SIDR Operations
Internet-Draft
Intended status: Standards Track
Expires: 12 June 2026

Q. Li
Beijing Zhongguancun Laboratory
K. Xu
Z. Liu
Q. Li
J. Wu
Tsinghua University

9 December 2025

A Profile for Signed Group of Multiple-Origin Autonomous Systems for Use in the Resource Public Key Infrastructure (RPKI)
draft-li-sidrops-rpki-moasgroup-02

Abstract

This document defines a "Signed MOAS Group", a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI) to authenticate the collective announcement of IP prefixes by Multiple Origin Autonomous System (MOAS). The Signed MOAS Group mainly includes two parts: an IP prefix and a list of Autonomous Systems (ASes) authorized to announce the prefix. At least one of these ASes SHOULD be authorized to announce the prefix by the prefix owner through a Route Origin Authorization (ROA). The validation of a Signed MOAS Group confirms that the authorized ASes and other listed ASes have collectively agreed to announce the prefix, ensuring that the announcement is legitimate, accurate, and mutually authorized.

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 12 June 2026.

Table of Contents

1. Introduction

This document defines a "Signed MOAS Group", a Cryptographic Message Syntax (CMS) [RFC5652] protected content type to carry an IP prefix and a list of Autonomous Systems (ASes) authorized to announce this prefix. The Signed MOAS Group allows multiple ASes to collaboratively and securely announce an IP prefix, supporting scenarios such as business partnerships, traffic engineering, and DDoS protection services.

A Signed MOAS Group object mainly consists of two components: an IP prefix and a list of Autonomous Systems (ASes) intended to announce the prefix collaboratively, which allows other RPKI-validating routing entities to audit the collection of announcements from multiple originating AS. At least one AS in the AS list SHOULD be authorized to announce the prefix by the prefix owner through an ROA, which means the IP prefix in the ROA SHOULD match the IP prefix in the Signed MOAS Group and the AS number in the ROA SHOULD appear in the AS list. The object is collectively signed by the listed ASes using a multi-signature technique, and the aggregated global signature is attached to the Signed MOAS Group object, ensuring that the announcement could be legitimately proposed by all participating ASes and is verifiable by any RPKI-validating remote routing entities.

When validating a Signed MoasGroup, a relying party (RP) aggregates the public keys of all ASes in the AS list into a single global public key. This global key is then used to verify the multi-signature of the Signed MoasGroup. There are three possible validation outcomes. First, if the Signed MoasGroup is verified and at least one corresponding ROA is found, it is considered valid. Second, if the Signed MoasGroup is verified but no corresponding ROA is found, it is deemed suspicious. Finally, if the Signed MoasGroup fails verification, it is considered invalid.

The Signed MOAS Group provides a technical way for securely managing multi-origin AS announcements, offering a robust and flexible solution to handle modern routing requirements. Any prefixes announced by ASes that are not included in an ROA or a validated Signed MOAS Group SHOULD be regarded as invalid, though their handling is subject to local routing policies. The intent is to offer a secure and authenticated method for managing MOAS scenarios, enhancing the overall security and integrity of the routing system.

Signed MOAS Group objects follow the Signed Object Template for the RPKI [RFC6488].

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.

3. Signed MoasGroup eContentType

The eContentType for a MoasGroup is defined as id-ct-rpkiSignedMoasGroup, with Object Identifier (OID) 1.2.840.113549.1.9.16.1.TBD. It is encoded using the Cryptographic Message Syntax (CMS). The ASN.1 structures and encoding rules follow the updated CMS modules defined in [RFC5911], consistent with other RPKI signed object profiles.

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

4. Signed MoasGroup eContent

A MoasGroup is formally defined as follows:

```
   RpkiSignedMoasGroup-2024
     { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs9(9) smime(16) mod(0)
      id-mod-rpkiSignedMoasGroup-2024(TBD) }

      DEFINITIONS EXPLICIT TAGS ::=
   BEGIN

   IMPORTS
     CONTENT-TYPE, DigestAlgorithmIdentifier, Digest
     FROM CryptographicMessageSyntax-2009 -- in [RFC5911]
     { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs-9(9) smime(16) modules(0) id-mod-cms-2004-02(41) }

     ASId, IPAddressFamily
     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-rpkiSignedMoasGroup CONTENT-TYPE ::=
     { TYPE RpkiSignedMoasGroup
      IDENTIFIED BY id-ct-rpkiSignedMoasGroup }

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

     RpkiSignedMoasGroup ::= SEQUENCE {
      smgo SignedMoasGroupObject,
      digestAlgorithm DigestAlgorithmIdentifier,
      objectDigest Digest
     }

     SignedMoasGroupObject ::= SEQUENCE {
      version [0]          INTEGER DEFAULT 0,
      ipAddressPrefix      IPAddressFamily,
      asList               SEQUENCE (SIZE(0..MAX)) OF ASId,
     }

   END
```

4.1. version

The version number of the RpkiSignedMoasGroup MUST be 0.

4.2. ipAddressPrefix

The ipAddressPrefix field follows the IP address and Autonomous System Identifier extension semantics defined in [RFC3779]. This field contains an IPAddressFamily which contains one instance of addressFamily and one instance of prefix.

4.3. asList

This field contains the AS numbers that are intended to originate routes to the given IP address prefixes. The AS numbers that are authorized by ROA SHOULD be put in front of other AS numbers. The AS numbers MUST NOT duplicate.

4.4. digestAlgorithm

The digest algorithm used to create the message digest of the attested digital object. This algorithm MUST be a hashing algorithm defined in [RFC7935].

4.5. messageDigest

The message digest of the SignedMoasGroupObject using the algorithm specified in the digestAlgorithm field.

