

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 September 2022

J. Snijders
Fastly
M. Abrahamsson
NTT
B. Maddison
Workonline
7 March 2022

Resource Public Key Infrastructure (RPKI) object profile for Discard
Origin Authorizations (DOA)
draft-spaghetti-sidrops-rpki-doa-00

Abstract

This document defines a Cryptographic Message Syntax (CMS) profile for Discard Origin Authorizations (DOAs), for use with the Resource Public Key Infrastructure (RPKI). A DOA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate routes to one or more prefixes within the address block tagged with a specific set of Border Gateway Protocol (BGP) Communities, to signal a request to discard IP traffic destined towards the tagged IP prefix.

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 8 September 2022.

Internet-Draft

RPKI DOA

March 2022

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	3
2.	DOA EncapsulatedContentInfo	3
2.1.	ASN.1 Module	3
2.2.	The DOA eContentType	5
2.3.	The DOA eContent	5
2.3.1.	version	5
2.3.2.	ipAddrBlocks	5
2.3.3.	originAsID	5
2.3.4.	peerAsIDs	6
2.3.5.	communities	6
3.	DOA Validation	6
4.	RPKI-RTR protocol extensions	6
5.	BGP Route Matching	6
6.	Route Origin Validation Co-Existence	7
7.	Exporting RTBH Routes	8
8.	Operational Considerations	8
9.	Security Considerations	8
10.	Implementation status	8
11.	IANA Considerations	9
11.1.	SMI Security for S/MIME CMS Module Identifier (1.2.840.113549.1.9.16.0)	9
11.2.	SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)	9
11.3.	RPKI Signed Objects registry	9
11.4.	RPKI Repository Name Schemes registry	10
11.5.	Media Types registry	10
12.	References	10

12.1.	Normative References	11
12.2.	Informative References	11
Appendix A.	Acknowledgements	12
Appendix B.	Document Changelog	12
B.1.	Individual Submission Phase	12

Authors' Addresses	12
------------------------------	--------------------

[1.](#) Introduction

Internet operators commonly provide a means for adjacent networks to advertise routes in BGP with the intention that traffic matching such a route be discarded, rather than being forwarded towards the advertising network. This is referred to as Remotely Triggered Blackholing (RTBH), and is typically achieved through the use of a BGP Community [[RFC1997](#)]. [[RFC7999](#)] defines a "well known" community value for this purpose. The route used to signal an RTBH request is referred to as an RTBH route.

Inter-AS RTBH signalling, however, is in tension with the deployment of Route Origin Validation (ROV) based on the Resource Public Key Infrastructure (RPKI) [[RFC6811](#)]. Because a blackhole route is likely to have a prefix length greater than permitted in any covering ROA, an operator wishing to deploy routing policy to discard BGP paths with an ROV status of "Invalid", and simultaneously maintain a blackhole signalling service must choose either:

1. to exempt blackhole routes from processing based on ROV status, thus foregoing the benefit of ROV altogether; or
2. to insist that users of the blackhole signalling service create ROAs with a sufficiently large "maxLength" values to accomodate blackhole routes.

This document defines a Cryptographic Message Syntax (CMS) [[RFC5652](#)] profile for Discard Origin Authorizations (DOAs), for use with the Resource Public Key Infrastructure (RPKI) [[RFC6480](#)], along with associated processing rules.

DOAs can be used to validate whether incoming BGP route announcements carrying specific BGP Communities are meant to signify a request to discard IP traffic towards the IP destination carried in the BGP

route. This enhances the concepts of [[RFC3882](#)] and [[RFC7999](#)], and can co-exist with deployed ROV policy.

[2.](#) DOA EncapsulatedContentInfo

DOA follows the Signed Object Template for the RPKI [[RFC6488](#)].

