Workgroup: sidrops
Internet-Draft:
draft-spaghetti-sidrops-rpki-asgroup-00
Published: 16 November 2022
Intended Status: Standards Track
Expires: 20 May 2023
Authors: J. Snijders FK. Korsbäck
Fastly Amazon

A profile for RPKI Signed Groupings of Autonomous System Numbers (ASGroup)

Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI) to carry a general-purpose listing of Autonomous System Numbers (ASNs) and/or pointers to other groupings of ASNs, called an ASGroup. Additionally, the document specifies a mechanism for ASN holders to opt-out of being listed in a given ASGroup. The objective is to offer a RPKI-based successor to plain-text RFC 2622 'as-set' class objects. When validated, an ASGroup confirms that the respective ASN holder produced the ASGroup object.

Status of This Memo

This Internet-Draft will expire on 20 May 2023.

Copyright Notice

Table of Contents

1. Introduction
  1.1. Requirements Language
2. ASGroup and ASGroup Opt-Out Listing Profile
  2.1. EE Certificates
  2.2. Object Filenames
3. eContentType
  3.1. The ASGroup eContentType
  3.2. The ASGroup Opt-Out Listing eContentType
4. eContent
  4.1. The ASGroup eContent
    4.1.1. Version
    4.1.2. asID
    4.1.3. label
    4.1.4. referenceable
    4.1.5. members
  4.2. The ASGroup Opt-Out Listing eContent
    4.2.1. Version
    4.2.2. asID
    4.2.3. label
    4.2.4. optOut
5. ASGroup Validation
6. Operational Considerations
7. Security Considerations
8. IANA Considerations
  8.1. SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)
  8.2. RPKI Signed Objects
  8.3. RPKI Repository Name Schemes
  8.4. SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)
  8.5. Media Types
    8.5.1. ASGroup Media Type
    8.5.2. ASGroup Opt-Out Listing Media Type
9. References
  9.1. Normative References
  9.2. Informative References
Appendix A. Acknowledgements
Appendix B. Example payloads
  B.1. Example ASGroup eContent Payload
  B.2. Example ASGroup Opt-Out Listing eContent Payload
Appendix C. Implementation status

Authors' Addresses

1. Introduction

This document defines a Cryptographic Message Syntax (CMS) [RFC5652] [RFC6268] protected content type for a general-purpose listing of Autonomous System Numbers (ASNs) and/or pointers to other groupings of ASNs (an 'ASGroup'), for use with the Resource Public Key Infrastructure (RPKI) [RFC6480]. The CMS protected content type is intended to provide for the creation and validation of an RPKI ASGroup, a listing signed by the holder of the private key associated with a particular ASN.

RPKI ASGroups are expected to facilitate inter-domain business use cases that depend on an ability to exchange listings of ASNs. Through the use of RPKI ASGroup Opt-Out Listings, resource holders have a degree of control over what Relying Party (RP) implementations emit in relationship to their AS Identifier resources and ASGroups when expanding ASGroups.

The objective is to offer a RPKI-based successor to plain-text RFC 2622 'as-set' class objects. The main differences between IRR 'as-set' objects and RPKI ASGroups is the robust cryptographically verifiable authorization and the notion of being able to 'opt-out' of an listing (a feature that in the IRR context is not possible).

1.1. 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. ASGroup and ASGroup Opt-Out Listing Profile

ASGroup and ASGroup Opt-Out Listing objects follow the Signed Object Template for the RPKI [RFC6488].

2.1. EE Certificates

The Certification Authority (CA) **MUST** only sign one ASGroup or ASGroup Opt-Out Listing with each EE certificate and **MUST** generate a new key pair for each new ASGroup or ASGroup Opt-Out Listing. This type of EE certificate is termed a "one-time-use" EE certificate (see Section 3 of [RFC6487]).

2.2. Object Filenames

A guideline for naming ASGroup and ASGroup Opt-Out objects is that the file name chosen in the repository be a value derived from the public key of the EE certificate. One such method of generating a publication name is described in Section 2.1 of [RFC4387]; convert the 160-bit hash of a EE's public key value into a 27-character string using a modified form of Base64 encoding, with an additional modification as proposed in Section 5, table 2, of [RFC4648].

3. eContentType

3.1. The ASGroup eContentType

The eContentType for an ASGroup is defined as id-ct-rpkiSignedGrouping, with Object Identifier (OID) 1.2.840.113549.1.9.16.1.TBD.

This OID **MUST** appear within both the eContentType in the encapContentInfo object and the ContentType signed attribute in the signerInfo object (see [RFC6488]).

