A Profile for Mapping Origin Authorizations (MOAs)

Chongfeng Xie	China Telecom
Guozhen Dong	China Telecom
Xing Li	CERNET Center/Tsinghua University
Geoff Huston	APNIC
Di Ma	ZDNS

sidrops@IETF 125，Mar. 2026

Overview

- MOA is an RPKI object for the verification of the address mapping announcement in IPv6-only networks, its goal it to ensures that IPv4 service data is transmitted to the correct egress.

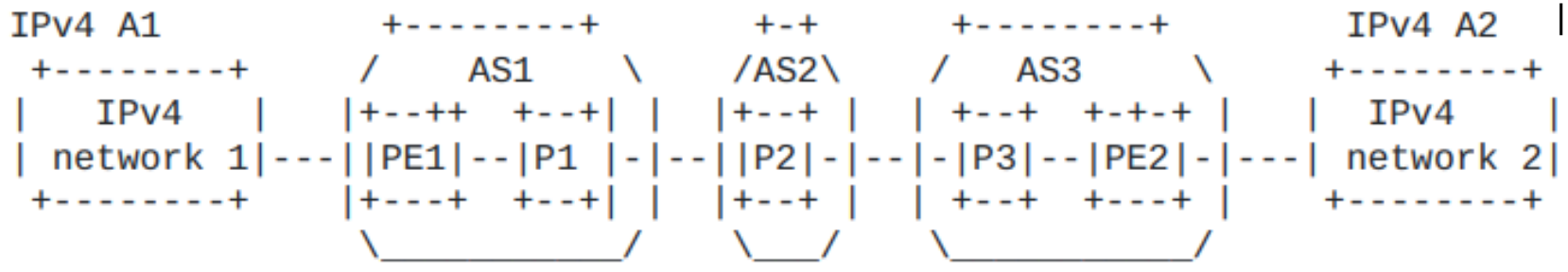
- It was adopted by SIDROPS WG October 2024 , the current version is -03.

Scenario

- For IPv4 service delivery in IPv6-only network(proposed in [*draft-ietf-v6ops-framework-md-ipv6only-underlay*]), IPv6 mapping prefixes are configured at the PE to identify the location of each IPv4 network. So IPv6 mapping prefix is considered as the **mapping origin** of given IPv4 address block.

