SIDROPS
Internet-Draft
Intended status: Standards Track
Expires: 18 April 2026

J. Snijders
BSD
B. Bakker
T. Bruijnzeels
RIPE NCC

15 October 2025

A Profile for Resource Public Key Infrastructure (RPKI) Canonical Cache Representation (CCR)
draft-spaghetti-sidrops-rpki-ccr-04

Abstract

This document specifies a Canonical Cache Representation (CCR) content type for use with the Resource Public Key Infrastructure (RPKI). CCR is a DER-encoded data interchange format which can be used to represent various aspects of the state of a validated cache at a particular point in time. The CCR profile is a compact and versatile format well-suited for a diverse set of applications such as audit trail keeping, validated payload dissemination, and analytics pipelines.

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 18 April 2026.

Copyright Notice

Table of Contents

1. Introduction

This document specifies a Canonical Cache Representation (CCR) content type for use with the Resource Public Key Infrastructure (RPKI). A validated cache contains all RPKI objects that the Relying Party (RP) has verified to be valid according to the rules for validation (see [RFC6487], [RFC6488], [RFC9286]). CCR is a data interchange format using Distinguished Encoding Rules (DER, [X.690])

which can be used to represent various aspects of the state of a validated cache at a particular point in time. The CCR profile is a compact and versatile format well-suited for a diverse set of applications such as audit record keeping, validated payload dissemination, and analytics pipelines.

The format was primarily designed to support comparative analysis of uniformities and differences among multiple RP instances using different RPKI transport protocols (such as [RFC5781], [RFC8182], and [I-D.spaghetti-sidrops-rpki-erik-protocol]).

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 Canonical Cache Representation content type

The content of a CCR file is an instance of EncapsulatedContentInfo.

The contentType for a CCR currently is defined as id-ct-rpkiCanonicalCacheRepresentation, with temporary Object Identifier (OID) 1.3.6.1.4.1.41948.825.

The eContent is the payload of the CCR encapsulated as an OCTET STRING.

Note: as part of the standardization process, at a future point in time, the aforementioned contentType value will change from the current Private Enterprise Number ([RFC9371]) to an OID assigned by IANA (Section 6).

3. The Canonical Cache Representation content

The content of a Canonical Cache Representation is formally defined as follows:

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

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
```

```
    CONTENT-TYPE, Digest, DigestAlgorithmIdentifier, SubjectKeyIdentifier
    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) }

    ASID, ROAIPAddressFamily
    FROM RPKI-ROA-2023 -- in [RFC9582]
      { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
        pkcs9(9) smime(16) mod(0) id-mod-rpkiROA-2023(75) }

    CertificateSerialNumber, SubjectPublicKeyInfo
    FROM PKIX1Explicit-2009
      { iso(1) identified-organization(3) dod(6) internet(1) security(5)
        mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }

    AccessDescription, KeyIdentifier
    FROM PKIX1Implicit-2009
       {iso(1) identified-organization(3) dod(6) internet(1) security(5)
       mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-implicit-02(59) }
    ;

  EncapsulatedContentInfo ::= SEQUENCE {
    eContentType      CONTENT-TYPE.&id({ContentSet}),
    eContent      [0] EXPLICIT OCTET STRING
      (CONTAINING CONTENT-TYPE.&Type({ContentSet}{@eContentType})) OPTIONAL }

  ContentSet CONTENT-TYPE ::= {
    ct-rpkiCanonicalCacheRepresentation, ... }

  ct-rpkiCanonicalCacheRepresentation CONTENT-TYPE ::=
    { TYPE RpkiCanonicalCacheRepresentation
      IDENTIFIED BY id-ct-rpkiCanonicalCacheRepresentation }

  id-ct-rpkiCanonicalCacheRepresentation OBJECT IDENTIFIER ::=
    { iso(1) identified-organization(3) dod(6) internet(1) private(4)
      enterprise(1) snijders(41948) ccr(828) }

  RpkiCanonicalCacheRepresentation ::= SEQUENCE {
    version     [0] INTEGER DEFAULT 0,
    hashAlg         DigestAlgorithmIdentifier,
    producedAt      GeneralizedTime,
    mfts        [1] ManifestState OPTIONAL,
    vrps        [2] ROAPayloadState OPTIONAL,
    vaps        [3] ASPAPayloadState OPTIONAL,
    tas         [4] TrustAnchorState OPTIONAL,
    rks         [5] RouterKeyState OPTIONAL,
    ... }
    -- at least one of mfts, vrps, vaps, or tas MUST be present
```

