Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 January 2026

C. Xie
G. Dong
China Telecom
X. Li
CERNET Center/Tsinghua University
G. Huston
APNIC
D. Ma
ZDNS

19 July 2025

A Profile for Mapping Origin Authorizations (MOAs)
draft-ietf-sidrops-moa-profile-02

Abstract

This document proposes a new approach by leveraging Resource Public Key Infrastructure (RPKI) architecture to verify the authenticity of the mapping origin of an IPv4 address block. MOA is a newly defined cryptographically signed object, it provides a means that the address holder can authorize an IPv6 mapping prefix to originate mapping for one or more IPv4 prefixes. When receiving the MOA objects from the relying partie, PE device can verify and discard invalid address mapping announcements from unauthorized IPv6 mapping prefixes to prevent IPv4 prefix hijacking.

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
2. Terminology, Abbreviations and Acronyms 3
3. The MOA Content-Type 4
4. The MOA eContent 4
4.1. Element version 5
4.2. Element mappings 5
4.2.1. type MOAIPMapping 5
5. MOA Validation 6
6. Security Considerations 6
7. IANA Considerations 7
8. Acknowledgement 7
9. References 7
9.1. Normative References 7
9.2. Informative References 8
Appendix A. ASN.1 Module 9
Authors' Addresses 10

1. Introduction

This document defines security enhancement for the address mapping announcement in multi-domain IPv6-only underlay networks [I-D.ietf-v6ops-framework-md-ipv6only-underlay]. For IPv4 service delivery in IPv6-only network, IPv6 mapping prefixes are configured at the PE devices to identify the location of IPv4 address blocks, for any given IPv4 address block, its corresponding IPv6 mapping prefix is considered as the mapping origin. In [I-D.ietf-idr-mpbgp-extension-4map6], PE device at the edge of the IPv6-only network distributes the mapping between an IPv4 address block and its mapping origin through 4map6 extension of MP-BGP. Based on the obtained mapping data, the ingress PE can statelessly transform the incoming IPv4 packets into IPv6 ones and send them to the correct egress PE.

From above it can be seen that the correctness of transmitting IPv4 service data in an IPv6-only network lies on the authenticity of the address mapping relationship. This can be further explained by the

case where if an attacker maps an IPv4 address block using a fake IPv6 mapping prefix, IPv4 service data will be sent to the wrong egress PE, resulting in a situation of IPv4 prefix hijacking. In a small-scale controlled network, this problem may not be too serious. However, as the scale of IPv6-only deployment increases and there is interconnection between multiple operators, it is necessary to guarantee the authenticity of mapping relationship. This document proposes a new approach by leveraging Resource Public Key Infrastructure (RPKI) architecture to verify the authenticity of the mapping origin of an IPv4 address block. RPKI is a security framework by which network owners can validate and secure the critical route update or BGP announcements between public Internet networks [RFC6480]. For the scenario discussed, a new object, namely Mapping Origin Authorization (MOA), under the RPKI framework is defined in this document. MOA is a cryptographically signed mapping object between an IPv4 address block and its right mapping origin that is allowed to be declared in the announcement of MP-BGP. With this architecture, a legitimate holder of IPv4 address block, e.g. an ISP, can authorize an IPv6 mapping prefix to map IPv4 address block. A distributed repository system stores and disseminates the data objects that comprise the RPKI, as well as other signed objects necessary for improved mapping data and routing security. When receiving MOA objects from the relying parties, the PE routers can use them for Mapping Origin Validation (MOV) of IPv4 address blocks: verifying and discarding "invalid" address mapping announcements to prevent IPv4 prefix hijacking in an IPv6 network.

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. Terminology, Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

CMS: Cryptographic Message Syntax

MOA: Mapping Origin Authorization

MOV: Mapping Origin Validation

MP-BGP: Multiprotocol BGP

PE: Provider Edge

PKI: Public Key Infrastructure

RPKI: Resource Public Key Infrastructure

ROA: Route Origin Authorization([RFC9582])

3. The MOA Content-Type

The content-type for a MOA is defined as MappingOriginAuthz and has the numerical value of x.x.xxx.xxxxx.x.x.x.x.xx.

This OID MUST appear both within the eContentType in the encapContentInfo object as well as the content-type signed attribute in the signerInfo object (see [RFC6488]).

