SIDROPS
Internet-Draft
Intended status: Standards Track
Expires: 14 August 2026

S. Ling
Zhongguancun Lab
K. Xu
Q. Li
Z. Liu
Tsinghua University
X. Wang
Capital Normal University

10 February 2026

A Profile for ROV Deployment Transparency
draft-ling-sidrops-rov-tag-profile-01

Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for ROV Deployment Transparency (ROV_TAG) objects for use with the Resource Public Key Infrastructure (RPKI). An ROV_TAG is a digitally signed object through which an Autonomous System (AS) that has deployed Route Origin Validation (ROV) can declare its ROV deployment status. When validated, an ROV_TAG's eContent can be used by ASes to identify which ASes have deployed ROV, enabling path selection decisions when hijacked routes are detected (see Section 3).

Table of Contents

1. Introduction

Route Origin Validation (ROV) [RFC6811] is a critical security mechanism for BGP routing that uses the Resource Public Key Infrastructure (RPKI) to verify the legitimacy of route announcements. However, ROV deployment is currently partial, with a significant portion of ASes not yet having deployed ROV.

In partial ROV deployment scenarios, the main security concern is:

When an AS has deployed ROV and performs ROV validation, it may detect a hijacked route announcement that was propagated by an upstream AS. This indicates that the upstream AS has not deployed

ROV or is not properly performing ROV validation. If the AS continues using paths through that upstream AS, its traffic may be hijacked. However, the AS cannot determine which alternative paths go through upstream ASes that have deployed ROV, making it difficult to make informed path selection decisions to avoid the compromised upstream AS.

This document defines a profile for ROV Deployment Transparency (ROV_TAG) objects that allows ASes to register their ROV deployment status in RPKI. This provides transparency about which ASes have deployed ROV. When an AS detects a hijacked route announcement from an upstream AS, it can use ROV_TAG information to identify alternative paths where the immediate upstream AS has deployed ROV, enabling it to avoid paths through upstream ASes that have propagated hijacked routes (see Section 3).

This CMS [RFC5652] protected content type definition conforms to the [RFC6488] template for RPKI signed objects. This document defines the object identifier (OID), ASN.1 syntax, and validation steps for ROV_TAG objects.

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.

1.2. Terminology

This document uses the following terminology:

* *Origin AS*: The Autonomous System (AS) that originates a BGP route announcement. The Origin AS is defined as the last AS in the AS_PATH attribute of the BGP route announcement, as specified in [RFC4271].

* *Non-origin AS*: Any AS in the AS_PATH of a BGP route announcement that is not the Origin AS. In an AS_PATH containing multiple ASes, all ASes except the last one (the Origin AS) are non-origin ASes.

2. The ROV_TAG

2.1. The ROV_TAG Content Type

The content-type for an ROV_TAG is defined as id-ct-ROVTAG, 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 content-type signed attribute within the signerInfo structure (see [RFC6488]).

2.2. The ROV_TAG eContent

The content of an ROV_TAG identifies the AS that has deployed ROV.

The eContent of an ROV_TAG is an instance of ROVDeploymentAttestation, formally defined by the following ASN.1 module:

```
RPKI-ROV-TAG-2026
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-9(9) smime(16) modules(0) id-mod-rpki-rov-tag-2026(TBD) }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
  CONTENT-TYPE
  FROM CryptographicMessageSyntax-2010  -- RFC 6268
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
       pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) } ;

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

ct-ROVTAG CONTENT-TYPE ::=
  { TYPE ROVDeploymentAttestation IDENTIFIED BY id-ct-ROVTAG }

ROVDeploymentAttestation ::= SEQUENCE {
  version        [0] INTEGER DEFAULT 0,
  asID           ASID,
  rovDeployed    BOOLEAN }

ASID ::= INTEGER (0..4294967295)

END
```

Note that this content appears as the eContent within the encapContentInfo as specified in [RFC6488].

2.3. version

The version number of the ROVDeploymentAttestation that complies with this specification MUST be 0 and MUST be explicitly encoded.

