i to i+1. Go to Step #4.

The differences between the above procedure and the corresponding procedure in Section 4.1.2.2 for Algorithm A are at steps #2 and #5.

5. Operational Considerations

Every AS operator doing ASPA/ASRA SHOULD periodically check their own ASPA/ASRA objects for correctness and completeness. They SHOULD also ensure that the same are refreshed well before their expiry dates.

Every AS operator doing ASPA SHOULD periodically monitor all the ASPAs in the RPKI repositories to check if their AS number is incorrectly included as a provider in an ASPA (X.509 valid), and if so, they SHOULD report it to the responsible party (or parties) so that the ASPA can be rectified.

Every AS operator doing ASPA SHOULD periodically monitor all the ASPAs in the RPKI repositories to check if their AS number is incorrectly not included as a provider in the ASPA of a customer AS (CAS), and if so, they SHOULD report it to the CAS operator so that the ASPA can be rectified.

Every AS operator doing ASRA SHOULD periodically monitor all the ASRAs in the RPKI repositories to check if their AS number is incorrectly included (or incorrectly not included) in an ASRA (X.509 valid), and if so, they SHOULD report it to the responsible party (or parties) so that the ASRA can be rectified.

6. Security Considerations

Security concerns for AS path verification using ASPA and ASRA are largely alleviated if the operational recommendations (Section 5) are followed.

7. IANA Considerations

This document does not have IANA considerations.

8. Acknowledgements

The authors wish to thank Mingqing (Michael) Huang, Alexander Azimov, Jeff Haas, Doug Montgomery, and Oliver Borchert for very helpful comments and discussions.

9. References

9.1. Normative References

[I-D.ietf-sidrops-aspa-verification]
Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-22, 23 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-22>.

[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>.

[I-D.geng-sidrops-asra-profile]
Geng, N., Sriram, K., and M. Huang, "A Profile for Autonomous System Relationship Authorization (ASRA)", Work in Progress, Internet-Draft, draft-geng-sidrops-asra-profile-01, 15 April 2025, <https://datatracker.ietf.org/doc/html/draft-geng-sidrops-asra-profile-01>.

[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>.

9.2. Informative 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>.

Authors' Addresses

Kotikalapudi Sriram
NIST
Gaithersburg, MD 20899,
United States of America
Email: ksriram@nist.gov

Nan Geng
Huawei
Beijing
China
Email: gengnan@huawei.com

Amir Herzberg
University of Connecticut
Storrs, CT 06269,
United States of America
Email: amir.herzberg@uconn.edu