4. The MOA eContent

The content of a MOA identifies a single IPv6 mapping prefix that has been authorized by the address holder to originate mapping of one or more IPv4 prefixes that will be advertised. If the address holderneeds to authorize multiple IPv6 mapping prefixes to advertise the same set of IPv4 prefixes, the holder issues multiple MOAs, one per IPv6 mapping prefix. A MOA is formally defined as:

```
MappingOriginAttestation ::= SEQUENCE {

    version [0] INTEGER DEFAULT 0,

    mappings SEQUENCE (SIZE(1..MAX)) OF MOAIPMapping }


MOAIPMapping ::= SEQUENCE {

    v6MappingPrefix IPv6MappingPrefix,

    v4Prefixes SEQUENCE (SIZE(1..MAX)) OF IPv4Prefix }


IPv6MappingPrefix ::= BIT STRING (SIZE (0..ub-IPv6))


IPv4Prefix ::= BIT STRING (SIZE (0..ub-IPv4))


ub-IPv6 INTEGER ::= 128


ub-IPv4 INTEGER ::= 32
```

Note that this content appears as the eContent within the encapContentInfo (see [RFC6488]).

4.1. Element version

The version number of the MappingOriginAttestation MUST be xxx.

4.2. Element mappings

The mappings element encodes the set of address mapping behavior, which indicates that the given IPv6 Mapping Prefix is authorized to originate mappings for single or a set of IPv4 prefixes.

4.2.1. type MOAIPMapping

Within the MOAIPMapping structure, v6MappingPrefix element contains the IPv6 prefix used to originate mapping for a set of IPv4 prefixes. The length of v6MappingPrefix can be set as 40, 48, 56, 64 or 96 in actual deployment. The v4Prefixes element represents IPv4 prefixes as a sequence of IPv4Prefix.

It is proposed to define a canonical ordering for v4Prefixes, this allows RP software to more easily verify the contents of the eContent. In section 3.3.2 of [I-D.ietf-sidrops-rpki-prefixlist], a canonical form is defined such that every set of IPv4 address prefixes has a unique representation. it can be used for the case of MOA defined in this document.

To semantically compare, sort, and deduplicate the contents of the v4Prefix field, each v4Prefix element is mapped to an abstract data element composed of two integer values:

addr

The first IPv4 address of the IPv4 prefix appearing in the v4Prefix field, as a 32-bit (IPv4) integer value.

plen

The prefix length of the IPv4 prefix appearing in the v4Prefix address field as an integer value.

Thus, the equality or relative order of two v4Prefix elements can be tested by comparing their abstract representations.

With comparator the set of v4Prefix is totally ordered. The order of two v4Prefixes is determined by the first non-equal comparison in the following list.

1. Data elements with a lower addr value precede data elements with a higher addr value.

2. Data elements with a lower plen value precede data elements with a higher plen value.

Data elements for which all two values compare equal are duplicates of one another.

5. MOA Validation

Before a relying party can use a MOA to validate a mapping announcement received, the relying party MUST first validate the MOA. To validate a MOA, the relying party MUST perform all the validation checks specified in [RFC6488] as well as the following additional MOA-specific validation step.

-The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the MOA), and each IPv4 prefix(es) in the MOA is contained within the set of IP addresses specified by the EE certificate’ s IP address delegation extension.

6. Security Considerations

There is no assumption of confidentiality for the data in a MOA; it is anticipated that MOAs will be stored in repositories that are accessible to all ISPs, and perhaps to all Internet users. There is no explicit authentication associated with a MOA, since the PKI used for MOA validation provides authorization but not authentication.

Although the MOA is a signed, application-layer object, there is no intent to convey non-repudiation via a MOA.

The purpose of a MOA is to convey authorization for an IPv6 mapping prefix to originate a mapping to the prefix(es) in the MOA. Thus, the integrity of a MOA MUST be established. The MOA specification makes use of the RPKI signed object format; thus, all security considerations in [RFC6448] also apply to MOAs. Additionally, the signed object profile uses the CMS signed message format for integrity; thus, MOAs inherit all security considerations associated with that data structure.

The right of the MOA signer to authorize the target IPv6 mapping prefix to originate mappings to the prefix(es) is established through use of the address space and IPv6 mapping prefix number PKI described in [RFC6480]. Specifically, one MUST verify the signature on the MOA using an X.509 certificate issued under this PKI, and check that the prefix(es) in the ROA match those in the certificate's address space extension.

As mentioned in [I-D.ietf-idr-mpbgp-extension-4map6], the 4map6 extension is mainly used for controlled IPv6-only network operated by single or multiple ISPs. In this scenario, as the IPv6 mapping prefix indicates the direction of IPv4 service data transmission in the IPv6-only network, and MOA is used to validate the mapping origin of IPv4 address block, there is no need to use IPv4 ROA for the validation of IPv4 BGP announcements; On the other hand, as the operation of MOA depends on the authenticity of address authorization in the underlying IPv6 network, if the IPv6 address prefix is maliciously originated by a third-party AS, even if the IPv4 address block is legitimately authorized to its corresponding IPv6 mapping prefix, traffic hijacking may occur due to the malicious announcement of the IPv6 mapping prefix. Therefore, it is recommended to also deploy IPv6 ROA validation where MOA is deployed.

