Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 17 October 2025

N. Geng
Huawei
K. Sriram
NIST
M. Huang
Zhongguancun Laboratory

15 April 2025

A Profile for Autonomous System Relationship Authorization (ASRA)
draft-geng-sidrops-asra-profile-01

Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for Autonomous System Relationship Authorization (ASRA) objects for use with the Resource Public Key Infrastructure (RPKI). An ASRA is a digitally signed object through which the issuer (the holder of an Autonomous System identifier), can authorize one or more other Autonomous Systems (ASes) as its customers and lateral peers. When validated, an ASRA's eContent can be used for detection and mitigation of BGP AS path manipulation attacks together with Autonomous System Provider Authorization (ASPA). ASRA is complementary to ASPA.

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 17 October 2025.

Table of Contents

1. Introduction

This document defines a Cryptographic Message Syntax (CMS) protected content type for Autonomous System Relationship Authorization (ASRA) objects for use with the Resource Public Key Infrastructure (RPKI) [RFC6480]. An ASRA is a digitally signed object through which the issuer (the holder of an Autonomous System identifier), can authorize one or more other Autonomous Systems (ASes) as its customers and lateral peers. When validated, an ASRA's eContent can be used for

detection and mitigation of BGP AS path manipulation attacks together with Autonomous System Provider Authorization (ASPA) [I-D.ietf-sidrops-aspa-profile] [I-D.ietf-sidrops-aspa-verification]. ASRA-based verification is complementary to ASPA-based verification.

BGP relationships that an Autonomous System (AS) may have with eBGP neighbors are discussed in [I-D.ietf-sidrops-aspa-verification]. ASPA object is used to register the set of provider ASes that the subject (signing) AS has. ASRA object is used to register the set of ASes with which the subject AS has customer and/or lateral peering relationships.

There are three subcategories of ASRAs defined: ASRA1, ASRA2, and ASRA3. 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 has the option to register an ASRA3 to register the combined list of customers and lateral peers. The details of ASRA registration requirements for ASes in different scenarios are specified in Section 3 of [I-D.sriram-sidrops-asra-verification]. In addition, the procedures for verifying AS_PATHs in BGP UPDATE messages using validated ASRA objects (in conjunction with the ASPA objects) are described in that document.

This CMS [RFC5652] protected content type definition conforms to the [RFC6488] template for RPKI signed objects. In accordance with Section 4 of [RFC6488], this document defines:

1. The object identifier (OID) that identifies the ASRA signed object. This OID appears in the eContentType field of the encapContentInfo object as well as the content-type signed attribute within the signerInfo structure.

2. The ASN.1 syntax for the ASRA content, which is the payload signed by the signer (subject) AS. The ASRA content is encoded using the ASN.1 [X.680] Distinguished Encoding Rules (DER) [X.690].

3. The steps required to validate an ASRA beyond the validation steps specified in [RFC6488].

2. ASRA Content Type

The content-type for an ASRA is defined as id-ct-ASRA, which has the numerical value of 1.2.840.113549.1.9.16.1.TBD. This OID MUST appear both within the eContentType in the encapContentInfo structure as well as the content-type signed attribute within the signerInfo structure (see [RFC6488]).

3. ASRA eContent

The content of an ASRA identifies the signer (subject) AS as well as the Set of ASes that are authorized by the signer AS to be its customers and/or lateral peers.

A user registering ASRA(s) must be cognizant of Section 3 of [I-D.sriram-sidrops-asra-verification] and the user (or their software tool) must comply with the ASRA registration recommendations in that section. In the case of the transition process between different CA registries, the ASRA records SHOULD be kept identical in all registries in terms of their authorization contents.

The eContent of an ASRA is an instance of ASRelationshipAttestation, formally defined by the following ASN.1 [X.680] module:

```
RPKI-ASRA-2024
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-9(9) smime(16) modules(0)
        id-mod-rpki-asra-2024(TBD) }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
  CONTENT-TYPE
  FROM CryptographicMessageSyntax-2010  -- RFC 6268
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
       pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) } ;

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

ct-ASRA CONTENT-TYPE ::=
  { TYPE ASRelationshipAttestation IDENTIFIED BY id-ct-ASRA }

ASRelationshipAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  SignerASID  ASID,
  ASRAsubcategory  subcategory,
  Relationships     RelationshipASSet }

ASID ::= INTEGER (0..4294967295)

subcategory ::= OCTET STRING (SIZE (1))

RelationshipASSet ::= SEQUENCE (SIZE(1..MAX)) OF ASID

END
```

Note that this content appears as the eContent within the encapContentInfo as specified in [RFC6488].

3.1. Version

The version number of the ASRelationshipAttestation that complies with this specification MUST be 0 and MUST be explicitly encoded.

3.2. SignerASID

The SignerASID field contains the AS number of the Autonomous System that is the authorizing entity (Signer AS).

3.3. ASRAsubcategory

ASRAsubcategory can have values 0 to 255. The values 1, 2, and 3 are assigned to represent ASRA1, ASRA2, and ASRA3, respectively. As explained in Section 1, ASRA1 means that the Relationships (see Section 3.4) field contains ASIDs of only the customer ASes of the Signer AS; ASRA2 means that the Relationships field contains ASIDs of only the lateral peer ASes; ASRA3 means that the Relationships field contains the combined list of ASIDs of customer and lateral peer ASes. Section 3 of [I-D.sriram-sidrops-asra-verification] for details of registration requirements for ASRA1, ASRA2, and ASRA3.

3.4. Relationships

Each element contained in the Relationships field is an instance of ASID. The Relationships field contains the listing of ASIDs of ASes that are authorized as customers and/or lateral peers (per ASRA1, ASRA2, and ASRA3 subcategory definitions).

In addition to the constraints described by the formal ASN.1 definition, the contents of the Relationships field MUST satisfy the following constraints:

* The SignerASID value MUST NOT appear in any ASID in the Relationships field.

* The elements of Relationships MUST be ordered in ascending numerical order (ASIDs).

* Each value of ASID MUST be unique (with respect to the other elements of Relationships).

4. ASRA Validation

Before a relying party can use an ASRA to validate a routing announcement, the relying party MUST first validate the ASRA object itself. To validate an ASRA, the relying party MUST perform all the validation checks specified in [RFC6488] as well as the following additional ASRA-specific validation steps.

* The Autonomous System Identifier Delegation Extension [RFC3779] MUST be present in the end-entity (EE) certificate (contained within the ASRA), and the SignerASID in the ASRA eContent MUST be contained within the set of AS numbers specified by the EE certificate’s Autonomous System Identifier Delegation Extension.

* The EE certificate’s Autonomous System Identifier Delegation Extension MUST NOT contain any "inherit" elements.

* The IP Address Delegation Extension [RFC3779] MUST be absent.

5. IANA Considerations

5.1. SMI Security for S/MIME Module Identifier registry

Please add the id-mod-rpki-asra-2024 to the SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0) registry (https://www.iana.org/assignments/smi-numbers/smi-numbers.xml#security-smime-0) as follows:

Decimal	Description	Specification
TBD2	id-mod-rpki-asra-2024	[RFC-to-be]

5.2. SMI Security for S/MIME CMS Content Type registry

Please add the ASRA to the SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1) registry (https://www.iana.org/assignments/smi-numbers/smi-numbers.xml#security-smime-1) as follows:

Decimal	Description	Specification
TBD	id-ct-ASRA	[RFC-to-be]

5.3. RPKI Signed Object registry

Please add Autonomous System Relationship Authorization to the RPKI Signed Object registry (https://www.iana.org/assignments/rpki/rpki.xhtml#signed-objects) as follows:

Name	OID	Specification
Autonomous System Relationship Authorization	1.2.840.113549.1.9.16.1.TBD	[RFC-to-be]

5.4. RPKI Repository Name Scheme registry

Please add an item for the Autonomous System Relationship Authorization file extension to the "RPKI Repository Name Scheme" registry created by [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.asa	Autonomous System Relationship Authorization	[RFC-to-be]

5.5. Media Type registry

The IANA is requested to register the media type application/rpki-asra in the "Media Type" registry as follows:

Type name: application
Subtype name: rpki-asra
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: binary
Security considerations: Carries an RPKI ASRA [RFC-to-be].
This media type contains no active content. See
Section xxx of [RFC-to-be] for further information.
Interoperability considerations: None
Published specification: [RFC-to-be]
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 list of
AS identifiers (ASIDs) as defined in [RFC-to-be].
Magic number(s): None
File extension(s): .asa
Macintosh file type code(s):
Person & email address to contact for further information:
Nan Geng <gengnan@huawei.com>
Intended usage: COMMON
Restrictions on usage: None
Change controller: IETF

6. Security Considerations

The security considerations of [RFC6481], [RFC6485], and [RFC6488] also apply to ASRAs.

7. Acknowledgments

The authors would like to thank the authors of [I-D.ietf-sidrops-aspa-profile] since that document was used as a template.

8. References

8.1. Normative References

[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.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.sriram-sidrops-asra-verification]
Sriram, K., Geng, N., and A. Herzberg, "Autonomous System Relationship Authorization (ASRA) as an Extension to ASPA for Enhanced AS Path Verification", Work in Progress, Internet-Draft, draft-sriram-sidrops-asra-verification-01, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-sriram-sidrops-asra-verification-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>.

[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>.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, DOI 10.17487/RFC6485, February 2012, <https://www.rfc-editor.org/info/rfc6485>.

[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>.

[X.680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 2021.

[X.690] ITU-T, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, 2021.

8.2. Informative References

[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>.

[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>.

[RFC7947] Jasinska, E., Hilliard, N., Raszuk, R., and N. Bakker, "Internet Exchange BGP Route Server", RFC 7947, DOI 10.17487/RFC7947, September 2016, <https://www.rfc-editor.org/info/rfc7947>.

Authors' Addresses

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

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

Mingqing Huang
Zhongguancun Laboratory
Beijing
China
Email: huangmq@mail.zgclab.edu.cn