[2.1.](#) ASN.1 Module

The following ASN.1 module specifies the encapContentInfo component for DOA objects:

```
RpkiDiscardOriginAuthorization-2021
{ iso(1) member-body(2) us(840) rsadsi(113549)
  pkcs(1) pkcs9(9) smime(16) mod(0) TBD }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
CONTENT-TYPE
FROM CryptographicMessageSyntax-2010 -- in [RFC6268]
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) }

IPAddressOrRange, IPAddressRange, IPAddress, ASId
FROM IPAddrAndASCertExtn -- in [RFC3779]
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) mod(0)
  id-mod-ip-addr-and-as-ident(30) } ;

ct-discardOriginAuthorization CONTENT-TYPE ::=
{ TYPE DiscardOriginAuthorization IDENTIFIED BY
  id-ct-discardOriginAuthorization }

id-ct-discardOriginAuthorization OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) id-smime(16) id-ct(1) TBD }

DiscardOriginAuthorization ::= SEQUENCE {
  version                [0] INTEGER DEFAULT 0,
```

```

    ipAddrBlocks      IPListRange,
    originAsID        ASId,
    peerAsIDs         [1] SEQUENCE SIZE(1..MAX) OF ASId OPTIONAL,
    communities       [2] SEQUENCE SIZE(1..MAX) OF Community
}

IPListRange ::= SEQUENCE (SIZE(1..MAX)) OF IPAddressFamilyRange

IPAddressFamilyRange ::= SEQUENCE {
    addressFamily      OCTET STRING (SIZE(2..3)),
    addressOrRange     IPAddressOrRange,
    prefixLengthRange  PrefixLengthRange OPTIONAL -- if omitted, assume hos
}

PrefixLengthRange ::= SEQUENCE {
    minLength          INTEGER,
    maxLength          INTEGER
}

```

```

Community ::= CHOICE {
    bgpCommunity      [0] OCTET STRING (SIZE(4)),
    bgpLargeCommunity [1] OCTET STRING (SIZE(12))
}

```

END

[2.2.](#) The DOA eContentType

The eContentType for a DOA is defined as id-ct-discardOriginAuthorization as specified in [Section 2.1](#).

This OID MUST appear both within the eContentType in the encapContentInfo object as well as the ContentType signed attribute in the signerInfo object (see [\[RFC6488\]](#)).

[2.3.](#) The DOA eContent

The content of a DOA is formally defined as DiscardOriginAuthorization as specified in [Section 2.1](#)

[2.3.1.](#) version

The version number of the DiscardOriginAuthorization MUST be 0.

[2.3.2.](#) ipAddrBlocks

The IP address prefixes for which the announcement of RTBH routes is authorized. The IP address resources contained here are the resources used to mark the authorization, and MUST match the set of resources listed by the EE certificate carried in the CMS certificates field. See [\[RFC6482\] Section 3.3](#) for a similar, but not entirely similar approach. A notable difference is the absence of MaxLength, and instead a PrefixLengthRange is used. If no PrefixLengthRange is present, only the "host route" prefix length (i.e. 32 for IPv4 and 128 for IPv6) is authorized.

[2.3.3.](#) originAsID

The asID field contains the AS number that is authorized to originate RTBH routes for the given IP address prefixes. The asID does not have to be contained by the resources listed on the EE certificate.

[2.3.4.](#) peerAsIDs

The peerAsIDs field contains zero or more AS numbers that are authorized to propagate routes intended to signal an RTBH request for the given IP address prefixes. The peerAsIDs do not have to be contained by the resources listed on the EE certificate. Network operators MUST only accept the RTBH request if it was received from any listed peerAsIDs. The peerAsIDs field allows DOAs to be used to validate RTBH routes with one AS hop between originator and recipient.

[2.3.5.](#) communities

The communities field contains the Classic BGP communities or Large BGP Communities which are to be the 'trigger' to start RTBH. TBD:

are communities 'and' or 'or'?

