Workgroup: SIDR Operations
Internet-Draft: draft-qin-sidrops-sispi-00
Published: 23 October 2024
Intended Status: Standards Track
Expires: 26 April 2025

Author: L. Qin
Zhongguancun Laboratory

TOA

A Profile for Signed Source Address List (SiSAL)

Abstract

This document defines a "Signed Source Address List (SiSAL)", a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI). A SiSAL is a digitally signed object which carries the complete list of IP addresses/prefixes that an Autonomous System (the subject AS) may use as the source IP address of its data packets. When validated, the eContent of a SiSAL object confirms that the holder of the subject AS produced the object, and that this list is an accurate description of IP addresses/prefixes that may be used as the source IP address of data packets generated by the subject AS.

who
way
shou

ASN
prefix

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 26 April 2025.

Copyright Notice

Table of Contents

1. Introduction

← Discuss Semantics / ops consideration

This document defines a "Signed Source Address List (SiSAL)", a Cryptographic Message Syntax (CMS) protected content type to carry the complete list of IP addresses/prefixes that an Autonomous System (the subject AS) may use as the source IP address of its data packets. The content is signed by the holder of the RPKI private key associated with the subject AS.

Although the SiSAL object and the ROA ~~Signed Prefix List~~ object [draft-ietf-sidrops-rpki-prefixlist]. both contain a single ASN (the subject AS) and a list of IP address prefixes, the intent of the SiSAL object is completely different from that of the Signed Prefix List object. The list of IP address prefixes in the SiSAL object specifies the addresses that may be used as the source IP address of data packets generated by the subject AS, while the list of IP address prefixes in the Signed Prefix List object specifies the prefixes that may be announced into the routing system originated by the subject AS. The IP address prefix lists of the two objects are different things.

The SiSAL object provides important and useful information for Source Address Validation (SAV). Existing SAV solutions (e.g., EFP-uRPF [RFC8704], BAR-SAV, Bicone SAV) need to know the maximal set of source IP addresses that an AS may use in its data packets. Currently, these solutions usually use BGP UPDATE, ROA, or IRR Route Object to learn this information. However, prefixes announced into the routing system and prefixes used as the source IP address in data packets may not be the same. Therefore, a dedicated object for SAV is needed.

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. The Signed Source Address List ContentType

The content-type for a SiSAL object is defined as id-ct-rpkiSiSAL, 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 ContentType signed attribute within the signerInfo structure (see [RFC6488]).

3. The Signed Source Address List eContent

The content of a SiSAL object is a single ? ASN and a list of IP addresses/prefixes. The eContent of a SiSAL object is an instance of SignedSourceAddressList, formally defined by the following ASN.1 [X.680] module:

```
RpkiSiSAL-2024
      { iso(1) member-body(2) us(840) rsadsi(113549)
        pkcs(1) pkcs9(9) smime(16) mod(0)
        id-mod-rpkiSiSAL-2024-2024(TBD0) }

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-rpkiSiSAL CONTENT-TYPE ::=
  { TYPE SignedSourceAddressList IDENTIFIED BY id-ct-rpkiSiSAL }

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

SignedSourceAddressList ::= SEQUENCE {
  version [0]   INTEGER (0..MAX) DEFAULT 0,
                                                long
  asID          INTEGER (0..4294967295),
  addressBlocks  SEQUENCE OF SourceAddressFamilySourceAddressPrefixes }

SourceAddressFamilySourceAddressPrefixes ::= SEQUENCE {
  SourceAddressFamily     SOURCE-ADDRESS-FAMILY.&afi
({SourceAddressFamilySet}),
  SourceAddressPrefixes SOURCE-ADDRESS-FAMILY.&Prefixes
({SourceAddressFamilySet}{@SourceAddressFamily}) }

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

SourceAddressFamilySet SOURCE-ADDRESS-FAMILY ::= { SourceAddressFamilyIPv4 |
SourceAddressFamilyIPv6 }

SourceAddressFamilyIPv4 SOURCE-ADDRESS-FAMILY ::= { AFI afi-IPv4 PREFIXES
IPv4Prefixes }

SourceAddressFamilyIPv6 SOURCE-ADDRESS-FAMILY ::= { AFI afi-IPv6 PREFIXES
IPv6Prefixes }

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

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

IPv4Prefixes ::= SEQUENCE (SIZE(1..MAX)) OF SourceAddressPrefix{ub-IPv4}

IPv6Prefixes ::= SEQUENCE (SIZE(1..MAX)) OF SourceAddressPrefix{ub-IPv6}

ub-IPv4 INTEGER ::= 32

ub-IPv6 INTEGER ::= 128
```

```
SourceAddressPrefix {INTEGER: ub} ::= BIT STRING (SIZE(0..ub))
END
```

3.1. version

The version number of the SignedSourceAddressList that compiles with this specification **MUST** be 0 and (**MUST** be explicitly encoded.) NO!