IPv4 address block

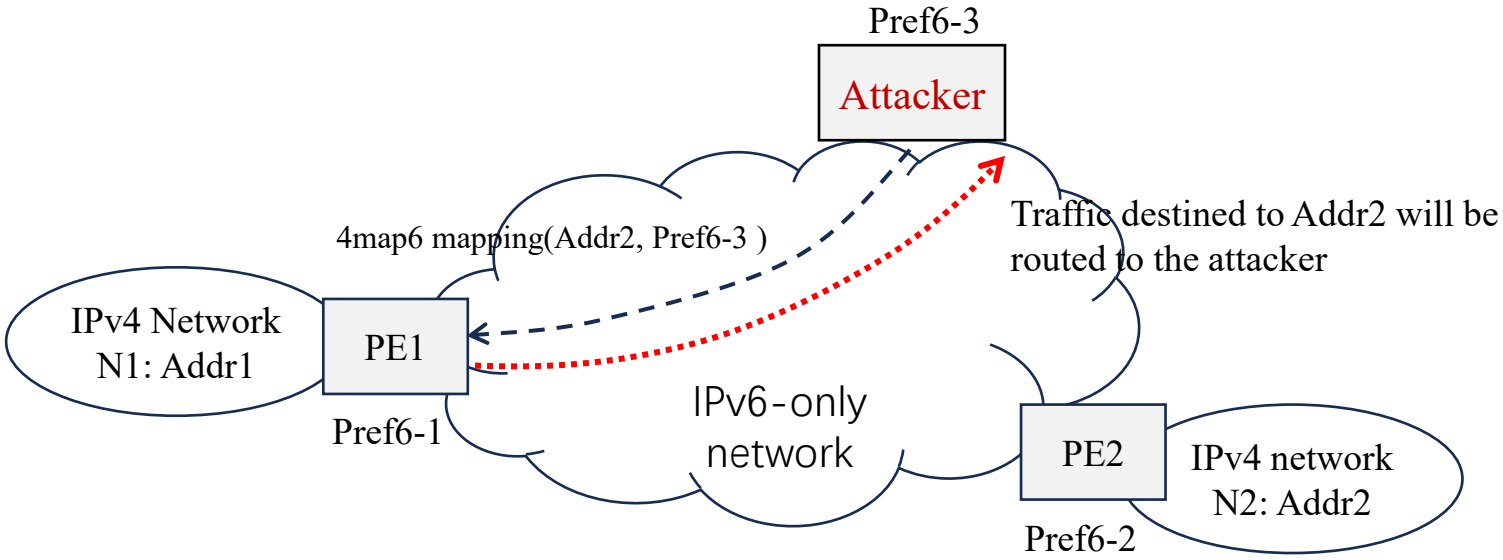
IPv6 mapping prefix



- [*draft-ietf-idr-mpbgp-extension-4map6*] defines MP-BGP extension, i.e. 4map6, for announcing the mapping relation from egress PE to ingress PE.

Problem statement

- The validity of transmitting IPv4 service data in IPv6-only underlay network relies on the authenticity of the mapping origin of the IPv4 address block.
- If an attacker maps an IPv4 address block using a fake IPv6 mapping prefix, IPv4 service data will be routed through the attacker-controlled route and reach to the wrong egress PE, resulting in a situation of IPv4 prefix hijacking.



MOA：Mapping Origin Authorizations

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.

➢MOA Definition

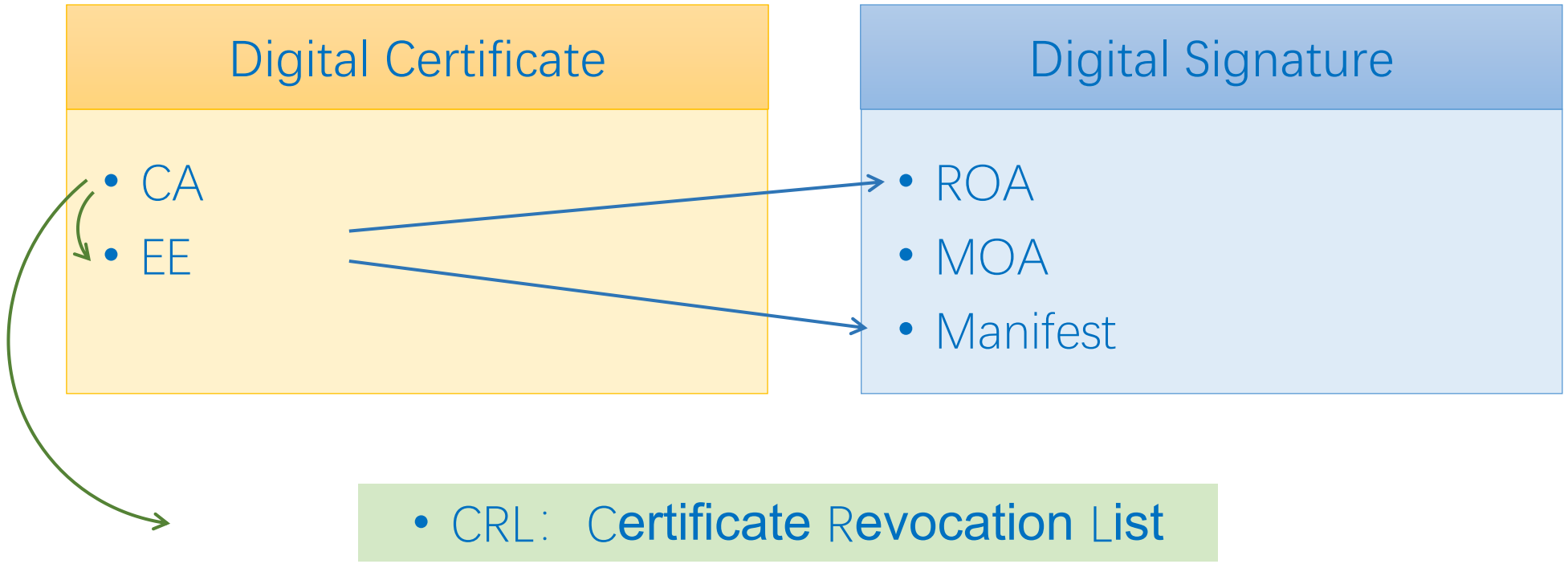
MOA is a cryptographic signature object that allows address holders to authorize IPv6 prefixes for IPv4 prefix mapping..