2.4. asID

The asID field contains the AS number of the Autonomous System that is declaring its ROV deployment status.

2.5. rovDeployed

The rovDeployed field is a BOOLEAN that indicates whether the AS has deployed ROV. Since only ASes that have deployed ROV register ROV_TAG objects, this field MUST be set to TRUE.

For ASes that provide transit services (i.e., ASes that forward traffic for other ASes) that have deployed ROV, it is RECOMMENDED that they register an ROV_TAG object with rovDeployed set to TRUE. Stub ASes (end networks, content providers, etc. that do not provide transit services) are NOT RECOMMENDED to register ROV_TAG objects, as they typically appear as Origin ASes in BGP route announcements.

2.6. ROV_TAG Validation

To validate an ROV_TAG, a relying party MUST perform all the validation checks specified in [RFC6488] as well as the following additional ROV_TAG-specific validation steps:

* The Autonomous System Identifier Delegation Extension [RFC3779] MUST be present in the end-entity (EE) certificate contained within the ROV_TAG. The asID in the ROV_TAG eContent MUST match the ASId specified by the EE certificate’s Autonomous System Identifier Delegation Extension.

* The Autonomous System Identifier Delegation Extension MUST contain exactly one "id" element (Section 3.2.3.6 of [RFC3779]) and MUST NOT contain any "inherit" elements (Section 3.2.3.3 of [RFC3779]) or "range" elements (Section 3.2.3.7 of [RFC3779]).

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

* The rovDeployed field MUST be present and MUST be set to TRUE. Since only ASes that have deployed ROV register ROV_TAG objects, this field MUST always be TRUE.

If any of the above checks fail, the ROV_TAG in its entirety MUST be considered invalid and an error SHOULD be logged.

3. Use Case: Secure Path Selection

In partial ROV deployment scenarios, when an AS filters a hijacked route announcement received from an upstream AS through ROV validation, this indicates that the upstream AS has accepted and propagated the hijacked route. This may occur because the upstream AS has not deployed ROV or is not properly performing ROV validation. In this situation, the AS SHOULD avoid using paths through that upstream AS for traffic destined to the affected prefix.

This use case describes a defensive mechanism that is triggered when an AS detects a security problem. Specifically:

1. The AS performs ROV validation and detects a hijacked route announcement.

2. The AS identifies that the hijacked route was propagated by an upstream AS (the immediate upstream AS).

3. The AS recognizes that *the current path it is using also goes through this same immediate upstream AS* that propagated the hijacked route.

4. *At this point*, if the AS continues using the current path through that upstream AS, the data plane traffic will go through the hijacked upstream AS, leading to the same hijacking.

5. As a defensive measure, the AS can use ROV_TAG information obtained from its RPKI Relying Party (RP) to identify alternative paths from the BGP route announcements it has already received. An alternative path is one where the immediate upstream AS has deployed ROV (i.e., has registered an ROV_TAG object with rovDeployed set to TRUE).

6. The AS checks the ROV deployment status of upstream ASes in the AS_PATH of received route announcements against the ROV_TAG information. If such alternative paths exist, the AS MAY prefer them over the path through the upstream AS that propagated the hijacked route.

This approach is based on the following reasoning:

* If an upstream AS has deployed ROV, it will filter invalid route announcements and will not propagate hijacked routes.

* If an upstream AS has deployed ROV, it may also implement secure path selection (i.e., avoid paths through upstream ASes that have propagated hijacked route announcements when it detects such

announcements). This creates a mechanism where ASes can prefer paths through upstream ASes that have deployed ROV. The logic is straightforward: if an AS detects that an upstream AS has propagated a hijacked route announcement (by filtering it through ROV validation), it SHOULD select an alternative secure path. Conversely, if no hijacked route announcements are detected from an upstream AS, that upstream AS is considered secure, and there is no need to select an alternative path.

* Therefore, if an alternative path exists where the immediate upstream AS has deployed ROV, that path is more likely to be secure from that point forward, reducing the risk that traffic will be hijacked.

