

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 23 August 2025

Y. Guo  
Zhongguancun Laboratory  
X. Wang  
K. Xu  
Z. Liu  
Q. Li  
Tsinghua University  
19 February 2025

A Profile for Forwarding Commitments (FCs)  
draft-guo-sidrops-fc-profile-00

## Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for Forwarding Commitments (FCs) objects used in Resource Public Key Infrastructure (RPKI). An FC is a digitally signed object that provides a means of verifying whether an IP address block is received from AS a to AS b and announced from AS b to AS c. When validated, an FC's eContent can be used for the detection and mitigation of route hijacking, especially providing protection for the AS\_PATH attribute in BGP-UPDATE.

## About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at  
<https://fcbgp.github.io/fc-profile/draft-guo-sidrops-fc-profile.html>.  
Status information for this document may be found at  
<https://datatracker.ietf.org/doc/draft-guo-sidrops-fc-profile/>.

Source for this draft and an issue tracker can be found at  
<https://github.com/FCBGP/fc-profile>.

## 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 23 August 2025.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
1.1. Requirements Language . . . . .	4
2. The FC Content-Type . . . . .	4
3. The FC eContent . . . . .	4
3.1. version . . . . .	5
3.2. asID . . . . .	5
3.3. routingIntents . . . . .	6
3.3.1. previousASes . . . . .	6
3.3.2. nexthopASes . . . . .	6
3.3.3. originASes . . . . .	6
4. Forwarding Commitment Validation . . . . .	6
5. Operational Consideration . . . . .	7
6. Security Considerations . . . . .	7
7. IANA Considerations . . . . .	7
7.1. SMI Security for S/MIME Module Identifier registry . . . . .	7
7.2. SMI Security for S/MIME CMS Content Type registry . . . . .	7
7.3. RPKI Signed Object registry . . . . .	8
7.4. RPKI Repository Name Scheme registry . . . . .	8
7.5. Media Type registry . . . . .	8
8. References . . . . .	9
8.1. Normative References . . . . .	9
8.2. Informative References . . . . .	10
Acknowledgments . . . . .	11
Authors' Addresses . . . . .	11

## 1. Introduction

The Border Gateway Protocol (BGP) [RFC4271] was designed with no mechanisms to validate the security of BGP attributes. There are two types of BGP security issues, BGP Hijacks and BGP Route Leaks [RFC7908], plague Internet security.

The primary purpose of the Resource Public Key Infrastructure (RPKI) is to improve routing security. (See [RFC6480] for more information.) As part of this system, a mechanism is needed to allow entities to verify that an IP address holder has permitted an AS to advertise a route along the propagation path. A Forwarding Commitment (FC) provides this function.

A Forwarding Commitment (FC) is a digitally signed object through which the issuer (the holder of an Autonomous System identifier), can authorize one or more other Autonomous Systems (ASes) as its upstream ASes or one or more other ASes as its downstream ASes. The upstream ASes, or previous ASes, mean that the issuer AS can receive BGP route updates from these ASes. The downstream ASes, or nexthop ASes, mean that the issuer AS would advertise the BGP route to these ASes.

In this propagation model, it uses a Web of Trust, i.e., the issuer AS trusts its previous ASes and authorizes nexthop ASes to propagate its received routes. Then, all nexthop ASes would also accept the routes and proceed to send them to their next hops. The relationship among them is the signed FC, which attests that a downstream AS has been selected by the directly linked upstream AS to announce the routes.

Initially, all ASes on the propagation path should sign one or more FCs independently if they want to propagate the route to its downstream ASes, and then be able to detect and filter malicious routes (e.g., route leaks and route hijacks). In addition, the FC can also attest that all ASes on a propagation path have received and selected this AS\_PATH, which can be certified as a trusted path.

The FC uses the template for RPKI digitally signed objects [RFC6488] for the definition of a Cryptographic Message Syntax (CMS) [RFC5652] wrapper for the FC content as well as a generic validation procedure for RPKI signed objects. As RPKI certificates issued by the current infrastructure are required to validate FC, we assume the mandatory-to-implement algorithms in [RFC6485] or its successor.