3.2. The ASGroup Opt-Out Listing eContentType

The eContentType for an ASGroup Opt-Out Listing is defined as id-ct-rpkiSignedGroupingOptOut, with Object Identifier (OID) 1.2.840.113549.1.9.16.1.TBD.

This OID **MUST** appear within both the eContentType in the encapContentInfo object and the ContentType signed attribute in the signerInfo object (see [RFC6488]).

4. eContent

4.1. The ASGroup eContent

The content of an ASGroup indicates a listing of arbitrary ASNs and pointers to other ASGroups which has been signed with a specific Autonomous System identifier. An ASGroup is formally defined as follows:

```
RpkiSignedGrouping-2022
  { iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs9(9) smime(16) mod(0)
    id-mod-rpkiSignedGrouping-2022(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) }

ct-rpkiSignedGrouping CONTENT-TYPE ::=
  { TYPE RpkiSignedGrouping
    IDENTIFIED BY id-ct-rpkiSignedGrouping }

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

RpkiSignedGrouping ::= SEQUENCE {
  version [0]      INTEGER DEFAULT 0,
  asID             ASID,
  label            GroupingLabel (SIZE(1..100)),
  referenceable    BOOLEAN DEFAULT TRUE,
  members          SEQUENCE (SIZE(0..MAX)) OF ASIdOrGroupingPointer }

ASIdOrGroupingPointer ::= CHOICE {
  id               ASID,
  pointer          GroupingPointer }

GroupingPointer ::= SEQUENCE {
  asID             ASID,
  label            GroupingLabel (SIZE(1..100)) }

ASID ::= INTEGER (1..4294967295)

GroupingLabel ::=
  IA5String (FROM("A".."Z" | "0".."9" | ":" | "_" | "-"))

END
```

4.1.1. Version

The version number of the RpkiSignedGrouping **MUST** be 0.

4.1.2. asID

The Autonomous System Number contained here **MUST** be a subset of the set of resources listed by the EE certificate carried in the CMS certificates field.

4.1.3. label

This field contains type GroupingLabel, a IA5String which **MUST** consist of at least one and no more than a hundred characters chosen from the set A-Z (UPPERCASE ALPHABET), 0-9, - (HYPHEN), _ (UNDERSCORE), or : (COLON). The label field serves as a differentiator to allow a resource holder to produce multiple different ASGroup objects carrying the same ASN in the asID field for different purposes. The value of the label field **MUST** adhere to the same naming conventions and constraints as hierarchical 'as-set' set names described in Section 5 of [RFC2622]; noting the first component of the set name is the value of the above asID field.

4.1.4. referenceable

This field is a BOOLEAN. If the referenceable boolean is set to FALSE, a Relying Party (RP) which encounters a GroupingPointer in an ASGroup which matches the asID and label of this ASGroup **MUST** ignore the GroupingPointer. If multiple ASGroup objects exist in the RPKI repositories with the same asID and label, but the referenceable boolean set to different values; the TRUE value takes precedence.

4.1.5. members

This field contains a SEQUENCE of ASIdOrGroupingPointer CHOICE.

4.1.5.1. Choice ASIdOrGroupingPointer

This field contains a CHOICE of either an ASID or a GroupingPointer.

4.1.5.2. Element ASID

This field contains a INTEGER which is a reference to an Autonomous System Number.

4.1.5.3. Element GroupingPointer

This field contains a SEQUENCE which contains an ASID (a reference to an Autonomous System Number) and a GroupingLabel (a IA5String). The asID value and label in a GroupingPointer **SHOULD NOT** match the asID and label in the RpkiSignedGrouping; e.g. an ASGroup **SHOULD NOT** point to itself.

4.2. The ASGroup Opt-Out Listing eContent

The content of an ASGroup Opt-Out Listing indicates an opt-out listing of arbitrary ASNs and pointers to other ASGroups which has been signed with a specific Autonomous System identifier. The purpose of ASGroup Opt-Out Listings is to provide a means to negate references in ASGroup objects (not under control of the resource holder) towards resources held by the resource holder. An ASGroup Opt-Out Listing is formally defined as follows:

```
RpkiSignedGroupingOptOut-2022
  { iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs9(9) smime(16) mod(0)
    id-mod-rpkiSignedGroupingOptOut-2022(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) }

  ASID, ASIdOrGroupingPointer, GroupingLabel
  FROM RpkiSignedGrouping-2022
    { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs9(9) smime(16) mod(0)
      id-mod-rpkiSignedGrouping-2022(TBD) }

ct-rpkiSignedGroupingOptOut CONTENT-TYPE ::=
  { TYPE RpkiSignedGrouping
    IDENTIFIED BY id-ct-rpkiSignedGroupingOptOut }

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

RpkiSignedGroupingOptOut ::= SEQUENCE {
  version [0]      INTEGER DEFAULT 0,
  asID             ASID,
  label            GroupingLabel (SIZE(1..100)) OPTIONAL,
  optOut           SEQUENCE (SIZE(0..MAX)) OF ASIdOrGroupingPointer }

END
```

4.2.1. Version

The version number of the RpkiSignedGroupingOptOut **MUST** be 0.