The decision to use alternative paths is a matter of local policy. An AS MAY:

* Continue using normal BGP path selection when no hijacked route announcements are detected.

* When an AS filters a hijacked route announcement received from an upstream AS, consider alternative paths (where the immediate upstream AS has deployed ROV) as a defensive measure to avoid the path through the upstream AS that propagated the hijacked route. This defensive measure is triggered only when a security problem is detected.

* Fall back to normal BGP path selection if no alternative paths with ROV-deployed upstream ASes are available.

This addresses the security vulnerability problem by enabling ASes to avoid paths through upstream ASes that have propagated hijacked routes. Such paths are identified through ROV validation. When alternative secure paths are available, this reduces the risk of route hijacking even in partial ROV deployment scenarios.

Note: This is a heuristic defensive mechanism and does not provide cryptographic security guarantees. The use of alternative paths is OPTIONAL and subject to local policy.

4. Operational Considerations

This section discusses operational aspects of ROV_TAG deployment and usage.

4.1. Querying ROV_TAG Information

ROV_TAG objects are stored in the RPKI repository alongside other RPKI objects (e.g., ROAs, ASPAs). Relying Parties (RPs) process ROV_TAG objects as part of their standard RPKI repository synchronization and validation procedures, as specified in [RFC6488].

ASes obtain ROV_TAG information from their RPKI Relying Party (RP) (e.g., through RPKI-to-Router protocols such as [RFC6810] or [RFC8210]). ASes can query this information efficiently to determine whether upstream ASes have deployed ROV. Real-time queries to the RPKI repository or RP are not required during BGP path selection.

4.2. Performance Considerations

The number of ASes that provide transit services is relatively small compared to the total number of ASes, which means the total number of ROV_TAG objects is expected to be manageable. This results in minimal storage and query overhead compared to other RPKI objects such as ROAs.

Query operations for ROV_TAG information can be performed efficiently using standard data structures (e.g., hash tables keyed by AS number), enabling fast lookups during BGP path selection.

4.3. Deployment Recommendations

For ASes that provide transit services and have deployed ROV, it is RECOMMENDED that they register an ROV_TAG object with rovDeployed set to TRUE. This provides transparency about ROV deployment. It also enables downstream ASes to make informed path selection decisions when hijacked routes are detected.

Stub ASes (end networks, content providers, etc.) are NOT RECOMMENDED to register ROV_TAG objects, as they typically appear as Origin ASes in BGP route announcements.

5. Implementation Considerations

This section provides guidance for implementers of ROV_TAG support.

ROV_TAG is a new RPKI object type. Existing RPKI RP implementations that do not support ROV_TAG will simply ignore ROV_TAG objects during repository synchronization, as per the RPKI validation rules specified in [RFC6488]. This ensures backward compatibility: ROV_TAG objects do not interfere with existing RPKI operations, and ASes that have not deployed ROV_TAG support can continue to operate normally.

RP implementations that support ROV_TAG SHOULD:

* Validate ROV_TAG objects according to the validation steps specified in Section 2.6.

* Make validated ROV_TAG information available to ASes (e.g., through RPKI-to-Router protocols such as [RFC6810] or [RFC8210]).

The number of ROV_TAG objects is expected to be relatively small compared to other RPKI objects such as ROAs. This is because only ASes that provide transit services are expected to register ROV_TAG objects.

Implementers that choose to implement the secure path selection described in Section 3 SHOULD:

* Obtain ROV_TAG information from the RPKI Relying Party (RP) (e.g., through RPKI-to-Router protocols such as [RFC6810] or [RFC8210]).

* Implement efficient ROV_TAG lookup mechanisms, such as hash tables keyed by AS number, to quickly determine whether upstream ASes in the AS_PATH have deployed ROV by querying the ROV_TAG information.

* Implement logic to detect when a hijacked route announcement is received from an upstream AS and identify alternative paths where the immediate upstream AS has deployed ROV.

* Provide configuration options to enable or disable secure path selection. This allows operators to make informed decisions based on their operational requirements and risk tolerance.