To complete the specification of the FC (see Section 4 of [RFC6488]), this document defines:

1. The object identifier (OID) that identifies the FC-signed object. This OID appears in the eContentType field of the encapContentInfo object as well as the content-type signed attribute within the signerInfo structure.
2. The ASN.1 syntax for the FC content, which is the payload signed by the BGP speaker. The FC content is encoded using the ASN.1 [X.680] Distinguished Encoding Rules (DER) [X.690].
3. The steps required to validate an FC beyond the validation steps specified in [RFC6488].

#### 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 FC Content-Type

The content-type for an FC is defined as ForwardingCommitment and 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 object as well as the content-type signed attribute in the signerInfo object (see [RFC6488]).

#### 3. The FC eContent

The content of an FC identifies a forwarding commitment that represents an AS's routing intent. Upon receiving a BGP-UPDATE message, other ASes can perform AS-path verification according to the validated FCs. An FC is an instance of ForwardingCommitmentAttestation, formally defined by the following ASN.1 [X.680] module:

```
RPKI-FC-2025
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) smime(16) modules(0) id-mod-rpki-FC-2025(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-FC OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-9(9) id-smime(16) id-ct(1) fc(TDB) }

ct-FC CONTENT-TYPE ::=
  { TYPE ForwardingCommitmentAttestation IDENTIFIED BY id-ct-FC }

ForwardingCommitmentAttestation ::= SEQUENCE {
  version [0]          INTEGER DEFAULT 0,
  asID                 ASID,
  routingIntents       SEQUENCE (SIZE(1..MAX)) OF ROUTING-INTENT }

ROUTING-INTENT ::= SEQUENCE {
  previousASes         SEQUENCE (SIZE(1..MAX)) OF ASID,
  nexthopASes          SEQUENCE (SIZE(1..MAX)) OF ASID,
  originASes           SEQUENCE (SIZE(0..MAX)) OF ASID OPTIONAL }

ASID ::= INTEGER (0..4294967295)

END

Note that this content appears as the eContent within the
encapContentInfo (see [RFC6488]).
```

### 3.1. version

The version number of the ForwardingCommitmentAttestation MUST be 0.

### 3.2. asID

The asID field contains the AS number of the issuer AS associated with this FC.

### 3.3. routingIntents

The routingIntents field comprises a list of routing intents associated with the issuing asID. Each routing intent generally includes an upstream AS, a downstream AS, and a specified route set. To optimize space, the field may aggregate routing intents that share the same route set. Therefore, the routingIntents field indicates that for a route set represented by originASes, the issuing asID can receive routes from any AS in previousASes and subsequently forward them to any AS in nexthopASes.

#### 3.3.1. previousASes

The previousASes field contains the upstream ASes' number of the issuer AS that can advertise the routes to the issuer AS.

#### 3.3.2. nexthopASes

The nexthopASes field contains the downstream ASes' number of the issuer AS that can receive advertised routes from the issuer AS.

#### 3.3.3. originASes

The originASes field contains a set of ASes. It associates with ROAs [RFC9582]. This is an optional field. When it is blank, it means that all routes received from upstream ASes defined in the previousASes field could be advertised to downstream ASes defined in the nexthopASes field.

## 4. Forwarding Commitment Validation

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

- \* The contents of the CMS eContent field MUST conform to all the constraints described in Section 3.
- \* The Autonomous System Identifier Delegation Extension described in [RFC3779] is also used in Forwarding Commitment and MUST be present in the EE certificate contained in the CMS certificates field.
- \* The AS identifier present in the ForwardingCommitmentAttestation eContent 'asID' field MUST be contained in the AS Identifiers present in the certificate extension.

- \* The Autonomous System Identifier Delegation extension MUST NOT contain "inherit" elements.
- \* The IP Address Delegation Extension [RFC3779] is not used in Forwarding Commitment, and MUST NOT be present in the EE certificate.

## 5. Operational Consideration

Multiple valid Forwarding Commitment objects which contain the same asID could exist. In such a case, the union of these objects forms the complete routing intent set of this AS. For a given asID, it is RECOMMENDED that a CA maintains a single Forwarding Commitment. If an AS holder publishes a Forwarding Commitment, then relying parties SHOULD assume that this object is complete for that issuer AS.