4.2.2. asID

The Autonomous System Number contained here **MUST** be a subset of the set of resources listed by the EE certificate carried in the CMS certificates field.

4.2.3. label

This optional field contains type GroupingLabel, a IA5String which **MUST** consist of at least one and no more than a hundred characters chosen from the set A-Z (UPPERCASE ALPHABET), 0-9, - (HYPHEN), _ (UNDERSCORE), or : (COLON). If the field is absent, the ASGroup Opt-Out Listing entry is considered to mean that any ASGroup objects referenced in the optOut SEQUENCE containing members entries which reference this object's asID value **MUST** be negated by the RP. if the field is present, any ASGroup objects matching the an entry in the optOut SEQUENCE containing a GroupingPointer which match this ASGroup Opt-Out Listing's asID and label **MUST** be negated.

4.2.4. optOut

This field is a SEQUENCE of ASIdOrGroupingPointer CHOICE entries from which the resource holder wishes to be excluded when expanding ASGroups.

4.2.4.1. asID

If the ASIdOrGroupingPointer CHOICE contains an INTEGER; the meaning is that any references to this RpkiSignedGroupingOptOut's asID in ASGroups matching the asID specified herein **MUST** be negated.

4.2.4.2. GroupingPointer

The GroupingPointer is a SEQUENCE of an ASID and GroupingLabel, and providers a more granular opt-out mechanism than the above mentioned opt-out.

5. ASGroup Validation

Before a Relying Party (RP) can expand an ASGroup into a listing of Autonomous System Numbers, the RP **MUST** first validate all ASGroup Opt-Out Listings to be able to honor opt-Out attestations.

To validate an ASGroup or ASGroup Opt-Out Listings, the RP **MUST** perform all the validation checks specified in [RFC6488]. In addition, the RP **MUST** perform the following validation steps:

1. The contents of the CMS eContent field **MUST** conform to all of the constraints described in Section 4.
2. The Autonomous System Identifier Delegation extension [RFC3779] **MUST** be present in the EE certificate contained in the CMS certificates field.
3. The AS identifier present in the RpkiSignedGrouping eContent 'asID' field respectively RpkiSignedGroupingOptOut eContent 'asID' field **MUST** be a subset of those present in the certificate extension.
4. The EE certificate's Autonomous System Identifier Delegation extension **MUST NOT** contain "inherit" elements.
5. The IP Address Delegation Extension described in [RFC3779] is not used in ASGroup or ASGroup Opt-Out Listings and **MUST NOT** be present.

A list of Validated ASGroup Listings (VALs) is produced by applying a recursive descent to each ASGroup, noting members which are ASIDs and following GroupingPointers. GroupingPointers which point to an ASGroup which has the 'referenceable' boolean set to false **MUST** be ignored. Members of an ASGroup which match an ASGroup Opt-Out Listing entry **MUST** be ignored.

6. Operational Considerations

Multiple ASGroup objects could exist which contain the same asID and label. In such cases the union of members forms the set of members. It is highly **RECOMMENDED** that a compliant CA maintains a single ASGroup for a given (asID, label) tuple.

Multiple ASGroup Opt-Out Listing objects could exist which contain the same asID and label. In such cases the union of optOut entries forms the set of optOut entries. It is highly **RECOMMENDED** that a compliant CA maintains a single ASGroup Opt-Out Listing for a given (asID, label) tuple.

If a CA becomes aware of a match in a valid ASGroup Opt-Out Listing for one of its subordinate ASGroup products; the CA **SHOULD** remove the offending asID or GroupingPointer from the members of the ASGroup and reissue the object.

7. Security Considerations

RPs are hereby warned that the data in an ASGroup is self-asserted. When determining the meaning of any data contained in an ASGroup, RPs **MUST NOT** make any assumptions about the signer beyond the fact that it had sufficient control of the issuing CA to create the object.