* Log secure path selection decisions (e.g., when alternative paths are selected) to facilitate troubleshooting and security auditing.

* Handle cases where ROV_TAG information is unavailable gracefully by falling back to normal BGP path selection.

6. Security Considerations

The security considerations of [RFC6481], [RFC6485], and [RFC6488] also apply to ROV_TAG objects.

There is no assumption of confidentiality for the data in an ROV_TAG; it is anticipated that ROV_TAG objects will be stored in repositories that are accessible to all ISPs, and perhaps to all Internet users. The integrity of an ROV_TAG MUST be established through cryptographic signing and validation according to [RFC6488].

A fundamental limitation of ROV_TAG is that the information is self-asserted: an AS may register an ROV_TAG with rovDeployed set to TRUE but not actually perform ROV validation. ROV_TAG does not provide cryptographic verification that ROV validation is actually being performed. A malicious AS could register an ROV_TAG to attract traffic when other ASes are looking for alternative paths. However, several factors mitigate this risk:

* The secure path selection mechanism is defensive in nature - it is triggered only when a security problem is detected (hijacked route), not used for general path selection. This reduces the opportunity for exploitation.

* Registering an ROV_TAG in RPKI creates a public record. ASes generally care about their reputation in the routing community, and false claims about ROV deployment could damage that reputation. While this does not provide cryptographic verification, it does provide some level of accountability.

* ASes could maintain local violation records (not in RPKI) to track when upstream ASes that have registered ROV_TAG propagate invalid route announcements. Such mechanisms are non-standardized and implementation-specific, but they demonstrate that ROV_TAG can enable accountability even without cryptographic verification of actual ROV deployment.

These factors reduce the risk of exploitation, though they do not eliminate it entirely.

7. IANA Considerations

This document will require IANA to assign values in several registries. The specific assignments will be determined during the IETF review process. The following registrations are anticipated:

* An OID for the RPKI-ROV-TAG-2026 ASN.1 module in the "SMI Security for S/MIME Module Identifier" registry.

* An OID for the ROV_TAG content type in the "SMI Security for S/MIME CMS Content Type" registry.

* An entry for ROV_TAG in the "RPKI Signed Object" registry.

8. References

8.1. 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/rfc/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/rfc/rfc3779>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/rfc/rfc4271>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/rfc6488>.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, DOI 10.17487/RFC6810, January 2013, <https://www.rfc-editor.org/rfc/rfc6810>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/rfc/rfc6811>.

[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>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/rfc/rfc8210>.

[X.680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", name ITU-T Recommendation, value X.680, 2021, <https://www.itu.int/rec/T-REC-X.680>.

[X.690] ITU-T, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", name ITU-T Recommendation, value X.690, 2021, <https://www.itu.int/rec/T-REC-X.690>.

8.2. Informative References

[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>.

Appendix A. Example ROV_TAG eContent Payload

Below is an example of a DER-encoded ROV_TAG eContent with annotation following the '#' character.

Example: Transit AS with ROV deployed

```
$ echo 30080201000203000D050201FF | xxd -r -ps | openssl asn1parse \
-inform DER -dump -i 0:d=0 hl=2 l= 8 cons: SEQUENCE 2:d=1 hl=2 l= 1
prim: INTEGER :00 # version = 0 5:d=1 hl=2 l= 3 prim: INTEGER :0D05 #
asID = 3333 10:d=1 hl=2 l= 1 prim: BOOLEAN :FF # rovDeployed = TRUE
```

Authors' Addresses

Sitong Ling
Zhongguancun Lab
Beijing
China
Email: lingst@zgclab.edu.cn

Ke Xu
Tsinghua University
Beijing
China
Email: xuke@tsinghua.edu.cn

Qi Li
Tsinghua University
Beijing
China
Email: qli01@tsinghua.edu.cn

Zhuotao Liu
Tsinghua University
Beijing
China
Email: zhuotaoliu@tsinghua.edu.cn

Xiaoliang Wang
Capital Normal University
Beijing
China
Email: wangxiaoliang@cnu.edu.cn