SIDR Operations
Internet-Draft
Intended status: Standards Track
Expires: 27 September 2025

Q. Misell, Ed.
AS207960
J. Snijders

26 March 2025

Resource Public Key Infrastructure (RPKI) Signed Messages (RSMs)
draft-blahaj-sidrops-rsm-01

Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI) to carry a signature over a detached message. This document is an iteration on RPKI Signed Checklists (RSCs) [RFC9323] to include an explicit purpose and audience, to allow for more secure automated processing.

Discussion

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

Source for this draft and an issue tracker can be found at https://github.com/AS207960/draft-blahaj-sidrops-rsm.

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 27 September 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

RPKI Signed Checklists (RSC) [RFC9323] do not signal a purpose, nor its intended audience. In the context of processing by humans this is of little concern as the context in which e.g. a signed PDF was sent makes its purpose evident. However, in automated machine-to-machine protocols these ambiguities can lead to security vulnerabilities.

To allow for better use of the RPKI in machine-to-machine communications, this document defines the RPKI Signed Message (RSM) content type, including an explicit audience and purpose field.

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 [BCP14] (RFC2119,RFC8174) when, and only when, they appear in all capitals, as shown here.

2. Motivation for a new content type

Protocols can assign the different meanings to the same data. In the context of human-to-human communication the worst outcome of this is often a mere opportunity for a pun; however in the context of automated machine-to-machine processing this can lead to serious security vulnerabilities.

An RSC with ambiguous content could, for example, be used in a cross-protocol replay attack. One might argue that a protocol which is vulnerable to such a replay attack is a poorly designed one; a counter-argument to this is that it should not be possible to design such a vulnerability into a protocol built on top of RSCs in the first place.

Further motivation for avoiding such ambiguity in protocols can be found in Is that ASCII or is it Protobuf? The importance of types in cryptographic signatures.

3. Profile and Distribution

RSMs follows the Signed Object Template for the RPKI [RFC6488] with one exception: because RSMs MUST NOT be distributed through the global RPKI repository system, the Subject Information Access (SIA) extension MUST be omitted from the RSM’s X.509 End-Entity (EE) certificate.

What constitutes suitable transport for RSM files is deliberately unspecified. In the context of machine-to-machine communication it is expected that they are attached to an API request, in a way compatible with said API.

3.1. End Entity Certificates

The Certification Authority (CA) MUST only sign one RSM with each EE certificate and MUST generate a new key pair for each new RSM. This type of EE certificate is termed a "one-time-use" EE certificate (seeSection 3 of [RFC6487]).

4. Content Type

The eContentType for an RSM is defined as id-ct-rpkiSignedMessage, with Object Identifier (OID) 1.2.840.113549.1.9.16.1.TDB.

This OID MUST appear within both the eContentType in the encapContentInfo object and the ContentType signed attribute in the signerInfo object (see[RFC6488]).

5. Content

The content of an RSM indicates that as arbitrary binary message has been signed with a specific set of Internet Number Resources. An RSM is formally defined as follows:

```
RpkiSignedMessage-2025
  { iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs9(9) smime(16) mod(0)
    id-mod-rpkiSignedMessage-2025(TBD) }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
  CONTENT-TYPE, Digest, DigestAlgorithmIdentifier
  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) }

  IPAddressOrRange, ASIdOrRange
  FROM IPAddrAndASCertExtn -- in [RFC3779]
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) mod(0)
      id-mod-ip-addr-and-as-ident(30) }

  ResourceBlock
  FROM id-mod-rpkiSignedChecklist-2022 -- in [RFC9323]
    { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs9(9) smime(16) mod(0)
      id-mod-rpkiSignedChecklist-2022(73) };

ct-rpkiSignedMessage CONTENT-TYPE ::=
  { TYPE RpkiSignedMessage
    IDENTIFIED BY id-ct-signedMessage }

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

RpkiSignedMessage ::= SEQUENCE {
    version [0]       INTEGER DEFAULT 0,
    purpose           OBJECT IDENTIFIER
    audience          OBJECT IDENTIFIER
    resources         ResourceBlock,
    digestAlgorithm   DigestAlgorithmIdentifier,
    hash              Digest }
END
```

5.1. Version

The version number of the RpkiSignedMessage MUST be 0.

5.2. Purpose

The purpose field includes an OID identifying for which purpose the RSM was created.

5.3. Audience

The audience fields includes an OID identifying for which audience the RSM was created, or that it was created for the general audience.

5.4. Resources

The resources in an RSM MUST be constructed as per Section 4.2 of [RFC9323].

5.5. Digest algorithm

The digest algorithm is used to create the message digest of the attested message. This algorithm MUST be a hash algorithm defined in [RFC7935].

5.6. Hash

The value of the hash field is the calculated message digest of the attested message. This message is carried externally to the RSM. That is, an RSM is a detached signature.

6. Well-known audiences and purposes

It would be advantages for implementations to have certain well-known purposes and audiences for uses of RSMs that are intended to be globally interoperable. To that end this document establishes an OID tree for well-known audiences and purposes, under 1.3.6.1.5.5.TBD.0 and 1.3.6.1.5.5.TBD.1 respectively.