While a one-time-use EE certificate must only be used to generate and sign a single ASGroup object, CAs technically are not restricted from generating and signing multiple different ASGroup objects with a single key pair. Any ASGroup objects sharing the same EE certificate cannot be revoked individually.

8. IANA Considerations

8.1. SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)

IANA is requested to allocated the following 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-rpkiSignedGrouping	draft-spaghetti-sidrops-rpki-asgroup
TBD	id-ct-rpkiSignedGroupingOptOut	draft-spaghetti-sidrops-rpki-asgroup

Table 1

8.2. RPKI Signed Objects

IANA is requested to register two OIDs in the "RPKI Signed Objects" registry [RFC6488] as follows:

Name	OID	Reference
Signed ASGroup	1.2.840.113549.1.9.16.1.TBD	draft-spaghetti-sidrops-rpki-asgroup
Signed ASGroup Opt-Out Listing	1.2.840.113549.1.9.16.1.TBD	draft-spaghetti-sidrops-rpki-asgroup

Table 2

8.3. RPKI Repository Name Schemes

IANA is requested to add the Signed ASGroup file extension to the "RPKI Repository Name Schemes" registry [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.grp	Signed ASGroup	

Filename Extension	RPKI Object	Reference
		draft-spaghetti-sidrops-rpki-asgroup
.ool	Signed ASGroup Opt-Out Listing	draft-spaghetti-sidrops-rpki-asgroup

Table 3

8.4. SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)

IANA is requested to allocate the following in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" registry:

Decimal	Description	References
TBD	id-mod-rpkiSignedGrouping-2022	draft-spaghetti-sidrops-rpki-asgroup
TBD	id-mod-rpkiSignedGroupingOptOut-2022	draft-spaghetti-sidrops-rpki-asgroup

Table 4

8.5. Media Types

IANA is requested to register the media types "application/rpki-asgroup" and "application/rpki-asgroupoptout" in the "Media Types" registry as follows:

8.5.1. ASGroup Media Type

Type name: application
Subtype name: rpki-asgroup
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: binary
Security considerations: Carries an RPKI Signed ASGroup. This media type contains no active content. See Section 5 of draft-spaghetti-sidrops-rpki-asgroup for further information.
Interoperability considerations: N/A
Published specification: draft-spaghetti-sidrops-rpki-asgroup
Applications that use this media type: RPKI operators
Fragment identifier considerations: N/A
Additional information:

Content:
This media type is a signed object, as defined in [RFC6488], which contains a payload of a list of checksums as defined in draft-spaghetti-sidrops-rpki-asgroup.
Magic number(s): N/A
File extension(s): .grp

Macintosh file type code(s): N/A

Person & email address to contact for further information: Job Snijders (job@fastly.com)

Intended usage: COMMON

Restrictions on usage: N/A

Author: Job Snijders (job@fastly.com)

Change controller: IETF

8.5.2. ASGroup Opt-Out Listing Media Type

Type name: application

Subtype name: rpki-asgroupoptout

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: binary

Security considerations: Carries an RPKI Signed ASGroup Opt-out. This media type contains no active content. See Section 5 of draft-spaghetti-sidrops-rpki-asgroup for further information.

Interoperability considerations: N/A

Published specification: draft-spaghetti-sidrops-rpki-asgroup

Applications that use this media type: RPKI operators

Fragment identifier considerations: N/A

Additional information:

Content:
This media type is a signed object, as defined in [RFC6488], which contains a payload of an opt-out list as defined in draft-spaghetti-sidrops-rpki-asgroup.

Magic number(s): N/A

File extension(s): .ool

Macintosh file type code(s): N/A

Person & email address to contact for further information: Job Snijders (job@fastly.com)

Intended usage: COMMON

Restrictions on usage: N/A

Author: Job Snijders (job@fastly.com)

Change controller: IETF

9. References

9.1. 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>.

[RFC2622]
Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., Terpstra, M., and RFC Publisher, "Routing Policy Specification Language (RPSL)", RFC 2622, DOI 10.17487/RFC2622, June 1999, <https://www.rfc-editor.org/info/rfc2622>.

[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>.

[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>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <https://www.rfc-editor.org/info/rfc6487>.

[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>.

[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

[RFC4387] Gutmann, P., Ed., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store

Access via HTTP", RFC 4387, DOI 10.17487/RFC4387, February 2006, <https://www.rfc-editor.org/info/rfc4387>.

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

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI 10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/info/rfc6268>.

[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>.

Appendix A. Acknowledgements

The authors wish to thank TBD...

