Workgroup:	Network Working Group		
Internet-Draft:	draft-qin-sidrops-toa-00		
Published:	28 November 2024		
Intended Status:	Standards Track		
Expires:	1 June 2025		
Authors:	L. Qin	B. Maddison	D. Li
	Zhongguancun Laboratory	*Workonline*	*Tsinghua University*

A Profile for Traffic Origin Authorizations (TOAs)

Abstract

This document defines a standard profile for Traffic Origin Authorizations (TOAs), a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI). A TOA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate traffic using source IP addresses within the address block.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 8174 [RFC8174].

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 1 June 2025.

Copyright Notice

Table of Contents

1. Introduction

Source address validation (SAV) requires verifying that an AS has been authorized to originate traffic using one or more prefixes as the source IP address. A Traffic Origin Authorization (TOA) provides this function.

The TOA makes use of the template for RPKI digitally signed object [RFC6488], which defines a Cryptographic Message Syntax (CMS) wrapper [RFC5652] for a generic validation procedure for RPKI signed objects. Therefore, to complete the specification of the TOA (see Section 4 of [RFC6488]), this document defines:

- The OID that identifies the signed object as being a TOA. (This OID appears within the eContentType in the encapContentInfo object as well as the content-type signed attribute in the signerInfo object.)
- The ASN.1 syntax for the TOA eContent. (This is the payload that specifies the ASes being authorized to originate traffic as well as the prefixes that the ASes may use as the source IP address.) The TOA eContent is ASN.1 encoded using the Distinguished Encoding Rules (DER) [X.690].
- Additional steps required to validate TOAs (in addition to the validation steps specified in [RFC6488]).

The content of a TOA identifies a list of one or more ASes that have been authorized by the IP address block holder to originate traffic and a list of one or more IP address prefixes within the address block that will be used as the source IP address. The TOA and the ROA [RFC9582] have different intentions and contents because prefixes used as the source IP address in traffic (which is contained in TOAs) and prefixes advertised into the routing system (which is contained in ROAs) can be different and asymmetric for the same AS. In addition, many ROAs include allocated but not advertised prefixes, but these prefixes will not be used as the source IP address in traffic.

The IP address block holder can register one or more TOAs to authorize which ASes can originate traffic using specific prefixes within the block as the source IP address. By registering TOAs, IP address block holders can protect their source IP addresses from being forged by attackers inside unauthorized ASes. ISP or enterprise AS operators can use TOAs to improve the accuracy and robustness of SAV (see Section 6 for details).

2. The TOA Content Type

The content-type for a TOA is defined as id-ct-trafficOriginAuthz and has the numerical value of 1.2.840.113549.1.9.16.1.TBD.

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

3. The TOA eContent

The content of a TOA identifies a list of one or more ASes that have been authorized by the address block holder to originate traffic and a list of one or more IP address prefixes within the address block that will be used as the source IP address. A TOA is formally defined as:

```
RPKI-TOA-2024
     { iso(1) member-body(2) us(840) rsadsi(113549)
       pkcs(1) pkcs9(9) smime(16) mod(0)
       id-mod-rpkiTOA-2024(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-trafficOriginAuthz CONTENT-TYPE ::=
  { TYPE TrafficOriginAttestation
    IDENTIFIED BY id-ct-trafficOriginAuthz }

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

TrafficOriginAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  asSet          ASSet,
  ipaddrBlocks  SEQUENCE (SIZE(1..2)) OF TOAIPAddressFamily }

ASSet ::= SEQUENCE (SIZE(1..10000)) OF ASID
ASID ::= INTEGER (0..4294967295)

SOURCE-ADDRESS-FAMILY ::= CLASS {
     &afi              OCTET STRING (SIZE(2)) UNIQUE,
     &Addresses
   } WITH SYNTAX { AFI &afi ADDRESSES &Addresses }

TOAIPAddressFamily ::= SEQUENCE {
  sourceAddressFamily  SOURCE-ADDRESS-FAMILY.&afi ({SourceAddressFamilySet}),
  sourceAddresses      SOURCE-ADDRESS-FAMILY.&Addresses
                                          ({SourceAddressFamilySet}
{@sourceAddressFamily}) }

SourceAddressFamilySet SOURCE-ADDRESS-FAMILY ::=
  { sourceAddressFamilyIPv4 | sourceAddressFamilyIPv6 }

sourceAddressFamilyIPv4 SOURCE-ADDRESS-FAMILY ::=
  { AFI afi-IPv4 ADDRESSES TOAAddressesIPv4 }

SourceAddressFamilyIPv6 SOURCE-ADDRESS-FAMILY ::=
  { AFI afi-IPv6 ADDRESSES TOAAddressesIPv6 }

afi-IPv4 OCTET STRING ::= '0001'H

afi-IPv6 OCTET STRING ::= '0002'H

TOAAddressesIPv4 ::= SEQUENCE (SIZE(1..MAX)) OF TOAIPAddress{ub-IPv4}

TOAAddressesIPv6 ::= SEQUENCE (SIZE(1..MAX)) OF TOAIPAddress{ub-IPv6}
```

```
ub-IPv4 INTEGER ::= 32

ub-IPv6 INTEGER ::= 128

TOAIPAddress {INTEGER: ub} ::= BIT STRING (SIZE(0..ub))

END
```

3.1. The version Element

The version number of the TrafficOriginAttestation entry MUST be 0.