6.1. Anyone Audience

When an RSM is intended anyone and everyone SHOULD use the 1.3.6.1.5.5.TBD.0.0 audience. This should be used sparingly, as its use can introduce the possibility for cross-protocol attacks.

6.2. Autonomous System Audience

When an RSM is intended for the operator of a specific AS implementors SHOULD use the 1.3.6.1.5.5.TBD.0.1.X audience, where X is the intended ASN. That is, an RSM intended for AS64496 will have the audience 1.3.6.1.5.5.TBD.0.1.64496.

7. Validation

The considerations of Section 5 of [RFC9323] also apply to validating RSMs.

Additionally, a Relying Party MUST verify:

* That the RSM is intended for the purpose that it is being used for.

* That it is in the intended audience of the RSM.

8. Security Considerations

The considerations of Section 8 of [RFC9323] also apply to RSMs.

Additionally, RPs MUST verify the purpose and audience fields, and protocols SHOULD ensure that the values used in these fields are specific enough to avoid cross-protocol attacks.

9. IANA Considerations

9.1. SMI Security for Mechanism Codes

The IANA is requested to allocate a new security mechanism under the "SMI Security for Mechanism Codes" registry:

OID Value	Name	Description	References
1.3.6.1.5.5.TBD	rsm	RPKI Signed Messages	This document

Table 1

9.2. SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)

The IANA is requested to allocate the following in the "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" registry:

Decimal	Description	References
TBD	id-ct-rpkiSignedMessage	This document

Table 2

9.3. RPKI Signed Objects

The IANA is requested to register the OID for the RSM in the "RPKI Signed Objects" registry [RFC6488] as follows:

Name	OID	Reference
Signed Message	1.2.840.113549.1.9.16.1.TBD	This document

Table 3

9.4. RPKI Repository Name Schemes

The IANA is requested to add the Signed Message file extension to the "RPKI Repository Name Schemes" registry [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.sme	Signed Message	This document

Table 4

9.5. SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)

The 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	References
TBD	id-mod-rpkiSignedMessage-2025	This document

Table 5

9.6. Media Types

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

Type name: application

Subtype name: rpki-signed-message

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: binary

Security considerations: Carries an RPKI Signed Message. This media type contains no active content.

Interoperability considerations: N/A

Published specification: This document

Applications that use this media type: RPKI operators

Fragment identifier considerations: N/A

Additional information: Content: This media type is a signed object, as defined in [RFC6488], which contains a payload of a list of checksums as defined in this document.

Magic number(s): N/A

File extension(s): .rsm

Macintosh file type code(s): N/A

Person & email address to contact for further information: Q Misell (q@as207960.net)

Intended usage: COMMON

Restrictions on usage: N/A

Author: Q Misell (q@as207960.net)

Change controller: IETF

9.7. New registries

The IANA is requested to create the following new registries:

* RPKI Signed Message well-known audiences (1.3.6.1.5.5.TBD.0)

* RPKI Signed Message well-known purposes (1.3.6.1.5.5.TBD.1)

9.7.1. RPKI Signed Message well-known audiences

This registry contains the audience OIDs which are to be understood globally. All values are in the 1.3.6.1.5.5.TBD.0 tree.

Template:

Decimal integer value of the OID tree node

Description a textual description of the audience

Reference where this audience is defined

Initial contents:

Decimal	Description	References
0	Global Audience	This document
1	Autonomous System	This document

Table 6

Values are to be allocated under the Specifications Required procedure.

9.7.2. RPKI Signed Message well-known purposes

This registry contains the purpose OIDs which are to be understood globally. All values are in the 1.3.6.1.5.5.TBD.1 tree.

Template:

Decimal integer value of the OID tree node

Description a textual description of the purpose

Reference where this purpose is defined

Initial contents:

Decimal	Description	References
No entries		

Table 7

Values are to be allocated under the Specifications Required procedure.

10. References

10.1. Normative References

[BCP14] Best Current Practice 14, <https://www.rfc-editor.org/info/bcp14>. At the time of writing, this BCP comprises the following:

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>.

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>.

[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>.

[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/info/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/info/rfc6488>.

[RFC7935] Huston, G. and G. Michaelson, Ed., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure", RFC 7935, DOI 10.17487/RFC7935, August 2016, <https://www.rfc-editor.org/info/rfc7935>.

[RFC9323] Snijders, J., Harrison, T., and B. Maddison, "A Profile for RPKI Signed Checklists (RSCs)", RFC 9323, DOI 10.17487/RFC9323, November 2022, <https://www.rfc-editor.org/info/rfc9323>.

10.2. Informative References

[ascii-or-protobuf] Varda, K., "Is that ASCII or is it Protobuf? The importance of types in cryptographic signatures", May 2015, <https://sandstorm.io/news/2015-05-01-is-that-ascii-or-protobuf>.

Authors' Addresses

Q Misell (editor)
AS207960 Cyfyngedig
13 Pen-y-lan Terrace
Caerdydd
CF23 9EU
United Kingdom
Email: q@as207960.net, q@magicalcodewit.ch
URI: magicalcodewit.ch

Job Snijders
Amsterdam
Netherlands
Email: job@sobornost.net