```
    ( WITH COMPONENTS { ..., mfts PRESENT } |
      WITH COMPONENTS { ..., vrps PRESENT } |
      WITH COMPONENTS { ..., vaps PRESENT } |
      WITH COMPONENTS { ..., tas PRESENT } |
      WITH COMPONENTS { ..., rks PRESENT } )

  ManifestState ::= SEQUENCE {
    mis               SEQUENCE OF ManifestInstance,
    mostRecentUpdate  GeneralizedTime,
    hash              Digest }

  ManifestInstance ::= SEQUENCE {
    hash              Digest,
    size              INTEGER (1000..MAX),
    aki               KeyIdentifier,
    manifestNumber    INTEGER (0..MAX),
    thisUpdate        GeneralizedTime,
    locations         SEQUENCE SIZE (1..MAX) OF AccessDescription,
    subordinates      SEQUENCE (SIZE(1..MAX)) OF SubjectKeyIdentifier OPTIONAL }

  ROAPayloadState ::= SEQUENCE {
    rps               SEQUENCE OF ROAPayloadSet,
    hash              Digest }

  ROAPayloadSet ::= SEQUENCE {
    asID              ASID,
    ipAddrBlocks      SEQUENCE (SIZE(1..2)) OF ROAIPAddressFamily }

  ASPAPayloadState ::= SEQUENCE {
    aps               SEQUENCE OF ASPAPayloadSet,
    hash              Digest }

  ASPAPayloadSet ::= SEQUENCE {
    customerASID      ASID,
    providers         SEQUENCE (SIZE(1..MAX)) OF ASID }

  TrustAnchorState ::= SEQUENCE {
    skis              SEQUENCE (SIZE(1..MAX)) OF SubjectKeyIdentifier,
    hash              Digest }

  RouterKeyState ::= SEQUENCE {
    rksets            SEQUENCE OF RouterKeySet,
    hash              Digest }

  RouterKeySet ::= SEQUENCE {
    asID              ASID,
    routerKeys        SEQUENCE (SIZE(1..MAX)) OF RouterKey }
```

```
   RouterKey ::= SEQUENCE {
     ski               SubjectKeyIdentifier,
     spki              SubjectPublicKeyInfo }