If one AS receives a BGP UPDATE message with the issuer AS in the AS\_PATH attribute which cannot match any routing intents of this issuer AS, it implies that there is an AS-path forgery in this message.

## 6. Security Considerations

The security considerations of [RFC6480], [RFC6481], [RFC6485], [RFC6487] and [RFC6488] also apply to FCs.

## 7. IANA Considerations

### 7.1. SMI Security for S/MIME Module Identifier registry

Please add the id-mod-rpki-fc-2025 to the SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0) registry (<https://www.iana.org/assignments/smi-numbers/smi-numbers.xml#security-smime-0>) as follows:

Decimal	Description	Specification
TBD	id-mod-rpki-fc-2025	[RFC-to-be]

### 7.2. SMI Security for S/MIME CMS Content Type registry

Please add the FC to the SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1) registry (<https://www.iana.org/assignments/smi-numbers/smi-numbers.xml#security-smime-1>) as follows:

Decimal	Description	Specification
TBD	id-ct-FC	[RFC-to-be]

### 7.3. RPKI Signed Object registry

Please add Forwarding Commitment to the RPKI Signed Object registry (<https://www.iana.org/assignments/rpki/rpki.xhtml#signed-objects>) as follows:

Name	OID	Specification
Forwarding Commitment	1.2.840.113549.1.9.16.1.TBD	[RFC-to-be]

### 7.4. RPKI Repository Name Scheme registry

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

Filename Extension	RPKI Object	Reference
.for	Forwarding Commitment	[RFC-to-be]

### 7.5. Media Type registry

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



Type name: application  
Subtype name: rpki-fc  
Required parameters: N/A  
Optional parameters: N/A  
Encoding considerations: binary  
Security considerations: Carries an RPKI FC [RFC-to-be].  
    This media type contains no active content. See  
    Section xxx of [RFC-to-be] for further information.  
Interoperability considerations: None  
Published specification: [RFC-to-be]  
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  
    AS identifiers (ASIDs) as defined in [RFC-to-be].  
    Magic number(s): None  
    File extension(s): .for  
    Macintosh file type code(s):  
Person & email address to contact for further information:  
    Yangfei Guo <guoyangfei@zgclab.edu.cn>  
Intended usage: COMMON  
Restrictions on usage: None  
Change controller: IETF

## 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>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/rfc/rfc5652>>.
- [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>>.

- [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>>.
- [RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <<https://www.rfc-editor.org/rfc/rfc6487>>.
- [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>>.
- [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>>.
- [X.680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", Recommendation ITU-T X.680 , February 2021, <<https://itu.int/rec/T-REC-X.680-202102-I/en>>.
- [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)", Recommendation ITU-T X.690 , February 2021, <[<https://itu.int/rec/T-REC-X.680-202102-I/en>](<https://www.itu.int/rec/T-REC-X.690-202102-I/en>)>.

## 8.2. Informative References

- [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>>.
- [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <<https://www.rfc-editor.org/rfc/rfc6480>>.

- [RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <<https://www.rfc-editor.org/rfc/rfc7908>>.
- [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/rfc/rfc9582>>.

#### Acknowledgments

TODO acknowledge.

#### Authors' Addresses

Yangfei Guo  
Zhongguancun Laboratory  
Beijing  
China  
Email: [guoyangfei@zgclab.edu.cn](mailto:guoyangfei@zgclab.edu.cn)

Xiaoliang Wang  
Tsinghua University  
Beijing  
China  
Email: [wangxiaoliang0623@foxmail.com](mailto:wangxiaoliang0623@foxmail.com)

Ke Xu  
Tsinghua University  
Beijing  
China  
Email: [xuke@tsinghua.edu.cn](mailto:xuke@tsinghua.edu.cn)

Zhuotao Liu  
Tsinghua University  
Beijing  
China  
Email: [zhuotaoliu@tsinghua.edu.cn](mailto:zhuotaoliu@tsinghua.edu.cn)

Qi Li  
Tsinghua University  
Beijing  
China

Email: [qli01@tsinghua.edu.cn](mailto:qli01@tsinghua.edu.cn)