4.6. attestation

The attestation is a CMS detached signature in the SignedData format as defined in [RFC5485]. Each AS listed in the asList signs an individual digital signature of the message digest, and one AS aggregates all individual signatures into a global signature, referred to as the attestation.

5. Issuance of Signed MoasGroup

It is highly RECOMMENDED that the AS initiating the Signed MOAS Group object be authorized by the prefix owner via an ROA. This AS, referred to as the authorized AS, then initiates the creation of the Signed MOAS Group object, selects a digest algorithm, and calculates the digest of the Signed MOAS Group object. The authorized AS shares this Signed MOAS Group object with other ASes listed in the object. Each listed AS (including the authorized AS) signs the digest using its private key and returns the signature to the authorized AS. Upon receiving and verifying all individual signatures, the authorized AS aggregates them into a global signature, i.e. the attestation, and attaches it to the Signed MOAS Group object. After that, the prefix owner MAY verify the Signed MOAS Group. Finally, the prefix owner or the authorized AS uploads the Signed MOAS Group to the RPKI

repositories for validation and distribution.

6. Validation of Signed MoasGroup

To validate a Signed MoasGroup, the relying party 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 RP MUST verify the attestation of the Signed MOAS Group. This process involves two steps: first, aggregating the public keys of all ASes listed in the AS list to form a global public key; second, using this aggregated global public key to verify the attestation attached to the Signed MOAS Group object.

3. The RP MUST check for the existence of a corresponding ROA for the IP prefix in the Signed MOAS Group. The IP prefix in the ROA MUST match the IP prefix in the Signed MOAS Group, and the AS number in the ROA MUST appear in the AS list.

A Signed MOAS Group has three possible validation results. (1) Valid: If the Signed MOAS Group is verified and at least one corresponding ROA is found, it is considered valid. (2) Suspicious: If the Signed MOAS Group is verified but no corresponding ROA is found, the Signed MOAS Group is considered suspicious. (3) Invalid: If the Signed MOAS Group cannot be verified, it is considered invalid.

7. Operational Considerations

To aggregate the signatures efficiently, the Signed MOAS Group SHOULD use BLS Signatures with BLS12-381 elliptic curve [I-D.draft-ietf-cose-bls-key-representations-05].

ROA-authorized ASes SHOULD be placed at the beginning of the AS list to improve RP validation efficiency. It is highly RECOMMENDED that the RP only verifies the first AS and the prefix against the ROA.

Multiple valid Signed MOAS Group objects may exist for the same IP prefix. However, it is highly RECOMMENDED that an AS participate in only one Signed MOAS Group for a given IP prefix. If changes to the AS list are needed, it is highly RECOMMENDED to revoke the existing Signed MOAS Group and issue a new one.

8. Security Considerations

Although it is highly RECOMMENDED that a Signed MOAS Group SHOULD be validated by at least one ROA, the data contained in a Signed MOAS Group is still self-asserted by the group of AS holders. This means that the presence of an AS in the Signed MOAS Group does not inherently imply any authority from the IP prefix holder for the AS to originate a route for any prefixes. Such authority is separately conveyed in the RPKI through an ROA.

9. IANA Considerations

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

IANA is requested to allocate the following in the "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" registry:

Decimal	Description	Reference
TBD	Id-ct-rpkiSignedMoasGroup	draft-li-sidrops-rpki-moasgroup

Table 1

9.2. RPKI Signed Objects

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

Name	OID	Reference
Signed MoasGroup	1.2.840.113549.1.9.16.1.TBD	draft-li-sidrops-rpki-moasgroup

Table 2

9.3. RPKI Repository Name Schemes

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

Filename Extension	RPKI Object	Reference
.smg	Signed MoasGroup	draft-li-sidrops-rpki-moasgroup

Table 3

9.4. 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	Reference
.TBD	id-mod-rpkiSignedMoasGroup-2024	draft-li-sidrops-rpki-moasgroup

Table 4

10. References

10.1. Normative References

[I-D.draft-ietf-cose-bls-key-representations-05]
Looker, T. and M. B. Jones, "Barreto-Lynn-Scott Elliptic Curve Key Representations for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-bls-key-representations-05, 17 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-bls-key-representations-05>.

[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/rfc/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/rfc/rfc3779>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/rfc6488>.

[RFC7935] Huston, G. and G. Michaelson, Ed., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure", RFC 7935, DOI 10.17487/RFC7935, August 2016, <https://www.rfc-editor.org/rfc/rfc7935>.

[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/rfc/rfc8174>.

10.2. Informative References

[RFC5485] Housley, R., "Digital Signatures on Internet-Draft Documents", RFC 5485, DOI 10.17487/RFC5485, March 2009, <https://www.rfc-editor.org/rfc/rfc5485>.

[RFC5911] Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, DOI 10.17487/RFC5911, June 2010, <https://www.rfc-editor.org/rfc/rfc5911>.

Acknowledgments

The authors would like to thank Shenglin Jiang, Yangfei Guo, Xingang Shi, Shuhe Wang, Xiaoliang Wang, Hui Wang, and Di Ma.

Authors' Addresses

Qi Li
Beijing Zhongguancun Laboratory
Beijing
China
Email: li-q25@mails.tsinghua.edu.cn

Ke Xu
Tsinghua University
Beijing
China
Email: xuke@tsinghua.edu.cn

Zhuotao Liu
Tsinghua University
Beijing
China
Email: zhuotaoliu@tsinghua.edu.cn

Qi Li
Tsinghua University
Beijing
China
Email: qli01@tsinghua.edu.cn

Jianping Wu
Tsinghua University
Beijing
China
Email: jianping@cernet.edu.cn