(SIZE 1..MAX)

?

3.2. asID → AS set? SEQ OF INT (0...$2^{32}-1$)

This field contains the Autonomous System Number of the Subject AS.

3.3. addressBlocks

This field contains a SEQUENCE of SourceAddressFamilySourceAddressPrefixes.

Each AFI may appear 0-1 times

3.3.1. Element SourceAddressFamilySourceAddressPrefixes ← too long

This field contains a SEQUENCE which contains one instance of SourceAddressFamily and one instance of SourceAddressPrefixes.

3.3.1.1. SourceAddressFamily

This field contains an OCTET STRING which is either '0001'H (IPv4) or '0002'H (IPv6).

3.3.1.2. SourceAddressPrefixes

This field contains a SEQUENCE of SourceAddressPrefix instances. of the corresponding AFI

3.3.1.3. Element SourceAddressPrefix

This element is length bounded through the Information Object Class SOURCE-ADDRESS-FAMILY and its type is a BIT STRING.

Yuk!

4. Signed Source Address List Validation

To validate a SiSAL object, the relying party (RP) **MUST** perform all the validation checks specified in [RFC6488] as well as the following additional specific validation steps:

- The contents of the CMS eContent field **MUST** adhere to all the constraints described in Section 2.
- The AS Identifier Delegation Extension [RFC3779] **MUST** be present in the end-entity (EE) certificate (contained within the SiSAL object), and the asID in the SiSAL object eContent **MUST** be contained within the set of AS numbers specified by the EE certificate's AS Identifier Delegation Extension.

IP Addrs Extn.

- The EE certificate's AS Identifier Delegation Extension **MUST NOT** contain any "inherit" elements.

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

5. IANA Considerations

5.1. RPKI Signed Object Registry

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

```
Name                                | OID                         |
Reference
------------------------------------------------------------------------
-------------------------
Signed Source Address List | 1.2.840.113549.1.9.16.1.TBD | draft-qin-sidrops-
sisal
```

5.2. RPKI Repository Name Scheme Registry

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

```
Filename
Extension | RPKI Object                  | Reference
---------------------------------------------------------------------
   .sisal   | Signed Source Address List | draft-qin-sidrops-sisal
```

?
3 letters!

5.3. 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-rpkiSiSAL-2024 | draft-qin-sidrops-sisal
```

5.4. Media Type Registry

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

```
Type name: application
Subtype name: rpki-sisal
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: binary
Security considerations: Carries Signed Source Address List.
  This media type contains no active content. See
  Section 4 of draft-qin-sidrops-sisal for further information.
Interoperability considerations: N/A
Published specification: draft-qin-sidrops-sisal
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 list of IP addresses/prefixes
      as defined in draft-qin-sidrops-sisal.
Magic number(s): N/A
File extension(s): .sisal
Macintosh file type code(s):
Person & email address to contact for further information:
Lancheng Qin <qinlc@mail.zgclab.edu.cn>
Intended usage: COMMON
Restrictions on usage: N/A
Change controller: IETF
```

6. Security Considerations

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

— Operational —

7. Acknowledgement

8. References

8.1. Normative References

[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>.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI 10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/rfc/rfc6268>.

[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>.

[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/rfc/rfc6485>.

[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>.

[X.680] "Information technology - Abstract Syntax Notation One (ASN.1)&#59; Specification of basic notation", 2021.

[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>.

[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>.

8.2. Informative References

[draft-ietf-sidrops-rpki-prefixlist] "A profile for Signed Prefix Lists for Use in the Resource Public Key Infrastructure (RPKI)", 2024, <https://datatracker.ietf.org/doc/draft-ietf-sidrops-rpki-prefixlist/>.

Author's Address

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