SIDROPS
Internet-Draft
Intended status: Informational
Expires: 28 June 2026

G. Ren
M.L. Jia
X. Yin
S. Liu
Tsinghua University

25 December 2025

A Profile for Source Origin Authorizations(SOAs)
draft-ren-sidrops-soa-profile-01

Abstract

This document defines Source Origin Authorization (SOA), a new object in the Resource Public Key Infrastructure (RPKI), designed to extend RPKI's capabilities to securing the data plane. An SOA object is a digitally signed artifact that records information about the possible last-hop ASes traversed by packets before reaching a specific AS. By providing this information, the SOA enables other ASes to collaboratively filter traffic with spoofed source addresses claiming to originate from the IP space of the target AS, thereby enhancing global Internet security through mitigation of source address spoofing and DDoS attacks.

Table of Contents

1. Introduction

Source Address Validation (SAV) is essential for Internet security, ensuring that packets carry legitimate and verifiable source addresses and preventing spoofed traffic.

Existing SAV solutions, such as IEF[RFC2827] and uRPF[RFC3704][RFC8704], face deployment challenges due to their "self-deployment, global benefit" nature. Moreover, methods relying solely on local routing information suffer from two key limitations:

1. Spoofed traffic may already consume network resources before being filtered.

2. Reflection attacks can make spoofed packets appear legitimate by the time they reach the victim, rendering local SAV ineffective.

To address these issues, *inter-AS collaboration* is critical. Sharing routing information enables upstream ASes to help with validation and early filtering, reducing spoofed traffic's impact.

However, building trust and coordination among ASes is difficult, with key barriers being:

* The challenge of discovering and trusting peer ASes.

* The lack of effective mechanisms to express and enforce unilateral security needs.

A *centralized, standardized platform* is needed to support trust management and service discovery. The Resource Public Key Infrastructure (RPKI), as a global, open system, is well-suited to this role.

RPKI enables ASes to exchange verified routing data and coordinate source address validation, improving protection against spoofed and reflection-based attacks, reducing DoS risk, and enhancing network resilience.

While RPKI primarily supports routing security, it can also secure the data plane. A key component of SAV is determining the valid ingress direction for traffic from a given AS. The SOA (Source Origin Authorization) framework addresses this need.

The SOA object leverages RPKI to record the last-hop AS before reaching a destination AS, facilitating source address filtering and validation.

An SOA is generated by the source AS seeking protection and used by the AS responsible for enforcing SAV. For detailed procedures, see [I-D.ren-sidrops-soa-usage].

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

This section defines the key terms used in this document.

Source Address Protection Service (SAPS): Refers to a service in which one AS (service provider) deploys source validation rules on its border routers to protect the IP addresses belonging to another AS (service subscriber) from being spoofed. To further explain, the service provider filters those packets whose source addresses are spoofed to be the IP addresses belonging to the service subscriber.

IP Spoofing: A malicious attacker forges the source IP address, setting it to the target IP to conduct network attacks. Such packets may generate DDoS attack traffic against the target IP via reflection nodes or result in the target IP being incorrectly attributed as the source of malicious activity. Thus, IP spoofing serves as a precursor to network attacks or misattribution.

Service Subscriber: In the context of the Source Address Protection Service, this refers to the AS that requests the service and is being protected.

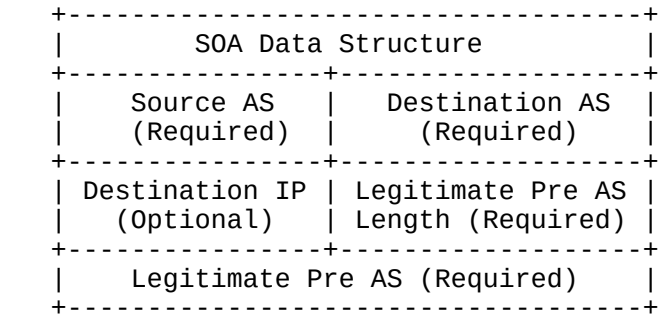
Service Provider: In the context of the Source Address Protection Service, this refers to the AS that provides the service and protects other ASes.

3. SOA Content-Type

The content-type for an SOA is defined as sourceOriginAuthz and has the numerical value of xxxxx. 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. SOA eContent

The content of an SOA identifies a single AS that has been authorized by the ASN holder to originate packets with IP address of this ASN as their source addresses. If the ASN holder needs to authorize multiple ASes to originate packets from the same AS, the holder issues multiple SOAs, one per AS number. An SOA has the following data structure:



And an SOA is formally defined as:

```
SourceOriginAttestation ::= SEQUENCE {
    srcAS          ASID,
    dstAS          ASID,
    dstIP          IPPrefix OPTIONAL,
    legitimatePreASLength INTEGER,
    legitimatePreASList    SEQUENCE (SIZE (1..MAX)) OF ASID
}

ASID ::= INTEGER

IPPrefix ::= SEQUENCE {
    address IPAddress,
    netmask INTEGER}

IPAddress ::= BIT STRING
```

5. SOA Validation

Before a service provider can use SOA to validate the authenticity of source addresses, the SOA must first be verified. To verify an SOA, a trusted party must perform all validation checks specified in [RFC6488].