➢MOA Validation

Routers validate IPv6-to-IPv4 mapping announcements using MOA objects, reject unauthorized ones, and prevent IPv4 prefix hijacking.

```
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
```

MOA Digital Signature Object



MOA Validation

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

MOA Issuance

- **Capability to Issue MOA Digitally Signed Objects on the CA side**

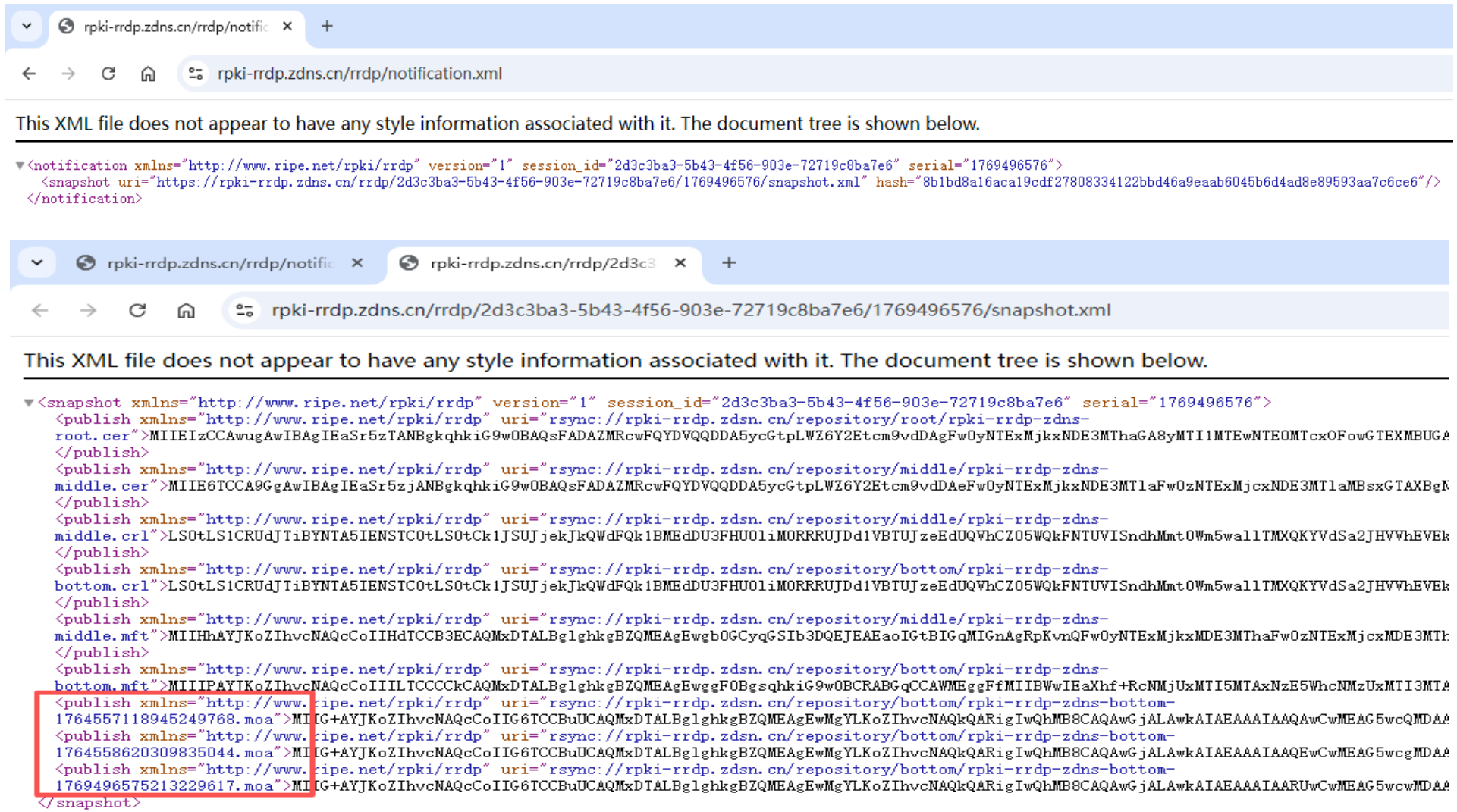
```
ContentInfo SEQUENCE (2 elem)
  contentType ContentType OBJECT IDENTIFIER 1.2.840.113549.1.7.2 signedData (PKCS #7)
  content [0] (1 elem)
    SignedData SEQUENCE (5 elem)
      version CMSVersion INTEGER 3
      digestAlgorithms DigestAlgorithmIdentifiers SET (1 elem)
        DigestAlgorithmIdentifier SEQUENCE (1 elem)
          algorithm OBJECT IDENTIFIER 2.16.840.1.101.3.4.2.1 sha-256 (NIST Algorithm)
      encapContentInfo EncapsulatedContentInfo SEQUENCE (2 elem)
        eContentType ContentType OBJECT IDENTIFIER 1.2.840.113549.1.9.16.1.24 routeOriginAttest (S/MIME Content Types)
        eContent [0] (1 elem)
          OCTET STRING (33 byte) 301F020100301A300B0309002001000020001003 00B0304006E70710303000A01
            SEQUENCE (2 elem)
              INTEGER 0
              SEQUENCE (2 elem)
                SEQUENCE (1 elem)
                  BIT STRING (64 bit) 0010000000000001000000000000000000000001000000000000000001000000 0
                SEQUENCE (2 elem)
                  BIT STRING (24 bit) 011011100111000001110001
                  BIT STRING (16 bit) 0000101000000001
```