[3.](#) DOA Validation

To validate a DOA the relying party MUST perform all the validation checks specified in [[RFC6488](#)] as well as the following additional DOA-specific validation step:

- * The IP delegation extension [[RFC3779](#)] MUST be present in the end-entity certificate (contained in the DOA), and every IP address prefix present in the ipAddrBlocks component of the DOA eContent is contained within the set of IP addresses specified in the EE certificate's IP address delegation extension.

[4.](#) RPKI-RTR protocol extensions

TODO: Seperate document?

[5.](#) BGP Route Matching

TODO: Seperate document?

A BGP speaker MAY assign to each path it receives from its peers one of 3 RTBH request validation states:

- * Matched: a validated DOA object was found covering the prefix of the received path, and matching the constraints of the DOA;
- * Unmatched: a validated DOA object was found covering the prefix of the received path, but the constraints of the DOA were not matched; or

- * NotFound: a validated DOA object covering the prefix of the received path was not found.

Where "covering" is used as in its definition in [Section 2 \[RFC6811\]](#).

In order for a BGP path to be considered to have matched the constraints of a DOA object, the following conditions MUST be met:

- * The route originated from the ASN listed in the ASId.
- * The route was received from a PeerAS which is either the ASId or listed in the peerAsIDs field.
- * The route's prefix length matches the listed permissible prefix lengths.
- * The route is tagged with (TODO: one or more of?) the designated BGP community.

[6.](#) Route Origin Validation Co-Existence

It is important to observe that ROAs and DOAs can and will be issued for the same covered address space, and that the resulting ROV validation state MUST be entirely independent of the resulting DOA validation state.

In particular it is expected that legitimate RTBH routes will commonly receive a DOA validation state of 'Matched' whilst also receiving a ROV validation state of 'Invalid' due to the (likely) longer prefix-length of an RTBH route.

For this reason, it is recommended that operators construct policy so as to act on the DOA validation early in the routing policy application process, such that routes that are 'Matched' may be installed as RTBH routes, and routes that are 'Unmatched' or 'NotFound' can "fall-through" to be processed as "normal" routes, including the possible application of policy based on their ROV validation state.

Critically, in order that operators are able to construct policy according to their needs conforming implementations MUST NOT take any policy action on a route based on either its DOA or ROV validation state by default. See also [[RFC8481](#)].

[7.](#) Exporting RTBH Routes

The guidance of [Section 3.2 \[RFC7999\]](#) that, in general, RTBH routes SHOULD NOT be propagated beyond the receiving AS continues to apply to RTBH routes validated in terms of the above mechanisms.

The exception to this guidance is that an operator MAY propagate a received RTBH route to neighboring ASes if its own AS number appears in the peerAsIDs field of the matched DOA, since this indicates a desire by the issuer that neighbors of the local AS honour the route as a legitimate RTBH signal.

To facilitate the construction of routing policies by operators that implemented this behaviour, conforming BGP speaker implementations SHOULD provide a means of distinguishing between 'Matched' routes for which the local AS appears in the peerAsIDs of the matched DOA from those for which it does not.

[8.](#) Operational Considerations

TODO

[9.](#) Security Considerations

TODO

[10.](#) Implementation status

This section is to be removed before publishing as an RFC.

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".

- * A signer implementation [[rpkimancer-doa](#)] written in Python has been developed by Ben Maddison.

[11.](#) IANA Considerations

[11.1.](#) SMI Security for S/MIME CMS Module Identifier (1.2.840.113549.1.9.16.0)

The IANA is requested to register the following entry for this document in the "SMI Security for S/MIME CMS Module Identifier (1.2.840.113549.1.9.16.0)" registry:

Decimal	Description	References
[TBD]	id-mod-rpkiDOA	[draft-spaghetti-sidrops-rpki-doa]

Upon publication of this document, IANA is requested to reference the RFC publication instead of this draft.

[11.2.](#) SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)

The IANA is requested to register the following entry for this document in the "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" registry:

Decimal	Description	References
[TBD]	id-ct-discardOriginAuthorization	[draft-spaghetti-sidrops-rpki-d]

Upon publication of this document, IANA is requested to reference the RFC publication instead of this draft.