Appendix B. Example payloads

B.1. Example ASGroup eContent Payload

Below an example of a DER encoded ASGroup eContent is provided with annotation following the '#' character. The example is fairly simple; the resource holder managing AS 16509 produced a ASGroup called "AS16509:AS-AMAZON" (asID + ':' + label), which cannot be referenced by other ASGroups, and which has 2 members: AS 16509 and 'AS16509:AS-CUSTOMERS' (the latter being a GroupingPointer).

```
$ echo 302c0202407d160941532d414d415a4f4e01010030180202407d30120202\
407d160c41532d435553544f4d455253 \
| xxd -r -ps \
| openssl asn1parse -inform DER -i
  0:d=0  hl=2 l=  44 cons: SEQUENCE                    # RpkiSignedGroup
  2:d=1  hl=2 l=   2 prim:  INTEGER      :407D         # asID 16509
  6:d=1  hl=2 l=   9 prim:  IA5STRING    :AS-AMAZON    # label
 17:d=1  hl=2 l=   1 prim:  BOOLEAN      :0            # not referenceab
 20:d=1  hl=2 l=  24 cons:  SEQUENCE                   # contains 2 memb
 22:d=2  hl=2 l=   2 prim:   INTEGER     :407D         # AS16509
 26:d=2  hl=2 l=  18 cons:   SEQUENCE                  # GroupingPointer
 28:d=3  hl=2 l=   2 prim:    INTEGER    :407D         #  \
 32:d=3  hl=2 l=  12 prim:    IA5STRING  :AS-CUSTOMERS #  /` AS16509:AS-
```

The 'AS16509:AS-CUSTOMERS' ASGroup object is as following:

```
$ echo 302d0202407d160c41532d435553544f4d455253301902021c380202231b\
0202391a02023cca02024a67020300f541 \
| xxd -r -ps
| openssl asn1parse -inform DER -i
  0:d=0  hl=2 l=  45 cons: SEQUENCE
  2:d=1  hl=2 l=   2 prim:  INTEGER    :407D     # signed by AS16509
  6:d=1  hl=2 l=  12 prim:  IA5STRING  :AS-CUSTOMERS
 20:d=1  hl=2 l=  25 cons:  SEQUENCE
 22:d=2  hl=2 l=   2 prim:   INTEGER    :1C38
 26:d=2  hl=2 l=   2 prim:   INTEGER    :231B
 30:d=2  hl=2 l=   2 prim:   INTEGER    :391A
 34:d=2  hl=2 l=   2 prim:   INTEGER    :3CCA    # AS15562
 38:d=2  hl=2 l=   2 prim:   INTEGER    :4A67
 42:d=2  hl=2 l=   3 prim:   INTEGER    :F541
```

B.2. Example ASGroup Opt-Out Listing eContent Payload

Below an example of a DER encoded ASGroup Opt-Out Listing eContent is provided with annotation following the '#' character. The example is as following: the resource holder managing AS 15562 produced a ASGroup Opt-Out Listing and which has 1 optOut: 'AS16509:AS-CUSTOMERS'. Should ASGroup 'AS16509:AS-CUSTOMERS' (directly or indirectly) contain a reference to AS 15562; a Relying Party should omit 15562 from its output.

```
$ echo 301a02023cca301430120202407d160c41532d435553544f4d455253 \
| xxd -r -ps \
| openssl asn1parse -inform DER -i
  0:d=0  hl=2 l=  26 cons: SEQUENCE                     # RpkiSignedGrou
  2:d=1  hl=2 l=   2 prim:  INTEGER       :3CCA         # produced by AS
  6:d=1  hl=2 l=  20 cons:  SEQUENCE                    # optOut
  8:d=2  hl=2 l=  18 cons:   SEQUENCE                   #   GroupingPoin
 10:d=3  hl=2 l=   2 prim:    INTEGER     :407D         # \
 14:d=3  hl=2 l=  12 prim:    IA5STRING   :AS-CUSTOMERS # /` AS16509:AS-
```

Based on the above 2 ASGroup payloads and 1 ASGroup Opt-Out Listing payload, a compliant validator would emit 7224, 8987, 14618, 16509, 19047, and 62785 when expanding 'AS16509:AS-AMAZON'.

Appendix C. 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".

*Example .grp and .ool files were created by Job Snijders with the use of asn1c and OpenSSL.

Authors' Addresses

Job Snijders
Fastly
Amsterdam
Netherlands

Email: job@fastly.com

Fredrik Korsbäck
Amazon Web Services
Malmskillnadsgatan 36
SE-111 57 Stockholm
Sweden

Email: fkback@amazon.com