V6MappingPrefix: "2001:0:200:100::/64“

V4Prefixes: {"110.112.113.0/24", "10.1.0.0/16"}

MOA Publication

- Capability to Publish MOA Digitally Signed Objects via the RRDP on the CA side



MOA Synchronization and Validation

- Capability to Synchronize and Validate MOA Certificates on the RP side

```
[root@Lab-Test-22 bottom]# pwd
/root/rpki/data/rrdprepo/rpki-rrdp.zdns.cn/repository/bottom
[root@Lab-Test-22 bottom]# ll
total 20
-rw-r--r-- 1 root root 1788 Mar  2 16:55 rpki-rrdp-zdns-bottom-1764557118945249768.moa
-rw-r--r-- 1 root root 1788 Mar  2 16:55 rpki-rrdp-zdns-bottom-1764558620309835044.moa
-rw-r--r-- 1 root root 1788 Mar  2 16:55 rpki-rrdp-zdns-bottom-1769496575213229617.moa
-rw-r--r-- 1 root root  556 Mar  2 16:55 rpki-rrdp-zdns-bottom.crl
-rw-r--r-- 1 root root 2112 Mar  2 16:55 rpki-rrdp-zdns-bottom.mft
```

```
[root@Lab-Test-22 bin]# ./rpstir2.sh exportmoas | jq .
[
  {
    "ipv6MappingPrefix": "2001:0:200:100::/64",
    "ipv4Prefixes": [
      "110.112.113.0/24",
      "10.1.0.0/16"
    ]
  },
  {
    "ipv6MappingPrefix": "2001:0:200:101::/64",
    "ipv4Prefixes": [
      "110.112.114.0/24",
      "10.2.0.0/16"
    ]
  }
]
```

Next Step

- The MOA Protocol Data Unit (PDU) for the RPKI-RTR protocol will be defined in new document.
- Router vendors will implement support for MOA.
- The MOA will undergo demonstration testing and verification.
- The draft is stable, should we ask for a last call?

Thank you !
Q&A