   END
```

3.1. version

The version field contains the format version for the RpkiCanonicalCacheRepresentation structure, in this version of the specification it MUST be 0.

3.2. hashAlg

The hashAlg field specifies the algorithm used to construct the message digests. This profile uses SHA-256 [SHS], therefore the OID MUST be 2.16.840.1.101.3.4.2.1.

3.3. producedAt

The producedAt field contains a GeneralizedTime and indicates the moment in time the CCR was generated.

3.4. State aspect fields

Each CCR contains one or more fields representing particular aspects of the cache’s state. Implementers should note the ellipsis extension marker in the RpkiCanonicalCacheRepresentation ASN.1 notation and anticipate future changes as new signed object types are standardized.

Each state aspect generally consists of a sequence of details extracted from RPKI Objects of a specific type, along with a digest computed by hashing the aforementioned DER-encoded sequence, optionally including some metadata.

3.4.1. ManifestState

An instance of ManifestState represents the set of valid, current Manifests ([RFC9286]) in the cache. It contains three fields: mis, mostRecentUpdate, and hash.

3.4.1.1. ManifestInstance

The mis field contains a SEQUENCE of ManifestInstance. There is one ManifestInstance for each current manifest. A manifest is nominally current until the time specified in nextUpdate or until a manifest is issued with a greater manifestNumber, whichever comes first (see Section 4.2.1 of [RFC9286]).

A ManifestInstance is a structure consisting of the following fields:

hash the hash of the DER-encoded manifest object

size the size of the manifest object

aki the manifest issuer's key identifier

manifestNumber the manifest number contained within the manifest's eContent field

thisUpdate the thisUpdate contained within the manifest's eContent field

locations a sequence of AccessDescription instances from the manifest's End-Entity certificate's Subject Information Access extension

subordinates a optional non-empty SEQUENCE of SubjectKeyIdentifier

The subordinates field represents the keypairs associated with the set of non-revoked, non-expired, validly signed resource certificates subordinate to the manifest issuer. Each SubjectKeyIdentifier is the 160-bit SHA-1 hash of the value of the DER-encoded ASN.1 bit string of the resource certificate's Subject Public Key, as described in Section 4.8.2 of [RFC6487]. The sequence elements of the subordinates field MUST be sorted in ascending order by interpreting each SubjectKeyIdentifier value as an unsigned 160-bit integer and MUST be unique with respect to each other.

The sequence elements in the mis field MUST be sorted in ascending order by hash value contained in each instance of ManifestInstance and MUST be unique with respect to the other instances of ManifestInstance.

3.4.1.2. mostRecentUpdate

The mostRecentUpdate is a metadata field which contains the most recent thisUpdate amongst all current manifests represented by the ManifestInstance structures. If the mis field contains an empty sequence, the mostRecentUpdate MUST be set to the POSIX Epoch ("19700101000000Z").

3.4.1.3. hash

The hash field contains a message digest computed using the mis value (encoded in DER format) as input message.

3.4.2. ROAPayloadState

An instance of ROAPayloadState contains a field named rps which represents the current set of Validated ROA Payloads (Section 2 of [RFC6811]) encoded as a SEQUENCE of ROAPayloadSet instances.

The ROAPayloadSet structure is modeled after the RouteOriginAttestation (Section 4 of [RFC9582]). The asID value in each instance of ROAPayloadSet MUST be unique with respect to other instances of ROAPayloadSet. The contents of the ipAddrBlocks field MUST appear in canonical form and ordered as defined in Section 4.3.3 of [RFC9582].

The hash field contains a message digest computed using the rps value (encoded in DER format) as input message.

3.4.3. ASPAPayloadState

An instance of ASPAPayloadState contains an aps field which represents the current set of deduplicated and merged ASPA payloads ([I-D.ietf-sidrops-aspa-profile]) ordered by ascending customerASID value encoded as a SEQUENCE of ASPAPayloadSet instances. The customerASID value in each instance of ASPAPayloadSet MUST be unique with respect to other instances of ASPAPayloadSet.

The ASPAPayloadSet structure is modeled after the ProviderASSet (Section 3.3 of [I-D.ietf-sidrops-aspa-profile]).

The hash field contains a message digest computed using the aps value (encoded in DER format) as input message.

3.4.4. TrustAnchorState

An instance of TrustAnchorState represents the set of valid Trust Anchor (TA) Certification Authority (CA) resource certificates used by the relying party when producing the CCR.

Each SubjectKeyIdentifier is the 160-bit SHA-1 hash of the value of the DER-encoded ASN.1 bit string of the TA's Subject Public Key, as described in Section 4.8.2 of [RFC6487]. The skis field contains a sequence of Subject Key Identifiers (SKI) sorted in ascending order by interpreting the SKI value as an unsigned 160-bit integer.

The hash field contains a message digest computed using the skis value (encoded in DER format) as input message.

3.4.5. RouterKeyState

An instance of RouterKeyState contains an rksets field which represents the current set of valid BGPsec Router Keys [RFC8205] encoded as a SEQUENCE of RouterKeySet instances. The asID value in each instance of RouterKeySet MUST be unique with respect to other instances of RouterKeySet. Instances of RouterKeySet are sorted by ascending value of asID. Instances of RouterKey are sorted by ascending value of ski by interpreting the SKI value as an unsigned 160-bit integer.

The hash field contains a message digest computed using the rks value (encoded in DER format) as input message.

4. Operational Considerations

Comparing the ManifestState mostRecentUpdate timestamp value with the producedAt timestamp might help offer insight into the timing and propagation delays of the RPKI supply chain.

Given the absence of public keys and fairly repetitive content in RPKI AccessDescription instances, it should be noted CCR content compresses well.

4.1. Verifying CCR file integrity

The integrity of a CCR object can be checked by confirming whether the hash values embedded inside state aspects match the computed hash value of the respective state aspect payload structure.