6. Operation Considerations

Both service providers and service subscribers should make efforts to minimize the synchronization delay between their router configurations and SOA objects to ensure the effectiveness of source address validation. For service subscribers, they should implement both periodic and event-triggered update strategies: SOA objects should be updated after a defined period of time and whenever there are changes to their routing policies. For service providers, they should implement either periodic polling or change-detection mechanisms to promptly identify SOA updates and update their filtering rules accordingly.

According to our study, the effectiveness of deploying SOA is positively correlated with the AS Rank of the deployment location, even without any prior assumption about the target of the attack traffic. Therefore, if there is no specific defensive objective, the scheme should be deployed on top-ranked ASes.

In addition, if, during actual network operation, a large amount of attack traffic is observed originating from a specific reflection point, it may indicate a reflection amplification attack using that node. In this case, SOA should be deployed in the AS where the reflection point resides.

7. IANA Considerations

With this document, IANA is requested to allocate the code for SOA 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. Security Considerations

Data in SOA is not assumed to be confidential; it is anticipated that SOAs will be stored in repositories accessible to all ISPs and potentially all Internet users. SOA does not have explicit authentication associated with it, as the PKI (Public Key Infrastructure) used for SOA validation provides authorization but not authentication. Although SOA is a signed application-layer object, there is no intent to convey non-repudiation through it.

The purpose of SOA is to convey authorization for an ASto originate traffic with source addresses from the prefixes specified in the SOA. Therefore, the integrity of SOA must be established. The SOA specification uses the RPKI (Resource Public Key Infrastructure) signed object format; thus, all security considerations discussed in [RFC6488] also apply to SOAs. Additionally, the signed object profile uses the CMS (Cryptographic Message Syntax) signed message format for integrity, so SOAs inherit all security considerations associated with this data structure.

The right of the SOA signer to authorize the target AS to originate traffic from IP addresses associated with the ASN in the SOA is established through the use of ROA objects within RPKI. In other words, SOA does not directly store the mapping between ASN and IP prefixes; this relationship is derived from ROAs. When using SOA, one must verify the validity of both the SOA and all ROAs associated with the AS, and integrate the information from both to generate and deploy filtering rules.

It is worth noting that the comprehensiveness of ROA coverage for an AS’s IP addresses does not critically affect SOA’s functionality. Specifically, IP addresses not covered by ROAs will not be filtered when traffic originates from them; instead, these addresses retain the same vulnerability as they would have without SOA deployment, meaning they could potentially be spoofed by other ASes.

For this reason, we strongly recommend that ASes deploying SOA fully cover their own IP addresses with ROAs. This ensures that these addresses can be properly protected under the SOA framework.

Looking to the future, if Traffic Origin Authorization (TOA)[I-D.qin-savnet-toa] is standardized and deployed, it should be used directly as a supplement to or replacement for ROAs when implementing SOA. TOA is expected to provide higher accuracy in verifying traffic origins compared to ROAs, which would further enhance the effectiveness of source address validation under the SOA framework.

9. References

9.1. Normative References

[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>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[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>.

[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>.

9.2. Informative References

[I-D.ren-sidrops-soa-usage]
Ren, G., Jia, M., Yin, X., and S. Liu, "Source Address Validation Using Source Origin Authorizations (SOAs)", Work in Progress, Internet-Draft, draft-ren-sidrops-soa-usage-02, 25 December 2025, <https://datatracker.ietf.org/doc/html/draft-ren-sidrops-soa-usage-02>.

[I-D.qin-savnet-toa]
Qin, L., Maddison, B., Li, D., and I. Lubashev, "A Profile for Traffic Origin Authorizations (TOAs)", Work in Progress, Internet-Draft, draft-qin-savnet-toa-00, 3 November 2025, <https://datatracker.ietf.org/doc/html/draft-qin-savnet-toa-00>.

Authors' Addresses

Gang Ren
Tsinghua University
Beijing
China
Email: rengang@cernet.edu.cn

Minglin Jia
Tsinghua University
Beijing
China
Phone: +86 18800137573
Email: jml20@mails.tsinghua.edu.cn, millionvoid@gmail.com

Xia Yin
Tsinghua University
Beijing
China
Email: yxia@tsinghua.edu.cn

Shuqi Liu
Tsinghua University
Beijing
China
Email: liu-sq23@mails.tsinghua.edu.cn, liushuq2001@gmail.com