7. IANA Considerations

With this document, IANA is requested to allocate the code for MOA in the registry of "RPKI Signed Objects". In addition, two OIDs need to be assigned by IANA, one for the module identifier, and another one for the content type. The codes will use this document as the reference.

8. Acknowledgement

The authors would like to express sincere thanks to Russ Housley and Job Snijders for their review, suggestions and contributions. Thanks are also given to Nan Geng, Lancheng Qin, Jie Dong, Linda Dunba, Jiankang Yao, Sriram Kotikalapudi, Giuseppe Fioccola, Yu Fu, Shunwan Zhuang, Aijun Wang, Shengnan Yue and Cong Li for their review and comments

9. References

9.1. Normative References

[I-D.ietf-sidrops-rpki-prefixlist]
Snijders, J. and G. Huston, "A profile for Signed Prefix Lists for Use in the Resource Public Key Infrastructure (RPKI)", Work in Progress, Internet-Draft, draft-ietf-

sidrops-rpki-prefixlist-04, 16 September 2024,
<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-rpki-prefixlist-04>.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC6448] Yount, R., "The Unencrypted Form of Kerberos 5 KRB-CRED Message", RFC 6448, DOI 10.17487/RFC6448, November 2011, <https://www.rfc-editor.org/info/rfc6448>.

[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>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

9.2. Informative References

[I-D.ietf-idr-mpbgp-extension-4map6]
Xie, C., Dong, G., Li, X., Han, G., and Z. Guo, "MP-BGP Extension and the Procedures for IPv4/IPv6 Mapping Advertisement", Work in Progress, Internet-Draft, draft-ietf-idr-mpbgp-extension-4map6-04, 14 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-mpbgp-extension-4map6-04>.

[I-D.ietf-v6ops-framework-md-ipv6only-underlay]
Xie, C., Ma, C., Li, X., Mishra, G. S., and T. Graf, "Framework of Multi-domain IPv6-only Underlay Network and IPv4-as-a-Service", Work in Progress, Internet-Draft, draft-ietf-v6ops-framework-md-ipv6only-underlay-11, 30 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-framework-md-ipv6only-underlay-11>.

[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. ASN.1 Module

This normative appendix provides an ASN.1 module that specifies the MOA content in ASN.1 syntax.

```
RPKIMappingOriginAuthz-2024

    {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)

      pkcs9(9) smime(16) mod(0) TBD0 }


DEFINITIONS EXPLICIT TAGS ::= BEGIN


IMPORTS

    CONTENT-TYPE

    FROM CryptographicMessageSyntax-2009--in [RFC5911]

        { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)

          pkcs9(9) smime(16) modules(0) id-mod-cms-2004-02(41) };


ct-MappingOriginAuthz CONTENT-TYPE ::=
```

```
    { TYPE MappingOriginAttestation
      IDENTIFIED BY id-ct-MappingOriginAuthz }

   id-ct-MappingOriginAuthz OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs9(9)smime(16) ct(1) TBD1 }

   MappingOriginAttestation ::= SEQUENCE {
       version [0] INTEGER DEFAULT 0,
       mappings SEQUENCE (SIZE(1..MAX)) OF MOAIPMapping }

   MOAIPMapping ::= SEQUENCE {
       v6MappingPrefix IPv6MappingPrefix,
       v4Prefixes SEQUENCE (SIZE(1..MAX)) OF IPv4Prefix }

   IPv6MappingPrefix ::= BIT STRING (SIZE (0..ub-IPv6))

   IPv4Prefix ::= BIT STRING (SIZE (0..ub-IPv4))

   ub-IPv6 INTEGER ::= 128

   ub-IPv4 INTEGER ::= 32

   END
```

Authors' Addresses

Chongfeng Xie
China Telecom
Beiqijia Town, Changping District
Beijing
102209
China
Email: xiechf@chinatelecom.cn

Guozhen Dong
China Telecom
Beiqijia Town, Changping District
Beijing
102209
China
Email: donggz@chinatelecom.cn

Xing Li
CERNET Center/Tsinghua University
Shuangqing Road No.30, Haidian District
Beijing
100084
China
Email: xing@cernet.edu.cn

Geoff Huston
APNIC
Email: gih@apnic.net

Di Ma
ZDNS
Floor 21, Block B, Greenland Center
Beijing
100102
China
Email: madi@zdns.cn