5. Security Considerations

CCR objects are not signed objects.

6. IANA Considerations

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

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-rpkiCanonicalCacheRepresentation	draft-spaghetti-sidrops-rpki-ccr

Table 1

6.2. RPKI Repository Name Schemes

IANA is requested to add the Canonical Cache Representation file extension to the "RPKI Repository Name Schemes" registry [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.ccr	Canonical Cache Representation	draft-spaghetti-sidrops-rpki-ccr

Table 2

6.3. 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	References
TBD	id-mod-rpkiCCR-2025	draft-spaghetti-sidrops-rpki-ccr

Table 3

6.4. Media Types

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

6.4.1. Canonical Cache Representation Media Type

Type name: application
Subtype name: rpki-ccr
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: binary
Security considerations: This media type contains no active content.
Interoperability considerations: N/A
Published specification: draft-spaghetti-sidrops-rpki-ccr
Applications that use this media type: RPKI operators
Fragment identifier considerations: N/A
Additional information:
Content: This media type is a RPKI Canonical Cache Representation object, as defined in draft-spaghetti-sidrops-rpki-ccr.
Magic number(s): N/A
File extension(s): .ccr
Macintosh file type code(s): N/A
Person & email address to contact for further information: Job Snijders (job@bsd.nl)
Intended usage: COMMON
Restrictions on usage: N/A
Author: Job Snijders (job@bsd.nl)
Change controller: IETF

7. References

7.1. Normative References

[I-D.ietf-sidrops-aspa-profile]
Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-profile-20, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-20>.

[I-D.spaghetti-sidrops-rpki-erik-protocol]
Snijders, J., Bruijnzeels, T., Harrison, T., and W. Ohgai, "The Erik Synchronization Protocol for use with the Resource Public Key Infrastructure (RPKI)", Work in Progress, Internet-Draft, draft-spaghetti-sidrops-rpki-erik-protocol-03, 25 September 2025, <https://datatracker.ietf.org/doc/html/draft-spaghetti-sidrops-rpki-erik-protocol-03>.

[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>.

[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>.

[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/info/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/info/rfc8174>.

[RFC9286] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 9286, DOI 10.17487/RFC9286, June 2022, <https://www.rfc-editor.org/info/rfc9286>.

[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/info/rfc9582>.

[SHS] National Institute of Standards and Technology, "Secure Hash Standard", March 2012, <https://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>.

[X.690] ITU-T, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (B ER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.690-202102-I/en>.

7.2. Informative References

[RFC5781] Weiler, S., Ward, D., and R. Housley, "The rsync URI Scheme", RFC 5781, DOI 10.17487/RFC5781, February 2010, <https://www.rfc-editor.org/info/rfc5781>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[RFC9371] Baber, A. and P. Hoffman, "Registration Procedures for Private Enterprise Numbers (PENs)", RFC 9371, DOI 10.17487/RFC9371, March 2023, <https://www.rfc-editor.org/info/rfc9371>.

[rpki-client] Jeker, C., Dzonsons, K., Buehler, T., and J. Snijders, "rpki-client", October 2025, <https://www.rpki-client.org/>.

[rpkitouch]
Snijders, J., "rpki-client", October 2025,
<https://www.github.com/job/rpkitouch>.

Appendix A. Acknowledgements

The authors wish to thank Theo Buehler and Russ Housley for their generous feedback on this specification,

Appendix B. Example CCR

The below is a Base64-encoded example CCR object. For a more elaborate example based on the global RPKI, see the URL in Appendix C.

MIIMugYKKwYBBAGCx1yGPKCCDKoEggymMIIMogYJYIZIAWUDBAIBGA8yMDI1MTAxMjIyMzcw
NVqhgggbMIIIFzCCB+AwgdEEIAAAHDo70vm2o1C6+wOn1T5yfeK0J0tUDJiGxJcvAn1GAgII
GAQUhbYRoLfUM0t6I5XozOew48m4OOgCAhHYGA8yMDI1MTAxMjE2MDIwOVowfjB8BggrBgEF
BQcwC4ZwcnN5bmM6Ly9ycGtpLnJpcGUubmV0L3JlcG9zaXRvcnkvREVGQVVMVC85OC85ZDU2
M2QtYzQ3MC00M2IzLTgyYmItODhjYjRlNzEwNmVhLzEvaGJZUm9MZlVNMHQ2STVYb3pPZXc0
OG00T09nLm1mdDCB1AQgAABagYSizHH1sGBKuaaMPjDuuPnIqquzYCccyLYpNbACAghBBBRm
6g+DvdNjK/8ZQAs6G6b+3/xVhwICNNgYDzIwMjUxMDEyMTUyNTA4WjCBgDB+BggrBgEFBQcw
C4ZycnN5bmM6Ly9ycGtpLmFwbmljLm5ldC9tZW1iZXJfcmVwb3NpdG9yeS9BOTE3Q0I2My9F
MUIwNTRGQzFEQTcxMUUyQjY4OEVCQTEwOEIwMkNEMi9adW9QZzczVFl5dl9HVUFMT2h1bV90
XzhWWWMubWZ0MIIBOwQgAAGCg7kka6eCMNVoPED8zAHbZx1RUOfUy0gXAj63fUoCAgmLBBRU
A12dxsmorHL2wFiEpud8B7o40wIUAQ0Mn0MoWEn1xyIpJWAG5AjJPVAYDzIwMjUxMDEyMTMw
MDAzWjCB1TCB0gYIKwYBBQUHMAuGgcVyc3luYzovL3Jwa2kuYXJpbi5uZXQvcmVwb3NpdG9y
eS9hcmluLXJwa2ktdGEvNWU0YTIzZWEtZTgwYS00MDNlLWIwOGMtMjE3MWRhMjE1N2QzL2Q2
YjVhZDI4LTFjYmMtNDdhYi05MDRlLTQ1MzYxYTU0ODdjMy9iMGI3OTNjMi02ZWQ0LTQ2NDIt
ODY4My1lNWI2MWU4ZDlmNzYvYjBiNzkzYzItNmVkNC00NjQyLTg2ODMtZTViNjFlOGQ5Zjc2
Lm1mdDCCAVMEIADN5ihJIC1p/1toEKmLaRQ29nJpfDHzTzWyI6ps+ydGAgIJRwQUDCzb6Jfs
kycnIBhIG20/x8Y5vnMCFAENDJ9DKFhBP3r8SduClFsuFxlhGA8yMDI1MTAxMjE2MDAwOFow
gdUwgdIGCCsGAQUFBzALhoHFcnN5bmM6Ly9ycGtpLmFyaW4ubmV0L3JlcG9zaXRvcnkvYXJp
bi1ycGtpLXRhLzVlNGEyM2VhLWU4MGEtNDAzZS1iMDhjLTIxNzFkYTIxNTdkMy9hNzM0MjBj
Yi1iM2NjLTRiMDMtYmRhNy0xYmUyMDQ5MzNhZTUvODhjNjk0ODYtM2UxNC00ZjI2LTlmOTkt
MDJjZjdhYWFiN2JmLzg4YzY5NDg2LTNlMTQtNGYyNi05Zjk5LTAyY2Y3YWFhYjdiZi5tZnQw
FgQUdQ/Tug9sCFY83b6RGXn7EieXZJwwggFTBCAEqsP0kBvlBpEmaaMV57UPt8zl4x4VIcLG
ZezXxcgUPAICCUcEFCMq6UmAO6mVaQ4fXI99CioXczjAAhQBDQyfQyhYQHOoVRREuw+XHTPW
thgPMjAyNTEwMTIxMzAwMDNaMIHVMIHSBggrBgEFBQcwC4aBxXJzeW5jOi8vcnBraS5hcmlu
Lm5ldC9yZXBvc2l0b3J5L2FyaW4tcnBraS10YS81ZTRhMjNlYS1lODBhLTQwM2UtYjA4Yy0y
MTcxZGEyMTU3ZDMvZjYwYzlmMzItYTg3Yy00MzM5LWEyZjMtNjI5OWEzYjAyZTI5LzMxNzAw
OGY0LTMwNDgtNDMzMC1hMzRiLTJhMzZkZmUwZjAzNi8zMTcwMDhmNC0zMDQ4LTQzMzAtYTM0
Yi0yYTM2ZGZlMGYwMzYubWZ0MBYEFL+idQl2ygf1amiXaw8B64YvF8OzMIIBUwQgBK/QKKOP
GVAWh0dlb1On+2zK2N0459cPk73dw8Sw3k4CAglHBBS++LX5I0cTVZFG8pwmnxtVXqASywIU
AQ0Mn0MoWEFhm/+1DVrplw0sCKQYDzIwMjUxMDEyMjEwMDAzWjCB1TCB0gYIKwYBBQUHMAuG
gcVyc3luYzovL3Jwa2kuYXJpbi5uZXQvcmVwb3NpdG9yeS9hcmluLXJwa2ktdGEvNWU0YTIz
ZWEtZTgwYS00MDNlLWIwOGMtMjE3MWRhMjE1N2QzL2E3MzQyMGNiLWIzY2MtNGIwMy1iZGE3
LTFiZTIwNDkzM2FlNS80NmJmMWYwMy0yZWJkLTQwNWUtYTViNy02MmJkZjNkN2RiZTYvNDZi