3.2. The asSet Element

The asSet element contains a set of AS numbers that are authorized to originate traffic using source IP addresses within the given IP address prefixes.

3.3. The ipaddrBlocks Element

The ipaddrBlocks element encodes the set of IP address prefixes that the AS is authorized to use as the source IP address when originating traffic.

3.3.1. Type TOAIPAddressFamily

Within the TOAIPAddressFamily structure, the sourceAddressFamily element contains the Address Family Identifier (AFI) of an IP address family. Each sourceAddressFamily MUST be either 0001 or 0002.

The sourceAddresses field contains IP prefixes as a sequence of TOAIPAddress.

3.3.2. TOAIPAddress

This element is of type BIT STRING and represents a single IP address prefix [RFC3779].

4. TOA Validation

To validate a TOA, the Relying Party (RP) MUST perform all the validation checks specified in [RFC6488] as well as the following additional specific validation steps:

- The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the TOA), and every IP address prefix in the TOA payload is contained within the set of IP addresses specified by the EE certificate's IP address delegation extension.
- The EE certificate's IP address delegation extension MUST NOT contain "inherit" elements as described in [RFC3779].
- The Autonomous System identifier delegation extension described in [RFC3779] is not used in TOAs and MUST NOT be present in the EE certificate.
- The TOA content fully conforms with all requirements specified in Sections 2 and 3.

If any of the above checks fail, the TOA MUST be considered invalid and an error SHOULD be logged.

5. Security Considerations

The security considerations of [RFC6481], [RFC6485], [RFC6488], and [RFC9582] also apply to the TOA object.

6. Enhancing SAV with TOAs

Recent SAV mechanisms (e.g., EFP-uRPF [RFC8704], BAR-SAV [draft-ietf-sidrops-bar-sav], Bicone SAV [draft-li-sidrops-bicone-sav]) typically use BGP data, ROAs, or IRR route objects to identify the legitimate source IP address space of traffic coming from an adjacent AS. However, due to the asymmetry between prefixes used as the source IP address and prefixes advertised into the routing system as well as the impact of allocated but not advertised prefixes (as mentioned in Section 1), using BGP data, ROAs, and IRR route objects to perform SAV will have false positives (i.e., blocking legitimate data packets) and false negatives (i.e., permitting spoofing data packets).

By using TOAs, SAV can accurately identify whether an AS is authorized to use a specific source IP address to originate traffic. If an AS originates spoofinig traffic using a source IP address authorized to other ASes in TOAs, TOA-based SAV can identify and discard this spoofing traffic. Therefore, it is highly recommended to improve the accuracy and robustness upon current SAV by using TOAs.

7. IANA Considerations

7.1. RPKI Signed Objects Registry

Please add an item for the TOA file extension to the RPKI Signed Object registry (https://www.iana.org/assignments/rpki/rpki.xhtml#signed-objects) as follows:

Name	OID	Reference
Traffic Origin Authorization	1.2.840.113549.1.9.16.1.TBD	draft-qin-sidrops-toa

Table 1

7.2. File Extension

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

Filename Extension	RPKI Object	Reference
.toa	Traffic Origin Authorization	draft-qin-sidrops-toa

Table 2

7.3. 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-rpkiTOA-2024	draft-qin-sidrops-toa

Table 3

7.4. Media Type Registry

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

```
Type name: application
Subtype name: rpki-toa
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: binary
Security considerations: Carries an RPKI TOA. This media type contains no
active content.
                         See Section 5 of draft-qin-sidrops-toa for further
information.
Interoperability considerations: None
Published specification: draft-qin-sidrops-toa
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 prefixes and an AS identifier as defined in
draft-qin-sidrops-toa.
Magic number(s): None
File extension(s): .toa
Macintosh file type code(s): None
Person & email address to contact for further information:
  Lancheng Qin <qinlc@mail.zgclab.edu.cn>
Intended usage: COMMON
Restrictions on usage: None
Change controller: IETF
```

8. References

8.1. Normative References

[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>.

[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>.

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

8.2. Informative References

[draft-ietf-sidrops-bar-sav] "Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)", 2024.

[draft-li-sidrops-bicone-sav] "Bicone Source Address Validation", 2024.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

Authors' Addresses

Lancheng Qin
Zhongguancun Laboratory
Beijing
China
Email: qinlc@mail.zgclab.edu.cn

Ben Maddison
Workonline
Cape Town
South Africa
Email: benm@workonline.africa

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn