

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 10 August 2026

A. Azimov  
Yandex  
E. Uskov  
JetLend  
R. Bush  
Internet Initiative Japan  
J. Snijders  
BSD  
R. Housley  
Vigil Security  
B. Maddison  
Workonline  
6 February 2026

A Profile for Autonomous System Provider Authorization  
draft-ietf-sidrops-aspa-profile-22

Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for Autonomous System Provider Authorization (ASPA) objects for use with the Resource Public Key Infrastructure (RPKI). An ASPA 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 providers. When validated, an ASPA's eContent can be used for detection and mitigation of route leaks.

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.

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 10 August 2026.

## Copyright Notice

Copyright (c) 2026 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
2. ASPA Content Type . . . . .	4
3. ASPA eContent . . . . .	4
3.1. version . . . . .	5
3.2. customerASID . . . . .	5
3.3. providers . . . . .	5
4. ASPA Validation . . . . .	6
5. IANA Considerations . . . . .	6
5.1. SMI Security for S/MIME Module Identifier registry . . . . .	7
5.2. SMI Security for S/MIME CMS Content Type registry . . . . .	7
5.3. RPKI Signed Object registry . . . . .	7
5.4. RPKI Repository Name Scheme registry . . . . .	7
5.5. Media Type registry . . . . .	7
6. Implementation Considerations . . . . .	8
7. Security Considerations . . . . .	9
8. Implementation status . . . . .	9
9. Acknowledgments . . . . .	10
Contributors . . . . .	10
References . . . . .	10
Normative References . . . . .	10
Informative References . . . . .	11
Appendix A. Example ASPA eContent Payload . . . . .	12
Authors' Addresses . . . . .	14

## 1. Introduction

The primary purpose of the Resource Public Key Infrastructure (RPKI) is to improve routing security [RFC6480]. As part of this infrastructure, a mechanism is needed to facilitate holders of Autonomous System (AS) identifiers in their capacity as Customer to authorize other ASes as their Provider(s). A Provider AS (PAS) is a network that:

- a. offers its customers outbound (customer to Internet) data traffic connectivity and/or
- b. further propagates in all directions (towards providers, lateral peers, and customers) any BGP Updates that the customer may send.

The digitally signed Autonomous System Provider Authorization (ASPA) object described in this document provides the above-mentioned authorization mechanism.

An ASPA object is a cryptographically verifiable attestation signed by the holder of an Autonomous System identifier (hereafter called the "Customer AS", or CAS). An ASPA contains a list of one or more ASes, each listing meaning the listed AS is authorized to act as Provider network. When the CAS has multiple Providers, all Provider ASes are listed in the ASPA, including any non-transparent Internet Exchange Point (IXP) Route Server (RS) ASes. The common case for RS ASes at IXPs is to operate transparently (see Section 2.2.2.1 [RFC7947]), and in those instances the ASNs of IXP Route Servers are not listed as PAS in ASPAs.

The BGP Roles that an Autonomous System (AS) may have in its peering relationships with eBGP neighbors are discussed in [I-D.ietf-sidrops-aspa-verification]. The details of ASPA registration requirements for ASes in different scenarios are also specified in that document. In addition, the procedures for verifying AS\_PATHs in BGP UPDATE messages using Validated ASPA Payloads (VAPs) are described in that document.

This CMS [RFC5652] protected content type definition conforms to the [RFC6488] template for RPKI signed objects. In accordance with Section 4 of [RFC6488], this document defines:

1. The object identifier (OID) that identifies the ASPA 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 ASPA content, which is the payload signed by the CAS. The ASPA content is encoded using the ASN.1 [X.680] Distinguished Encoding Rules (DER) [X.690].
3. The steps required to validate an ASPA beyond the validation steps specified in [RFC6488].

## 2. ASPA Content Type

The content-type for an ASPA is defined as id-ct-ASPA, which has the numerical value of 1.2.840.113549.1.9.16.1.49. 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]).

## 3. ASPA eContent

The content of an ASPA identifies the Customer AS (CAS) as well as the Set of Provider ASes (SPAS) that are authorized by the CAS to be its Providers.

A user registering ASPA(s) must be cognizant of Sections 2, 3, and 4 of [I-D.ietf-sidrops-asma-verification] and the user (or their software tool) must comply with the ASPA registration recommendations in Section 4 of that document.

It is highly recommended that for a given Customer AS, a single ASPA object be maintained which contains all providers, including any non-transparent RS ASes. Such a practice helps prevent race conditions during ASPA updates. Otherwise, said race conditions might affect route propagation. The software that provides hosting for ASPA records SHOULD support enforcement of this recommendation. In the case of the transition process between different CA registries, the ASPA records SHOULD be kept identical in all registries in terms of their authorization contents.

The eContent of an ASPA is an instance of ASProviderAttestation, formally defined by the following ASN.1 [X.680] module:

```
RPKI-ASPA-2023
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) smime(16) modules(0) id-mod-rpki-aspa-2023(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-ASPA OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) id-smime(16) id-ct(1) aspa(49) }

ct-ASPA CONTENT-TYPE ::=
{ TYPE ASProviderAttestation IDENTIFIED BY id-ct-ASPA }

ASProviderAttestation ::= SEQUENCE {
  version [0]    INTEGER DEFAULT 0,
  customerASID   ASID,
  providers       ProviderASSet }

ProviderASSet ::= SEQUENCE (SIZE(1..MAX)) OF ASID

ASID ::= INTEGER (0..4294967295)

END
```

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

### 3.1. version

The version number of the ASProviderAttestation that complies with this specification MUST be 1 and MUST be explicitly encoded.

### 3.2. customerASID

The customerASID field contains the AS number of the Customer Autonomous System that is the authorizing entity.

### 3.3. providers

The providers field contains the listing of ASes that are authorized as providers.

Each element contained in the providers field is an instance of ASID. Each ASID element contains the AS number of an AS that has been authorized by the customer AS as its provider or RS.

In addition to the constraints described by the formal ASN.1 definition, the contents of the providers field MUST satisfy the following constraints:

- \* The CustomerASID value MUST NOT appear in any ASID in the providers field.
- \* The elements of providers MUST be ordered in ascending numerical order.
- \* Each value of ASID MUST be unique (with respect to the other elements of providers).
- \* An ASID value of 0 can only be encoded in the providers field as a single item list, i.e., an element for AS 0 MUST NOT appear alongside any other elements.

#### 4. ASPA Validation

Before a relying party can use an ASPA to validate a routing announcement, the relying party MUST first validate the ASPA object itself. To validate an ASPA, the relying party MUST perform all the validation checks specified in [RFC6488] as well as the following additional ASPA-specific validation steps.

- \* The Autonomous System Identifier Delegation Extension [RFC3779] MUST be present in the end-entity (EE) certificate (contained within the ASPA), and the Customer ASID in the ASPA 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.

#### 5. IANA Considerations

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

Please add the id-mod-rpki-aspa-2023 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
TBD2	id-mod-rpki-aspa-2023	[RFC-to-be]

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

Please add the ASPA 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
49	id-ct-ASPA	[RFC-to-be]

### 5.3. RPKI Signed Object registry

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

Name	OID	Specification
Autonomous System Provider Authorization	1.2.840.113549.1.9.16.1.49	[RFC-to-be]

### 5.4. RPKI Repository Name Scheme registry

Please add an item for the Autonomous System Provider Authorization file extension to the "RPKI Repository Name Scheme" registry created by [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.asa	Autonomous System Provider Authorization	[RFC-to-be]

### 5.5. Media Type registry

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

Type name: application  
Subtype name: rpki-aspa  
Required parameters: N/A  
Optional parameters: N/A  
Encoding considerations: binary  
Security considerations: Carries an RPKI ASPA [RFC-to-be].  
    This media type contains no active content. See  
    Section 4 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 as defined in [RFC-to-be].  
    Magic number(s): None  
    File extension(s): .asa  
    Macintosh file type code(s):  
Person & email address to contact for further information:  
    Job Snijders <job@sobornost.net>  
Intended usage: COMMON  
Restrictions on usage: None  
Change controller: IETF

## 6. Implementation Considerations

While the ASN.1 profile specified in Section 3 imposes no limit on the number of Provider ASes that can be listed for a given Customer ASID, consideration will need to be given to limitations existing in validators and elsewhere in the RPKI supply chain. For example, the number of Provider ASes that can be listed in a single RPKI-To-Router protocol ASPA PDU (following the Length field constraints in Section 5.1 of [I-D.ietf-sidrops-8210bis]) is 16,380 providers. In addition to protocol limitations in the supply chain, locally defined restrictions could exist for the maximum file size of signed objects a Relying Party implementation is willing to accept.

Relying Party implementations are RECOMMENDED to impose an upper bound on the number of Provider ASes for a given Customer ASID. An upper bound value between 4,000 and 10,000 Provider ASes is suggested. If this threshold is exceeded, Relying Party implementations SHOULD treat all ASPA objects related to the Customer ASID invalid; e.g. not emit a partial list of Provider ASes. Additionally, an error SHOULD be logged in the local system, indicating the Customer ASID for which the threshold was exceeded.

Implementers and operators SHOULD periodically review whether imposed upper bounds still are reasonable in context of the global Internet routing system.

## 7. Security Considerations

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

## 8. 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".

- \* A validator implementation [rpki-client] (version 8.5 and higher), written in C was provided by Job Snijders.
- \* A validator implementation [routinator], written in Rust was provided by Martin Hoffman from NLnet Labs.
- \* A validator implementation [rpki-prover], written in Haskell was provided by Mikhail Puzanov.
- \* A signer implementation [rpki-aspa-demo] in Perl was reported on Tom Harrison from APNIC.
- \* A signer implementation [rpki-commons] in Java was reported on by Ties de Kock from RIPE NCC.

- \* A signer implementation [krill] in Rust was reported on by Tim Bruijnzeels from NLnet Labs.

## 9. Acknowledgments

The authors would like to thank Keyur Patel for helping kick-start the ASPA profile project, Ties de Kock & Tim Bruijnzeels for suggesting that the ProviderASSet be in a canonical form, and Claudio Jeker & Martin Hoffman for review and several suggestions for improvements.

## Contributors

The following people made significant contributions to this document:

Kotikalapudi Sriram  
USA National Institute of Standards and Technology  
Email: ksriram@nist.gov

## References

### Normative References

- [I-D.ietf-sidrops-8210bis]  
Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 2", Work in Progress, Internet-Draft, draft-ietf-sidrops-8210bis-23, 19 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-8210bis-23>>.
- [I-D.ietf-sidrops-aspa-verification]  
Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS\_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-24, 19 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-24>>.
- [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>>.

- [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/info/rfc3779>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/info/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/info/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/info/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/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>>.
- [X.680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 2021.
- [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)", ITU-T Recommendation X.690, 2021.

#### Informative References

- [krill] Bruijnzeels, T., "krill", 2023, <[https://mailarchive.ietf.org/arch/msg/sidrops/RrHCYTmevxDHgebdLC\\_adRlKH-o/](https://mailarchive.ietf.org/arch/msg/sidrops/RrHCYTmevxDHgebdLC_adRlKH-o/)>.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <<https://www.rfc-editor.org/info/rfc4648>>.

[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/info/rfc6480>>.

[RFC7947] Jasinska, E., Hilliard, N., Raszuk, R., and N. Bakker, "Internet Exchange BGP Route Server", RFC 7947, DOI 10.17487/RFC7947, September 2016, <<https://www.rfc-editor.org/info/rfc7947>>.

[routinator]  
Hoffman, M., "routinator", 2023,  
<<https://github.com/NLnetLabs/rpki-rs/pull/264>>.

[rpki-aspa-demo]  
Harrison, T., "rpki-aspa-demo", 2023,  
<<https://github.com/APNIC-net/rpki-aspa-demo>>.

[rpki-client]  
Jeker, C., Snijders, J., Dzonsons, K., and T. Buehler, "OpenBSD rpki-client", 2023,  
<<https://www.rpki-client.org/>>.

[rpki-commons]  
de Kock, T., "rpki-commons", 2023,  
<<https://mailarchive.ietf.org/arch/msg/sidrops/nNAmZMrr7t9NMzml2jRXU03ABN4/>>.

[rpki-prover]  
Puzanov, M., "rpki-prover", 2023,  
<<https://github.com/lolepezy/rpki-prover/compare/master...aspa-profile-16>>.

#### Appendix A. Example ASPA eContent Payload

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

```
$ echo 301DA003020101020300FE633011020300FC00020301000F020500FA56EA00 \  
| xxd -r -ps | openssl asn1parse -inform DER -dump -i  
0:d=0 hl=2 l= 29 cons: SEQUENCE  
2:d=1 hl=2 l= 3 cons: cont [ 0 ]  
4:d=2 hl=2 l= 1 prim: INTEGER :01  
7:d=1 hl=2 l= 3 prim: INTEGER :FE63 # Customer ASID 65123  
12:d=1 hl=2 l= 17 cons: SEQUENCE  
14:d=2 hl=2 l= 3 prim: INTEGER :FC00 # ProviderAS 64512  
19:d=2 hl=2 l= 3 prim: INTEGER :01000F # ProviderAS 65551  
24:d=2 hl=2 l= 5 prim: INTEGER :FA56EA00 # ProviderAS 4200000000
```

Below is a complete Base64 [RFC4648] encoded RPKI ASPA Signed Object.

```
MIIGLAYJKoZIhvcNAQcCoIIIGHTCCBhkCAQMxDtALBglghkgBZQMEAgEwMAYLKoZI
hvcNAQkQATGgIQQfMB2gAwIBAQIDAP5jMBECAwD8AAIDAQAPAgUA+lbqAKCCBCMw
ggQfMIIDB6ADAgECAgEEMA0GCSqGSIB3DQEBCwUAMA8xDtALBglghkgBZQMEAgEw
HhcNMjUwMTA2MTAyNjQ4WhcNMjYwMTA2MTAyNjQ4WjAPMQ0wCwYDVQQDEwRyb290
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmgjRVMrjafIK81cxs8GB
ehcj1P97o3CdlhceX8ogtUE19C1v3VZQttdzaBG1ViI2+TJiyueHm2M6nq7t17A9
HfkPWGdvwjTUEf4ynpxNlqqoG5pGPMLuuk6HdVaKbuEeX3ZAYD2daG8qm3zkmmF3
F7e+xPvr6nCTIQX7nr0WQyX74FmLGwlr6TV+6MGdCnp24A5aCXJo3mlvG1QUKdd/
bMsZpbfbzaX1rxBKA0GSdWx/QEOxFb1BPObjF+P/GpDXOq3i0DoZiDB+omgdUAWDZ
dmskG0l+2EyQaCS/pVCES50Y5zAagTcFabCLKnPvr3qh9tvjD/KlolyC35gNiFoX
7wIDAQABo4IBhDCCAYAwDgYDVR0PAQH/BAQDAgeAMB0GA1UdDgQWBBQrh8dvXu72
IET1KLgskpsolVcyrDafBgNVHSMEGDAWgBQ2mtAZLGdOeDIizTKFZreUErGPJjAY
BgNVHSABaf8EDjAMMAoGCCsGAQUFBw4CMF8GCCsGAQUFBwEBBFMwUTBpBggrBgEF
BQcwAoZDcnN5bmM6Ly9sb2NhbGhvc3Qvcmlvby8zNj1BRDAXOTJDNjc0RTc4MzIy
MkNEMzI4NTY2QjJc5NDEyQjE4RjI2LmNlcjBxBG9wMDU0FEMDE5MkM2NzRFNzgZMjIy
YzovL2xvY2FsaG9zZDc5YXZBbVl3RhLzZM2OUFEMDE5MkM2NzRFNzgZMjIyQ0Qz
Mjg1NjZCNzk0MTJCMThGMjYyY3JSMd4GCCsGAQUFBwELBDIwMDAuBggrBgEFBQcwC4Yi
cnN5bmM6Ly9sb2NhbGhvc3QvdGEvYW4tb2JqZW50LmFzYTAaBggrBgEFBQcBCAEB
/wQLMAmGbzAFAGMA/mMwDQYJKoZIhvcNAQELBQADggEBACqgWrD692DUuN1jrriv
SGqI7JqAtbqOSvnwxNGM1PZ6oTKarf4aDMJNcwqMaOUOzZPQ9VXA48h5R8TgvAub
s/HJ263DLtPiScwkWqLZZs6Ius2zFothzDwW0oe/rHKiecCF0YpJqFhaa6dw6vs0
zK77Ze+GfalSeeuI1DTwGDjiNBtXCaRxAPmvpYGxSKQmRYCio6vKPSZlZCPqzEZA
MVCmxdlaDQjVPUuWLBfV/bbZmS4wM1nbikt5WLZEVHMcAyyqWOb7a3KO2GIiw0Ak9
O6JgUoex/8y0s6smSWCre2y9d6kAhT0COW1KvFoNM5lFKSelrYqTtMFY33XfCI7e
IgsxggGqMIIBPgIBA4AUK4fHb17u9iBE9Si4LJKbKNVXMqwwCwYJYIZIAWUDBAIB
oGswGgYJKoZIhvcNAQkDMQ0GCyqGSIB3DQEJEAExMBwGCSqGSIB3DQEJBTEPFw0y
NTAxMDYxMDI2NDhaMC8GCSqGSIB3DQEJBDEiBCCLMweRYDN5u5auRQYv6+Dx+b9X
mlt5R3gkH9c3aX40gzANBgkqhkiG9w0BAQEFAASCAQATWDI3fYgku2fJPzFXAbnz
IKabFMRvhp9LAhvl8oPkCp0zQu4SyJsdvoWxkpHKnXGwwdgub/d4GF0weoJgauDr
ugUsB2e40aQwFoTyPcVuS/BirhlW5j0NwYovmuJ9GiBe67/sCRBaPC5sBKRBP0Iv
IpMpAe2QhaoeDUDc0KYCM42f1kFD+PD8PnlvXRisL3A3OFhB+0LY1Z3xivRAEdtf
qzobZT0Hq6CilAajNeocG0gmFjJ/lFyElLkJdfGHZCWLNVNX2I+9GbDDdYV13cUTG
yk5CFeQWetsX7D7XRNSdKwrrW6qWK/KxGF38SsuGeTyDQiNcOhwqvSfFc388ge/G
```

The above should decode as following:

Object SHA256 hash: S6B+jKOCFXPlRn7ws6Kd5tgpsSx609tJZpw60CVaf9Y=  
EE Subject key identifier: 2B:87:C7:6F:5E:EE:F6:20:44:F5:28:B8:2C:92:9B:28:D5:57:32:AC  
EE Certificate issuer: /CN=root  
EE Certificate serial: 04  
EE Authority key identifier: 36:9A:D0:19:2C:67:4E:78:32:22:CD:32:85:66:B7:94:12:B1:8F:26  
EE Authority info access: rsync://localhost/repo/369AD0192C674E783222CD328566B79412B18  
F26.cer  
EE Subject info access: rsync://localhost/ta/an-object.asa  
CMS Signing time: Mon 06 Jan 2025 10:26:48 +0000  
EE notBefore: Mon 06 Jan 2025 10:26:48 +0000  
EE notAfter: Tue 06 Jan 2026 10:26:48 +0000

ASPA eContent:  
Customer AS: 65123  
Provider Set:  
1: AS: 64512  
2: AS: 65551  
3: AS: 4200000000

#### Authors' Addresses

Alexander Azimov  
Yandex  
Email: a.e.azimov@gmail.com

Eugene Uskov  
JetLend  
Email: eu@jetlend.ru

Randy Bush  
Internet Initiative Japan  
Email: randy@psg.com

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

Russ Housley  
Vigil Security, LLC  
918 Spring Knoll Drive  
Herndon, VA 20170  
United States of America

Email: housley@vigilsec.com

Ben Maddison  
Workonline  
Cape Town  
South Africa  
Email: benm@workonline.africa