```
   ZjFmMDMtMmViZC00MDVlLWE1YjctNjJiZGYzZDdkYmU2Lm1mdDAWBBTLCIbSBEimY8fPXE4Z
   eaxvedsFIDCB7gQgDhZ5vv97/QzUkkv9ZKRYVkkamvfDmBMAJEsXGF0qsCICAgh+BBRvGhA+
   FCf/A0g6v9njTay+FST/iwICDxcYDzIwMjUxMDEyMDAxNTEyWjBXMFUGCCsGAQUFBzALhkly
   c3luYzovL3Jwa2kuYWZyaW5pYy5uZXQvcmVwb3NpdG9yeS9hcG5pYy9ieG9RUGhRbl93TklP
   cl9aNDAyc3ZoVWtfNHMubWZ0MEIEFFP3jYDKwOsurNd7AXXfMZ6PdSeWBBRy8IdBTOLfRLxP
   Tf9b4RR6enGprgQU7vdTJDjdpqMkdkrK+E72JOF34MUYDzIwMjUxMDEyMjEwMDAzWgQgoUpo
   sx2mojv22Q4FUvy66oh5ZDJzSXTAH2CM3NZ+hxWiggHmMIIB4jCCAbwwZAIBBzBfMEgEAgAB
   MEIwCQMEAMAjXgIBIDAJAwQAwEMrAgEgMAkDBADCIEUCASAwCQMEAcIg2gIBIDAJAwQAwiKK
   AgEgMAkDBAHCPVwCASAwEwQCAAIwDTALAwUDKgs7QAICAIAwgaMCAiBbMIGcMH4EAgABMHgw
   BgMEAFvQIjAGAwQAXo7wMAYDBANejvAwBgMEAF6O8TAGAwQAXo7yMAYDBABejvQwBgMEAF6O
   9TAGAwQAXo72MAYDBABejvcwBgMEALk04DAGAwQCuTTgMAYDBAC5NOEwBgMEALk04jAGAwQA
   uTTjMAYDBADLOCwwGgQCAAIwFDAJAwcAIAEGeAaIMAcDBQAqAgiYMIGtAgI8yjCBpjBXBAIA
   ATBRMAYDBABD3fUwBgMEAKX+4TAJAwQApf7/AgEgMAYDBADAk6gwCQMEAcY6AgIBGDAJAwQB
   zAIeAgEYMAYDBADRGAEwBgMEANEYBTAGAwQA0RgJMEsEAgACMEUwDAMHASABBBgUTgIBQDAJ
   AwcAIAEGfCCMMAkDBwAgAQcoGAgwCQMHACYH+uACRTAJAwcAKg6yQAAAMAkDBwAqDrJAARgE
   IHcJpPLR0t3hgPqbLKcFWRX7fHWgUz6U+tcU86xB08eXo4HFMIHCMIGdMA4CAgOxMAgCAgWN
   AgIeJzATAgIeJzANAgIDsQICBY0CAwDu0jAbAgIsXjAVAgIDQwICA5wCAhsbAgJP+QIDAIhv
   MDACAi6/MCoCAgNDAgIFEwICGxsCAwCIOAIDAIhvAgMAxuUCAwDiyQIDA0cZAgMDSxQwJwIC
   Qg0wIQICGxsCAk/5AgMAoFsCAwDLOQIDANGjAgMDRdECAwYgYwQgfxMBQtXeKH5UT2mykfQQ
   HAuhJk6NoAuABMHs1ul/D26kgZUwgZIwbgQUC5zKkN0Neoo3ZmsZIX/g2EA3t6IEFBPU8k+a
   n82Y2zb5MGMYCMiPOXS8BBToVSsf1tGk9+QExtjlaA0evBY/wwQU62gPOPXWxxu0sQa4vQZY
   UBLaMbYEFPyKnLPtGE4X0w7qHg+nYVzksa9HBCC5umayvNVOSBIkn2DtLek1dnDMSP+EjxvD
   X1mGcD3nH6WCARkwggEVMIHwMIHtAgI8yjCB5jBxBBRdQlDi2B1ESNiinvzpHSn/B17J4jBZ
   MBMGByqGSM49AgEGCCqGSM49AwEHA0IABIBXI0P4P/ywEHqwB9jKafhrnKAwBgW4SKg998DT
   7F8ZwBm/prWe10K1TvQ0OlJQEobYoOfkHxCqU7RYIqn4gBUwcQQUvoibVdC3Nzl9dcSfSFuF
   j6mK0R8wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATgXEmvSfZu7HW5fUS+X5BbBli8hp0+
   Mu4VfabGoq4AZSEqevtUssOCsT76X2nl4faRZM1UA3bYVRTd1v9EqkTbBCC6X7RJzvtroA82
   Enliou6m6Gf+hRK73a3pxuS4vBbB0g==
```

It decodes as follows:

```
   File:                    testvector.der
   Hash identifier:         o4CdVc36d+/f9c8W/ui9Wl1/E8Fs+1MQLRxI0zjZ+HQ=
   CCR produced at:         Sun 12 Oct 2025 22:37:05 +0000
   Manifest state hash:     QTE0QTY4QjMxREE2QTIzQkY2RDkwRTA1NTJGQ0JBRUE=
   Manifest last update:    Sun 12 Oct 2025 21:00:03 +0000
   Manifest instances:
                            hash:AAAcOjvS+bajULr7A6fVPnJ94rQnS1QMmIbEly8CfUY= size:2072
aki:85B611A0B7D4334B7A2395E8CCE7B0E3C9B838E8 seqnum:11D8 thisupdate:1760284929 sia:rsync:
//rpki.ripe.net/repository/DEFAULT/98/9d563d-c470-43b3-82bb-88cb4e7106ea/1/hbYRoLfUM0t6I5
XozOew48m4OOg.mft
                            hash:AABagYSizHH1sGBKuaaMPjDuuPnIqquzYCccyLYpNbA= size:2113
aki:66EA0F83BDD3632BFF19400B3A1BA6FEDFFC5587 seqnum:34D8 thisupdate:1760282708 sia:rsync:
//rpki.apnic.net/member_repository/A917CB63/E1B054FC1DA711E2B688EBA108B02CD2/ZuoPg73TYyv_
GUALOhum_t_8VYc.mft
                            hash:AAGCg7kka6eCMNVoPED8zAHbZx1RUOfUy0gXAj63fUo= size:2443
aki:54035D9DC6C9A8AC72F6C05884A6E77C07BA38D3 seqnum:010D0C9F43285849F5C72229256006E408C93
D50 thisupdate:1760274003 sia:rsync://rpki.arin.net/repository/arin-rpki-ta/5e4a23ea-e80a
-403e-b08c-2171da2157d3/d6b5ad28-1cbc-47ab-904e-45361a5487c3/b0b793c2-6ed4-4642-8683-e5b6
1e8d9f76/b0b793c2-6ed4-4642-8683-e5b61e8d9f76.mft
                            hash:AM3mKEkgLWn/W2gQqYtpFDb2cml8MfNPNbIjqmz7J0Y= size:2375
aki:0C2CDBE897EC9327272018481B6D3FC7C639BE73 seqnum:010D0C9F432858413F7AFC49DB82945B2E171
961 thisupdate:1760284808 sia:rsync://rpki.arin.net/repository/arin-rpki-ta/5e4a23ea-e80a
-403e-b08c-2171da2157d3/a73420cb-b3cc-4b03-bda7-1be204933ae5/88c69486-3e14-4f26-9f99-02cf
7aaab7bf/88c69486-3e14-4f26-9f99-02cf7aaab7bf.mft subordinates:750FD3BA0F6C08563CDDBE9119
79FB122797649C
                            hash:BKrD9JAb5QaRJmmjFee1D7fM5eMeFSHCxmXs18XIFDw= size:2375
aki:232AE949803BA995690E1F5C8F7D0A2A177338C0 seqnum:010D0C9F4328584073A8551444BB0F971D33D
6B6 thisupdate:1760274003 sia:rsync://rpki.arin.net/repository/arin-rpki-ta/5e4a23ea-e80a
-403e-b08c-2171da2157d3/f60c9f32-a87c-4339-a2f3-6299a3b02e29/317008f4-3048-4330-a34b-2a36
dfe0f036/317008f4-3048-4330-a34b-2a36dfe0f036.mft subordinates:BFA2750976CA07F56A68976B0F
01EB862F17C3B3
```