[11.3.](#) RPKI Signed Objects registry

The IANA is requested to register the OID for the RPKI Discard Origin Authorization in the "RPKI Signed Objects" registry ([[RFC6488](#)]) as

follows:

Name	OID	Reference
-----	-----	-----
DOA	1.2.840.113549.1.9.16.1.TBD	[RFC-TBD]

[11.4.](#) RPKI Repository Name Schemes registry

The IANA is requested to register the RPKI Discard Origin Authorization file extension in the "RPKI Repository Name Schemes" registry ([[RFC6481](#)]) as follows:

Filename Extension	RPKI Object	Reference
-----	-----	-----
.doa	Discard Origin Authorization	[RFC-TBD]

[11.5.](#) Media Types registry

The IANA is requested to register the media type application/rpki-doa in the "Media Types" registry ([[RFC6838](#)]) as follows:

Type name: application
Subtype name: rpki-doa
Required parameters: None
Optional parameters: None
Encoding considerations: binary
Security considerations: Carries an RPKI Discard Origin Authorization
[RFC-TBD].
Interoperability considerations: None
Published specification: This document.
Applications that use this media type: RPKI operators.
Additional information:
Content: This media type is a signed object, as defined
in [[RFC6488](#)], which contains a payload of a set of matching
criteria as defined above in [RFC-TBD].
Magic number(s): None
File extension(s): .doa
Macintosh file type code(s):
Person & email address to contact for further information:

Job Snijders <job@fastly.com>
Intended usage: COMMON
Restrictions on usage: None
Author: Job Snijders <job@fastly.com>
Change controller: Job Snijders <job@fastly.com>

12. References

Snijders, et al. Expires 8 September 2022 [Page 10]

Internet-Draft RPKI DOA March 2022

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>>.
- [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>>.
- [RFC3882] Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", [RFC 3882](#), DOI 10.17487/RFC3882, September 2004, <<https://www.rfc-editor.org/info/rfc3882>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, [RFC 5652](#), DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/info/rfc5652>>.
- [RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", [RFC 6481](#), DOI 10.17487/RFC6481, February 2012, <<https://www.rfc-editor.org/info/rfc6481>>.
- [RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", [RFC 6488](#), DOI 10.17487/RFC6488, February 2012, <<https://www.rfc-editor.org/info/rfc6488>>.
- [RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", [BCP 13](#),

[RFC 6838](#), DOI 10.17487/RFC6838, January 2013,
<<https://www.rfc-editor.org/info/rfc6838>>.

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

[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

Snijders, et al.

Expires 8 September 2022

[Page 11]

Internet-Draft

RPKI DOA

March 2022

[RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", [RFC 1997](#), DOI 10.17487/RFC1997, August 1996,
<<https://www.rfc-editor.org/info/rfc1997>>.

[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>>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", [RFC 6482](#), DOI 10.17487/RFC6482, February 2012,
<<https://www.rfc-editor.org/info/rfc6482>>.

[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>>.

[RFC8481] Bush, R., "Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)", [RFC 8481](#), DOI 10.17487/RFC8481, September 2018,
<<https://www.rfc-editor.org/info/rfc8481>>.

[rpkimancer-doa]

Maddison, B., "rpkimancer-doa", June 2021,

<<https://pypi.org/project/rpkimancer-doa/>>.

[Appendix A](#). Acknowledgements

TODO

[Appendix B](#). Document Changelog

This section is to be removed before publishing as an RFC.

[B.1](#). Individual Submission Phase

Authors' Addresses

Job Snijders
Fastly
Amsterdam
Netherlands
Email: job@fastly.com

Snijders, et al.

Expires 8 September 2022

[Page 12]

Internet-Draft

RPKI DOA

March 2022

Mikael Abrahamsson
NTT Ltd.
Stockholm
Sweden
Email: mikael@swm.pp.se

Ben Maddison
Workonline Communications
Cape Town
South Africa
Email: benm@workonline.africa