```
                              hash:BK/QKKOPGVAWh0dlb1On+2zK2N0459cPk73dw8Sw3k4= size:2375
aki:BEF8B5F9234713559146F29C269F1B555EA012CB seqnum:010D0C9F43285841619BFFB50D5AE9970D2C0
8A4 thisupdate:1760302803 sia:rsync://rpki.arin.net/repository/arin-rpki-ta/5e4a23ea-e80a
-403e-b08c-2171da2157d3/a73420cb-b3cc-4b03-bda7-1be204933ae5/46bf1f03-2ebd-405e-a5b7-62bd
f3d7dbe6/46bf1f03-2ebd-405e-a5b7-62bdf3d7dbe6.mft subordinates:CB0886D20448A663C7CF5C4E19
79AC6F79DB0520
                              hash:DhZ5vv97/QzUkkv9ZKRYVkkamvfDmBMAJEsXGF0qsCI= size:2174
aki:6F1A103E1427FF03483ABFD9E34DACBE1524FF8B seqnum:0F17 thisupdate:1760228112 sia:rsync:
//rpki.afrinic.net/repository/apnic/bxoQPhQn_wNIOr_Z402svhUk_4s.mft subordinates:EEF75324
38DDA6A324764ACAF84EF624E177E0C5,72F087414CE2DF44BC4F4DFF5BE1147A7A71A9AE,53F78D80CAC0EB2
EACD77B0175DF319E8F752796
   ROA payload state hash:    NzcwOUE0RjJEMUQyRERFMTgwRkE5QjJDQTcwNTU5MTU=
   ROA payload entries:
                              192.35.94.0/24-32 AS 7
                              192.67.43.0/24-32 AS 7
```

```
                              194.32.69.0/24-32 AS 7
                              194.32.218.0/23-32 AS 7
                              194.34.138.0/24-32 AS 7
                              194.61.92.0/23-32 AS 7
                              2a0b:3b40::/29-128 AS 7
                              91.208.34.0/24 AS 8283
                              94.142.240.0/24 AS 8283
                              94.142.240.0/21 AS 8283
                              94.142.241.0/24 AS 8283
                              94.142.242.0/24 AS 8283
                              94.142.244.0/24 AS 8283
                              94.142.245.0/24 AS 8283
                              94.142.246.0/24 AS 8283
                              94.142.247.0/24 AS 8283
                              185.52.224.0/24 AS 8283
                              185.52.224.0/22 AS 8283
                              185.52.225.0/24 AS 8283
                              185.52.226.0/24 AS 8283
                              185.52.227.0/24 AS 8283
                              203.56.44.0/24 AS 8283
                              2001:678:688::/48 AS 8283
                              2a02:898::/32 AS 8283
                              67.221.245.0/24 AS 15562
                              165.254.225.0/24 AS 15562
                              165.254.255.0/24-32 AS 15562
                              192.147.168.0/24 AS 15562
                              198.58.2.0/23-24 AS 15562
                              204.2.30.0/23-24 AS 15562
                              209.24.1.0/24 AS 15562
                              209.24.5.0/24 AS 15562
                              209.24.9.0/24 AS 15562
                              2001:418:144e::/47-64 AS 15562
                              2001:67c:208c::/48 AS 15562
                              2001:728:1808::/48 AS 15562
                              2607:fae0:245::/48 AS 15562
                              2a0e:b240::/48 AS 15562
                              2a0e:b240:118::/48 AS 15562
   ASPA payload state hash:  N0YxMzAxNDJENURFMjg3RTU0NEY2OUIyOTFGNDEwMUM=
   ASPA payload entries:
                              customer: 945 providers: 1421, 7719
                              customer: 7719 providers: 945, 1421, 61138
                              customer: 11358 providers: 835, 924, 6939, 20473, 34927
                              customer: 11967 providers: 835, 1299, 6939, 34872, 34927, 50
917, 58057, 214809, 215828
                              customer: 16909 providers: 6939, 20473, 41051, 52025, 53667,
 214481, 401507
   Trust anchor state hash:  QjlCQTY2QjJCQ0Q1NEU0ODEyMjQ5RjYwRUQyREU5MzU=
   Trust anchor keyids:      0B9CCA90DD0D7A8A37666B19217FE0D84037B7A2, 13D4F24F9A9FCD98DB
36F930631808C88F3974BC, E8552B1FD6D1A4F7E404C6D8E5680D1EBC163FC3, EB680F38F5D6C71BB4B106B
8BD06585012DA31B6, FC8A9CB3ED184E17D30EEA1E0FA7615CE4B1AF47
   Router key state hash:    QkE1RkI0NDlDRUZCNkJBMDBGMzYxMjc5NjJBMkVFQTY=
   Router keys:
```

asid:15562 ski:5D4250E2D81D4448D8A29EFCE91D29FF075EC9E2 pubkey:MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEgFcjQ/g//LAQerAH2Mpp+GucoDAGBbhIqD33wNPsXxnAGb+mtZ7XQrVO9DQ6UlAShtig5+QfEKpTtFgiqfiAFQ==
asid:15562 ski:BE889B55D0B737397D75C49F485B858FA98AD11F pubkey:MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE4FxJr0n2bux1uX1Evl+QWwZYvIadPjLuFX2mxqKuAGUhKnr7VLLDgrE++l9p5eH2kWTNVAN22FUU3db/RKpE2w==
Validation: N/A

Appendix C. Implementation status

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

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in RFC 7942. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to RFC 7942, "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

* Example .ccr files were created by Job Snijders. A current example CCR (regenerated every few minutes) is available here: https://console.rpki-client.org/rpki.ccr

* A CCR serializer and deserializer implementation based on [rpki-client] was provided by Job Snijders.

* Another CCR serializer and deserializer implementation based on [rpkitouch] was provided by Job Snijders.

Authors' Addresses

Job Snijders
BSD Software Development
Amsterdam
Netherlands
Email: job@bsd.nl
URI: https://www.bsd.nl

Bart Bakker
RIPE NCC
Netherlands
Email: bbakker@ripe.net

Tim Bruijnzeels
RIPE NCC
Netherlands
Email: tbruijnzeels@ripe.net