Workgroup: Network Working Group
Internet-Draft:
draft-ietf-sidrops-aspa-profile-09
Published: 29 July 2022
Intended Status: Standards Track
Expires: 30 January 2023

Authors: A. Azimov E. Uskov R. Bush
Yandex JetLend Internet Initiative Japan
J. Snijders R. Housley B. Maddison
Fastly Vigil Security Workonline

A Profile for Autonomous System Provider Authorization

Abstract

This document defines a standard profile for Autonomous System Provider Authorization in the Resource Public Key Infrastructure. An Autonomous System Provider Authorization is a digitally signed object that provides a means of validating that a Customer Autonomous System holder has authorized members of Provider set to be its upstream providers or provide route server service at internet exchange point. For the Providers it means that they are legal to send prefixes received from the Customer Autonomous System in all directions including providers and peers.

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

Copyright Notice

Table of Contents

1. Introduction
2. The ASPA Content Type
3. The ASPA eContent
  3.1. version
  3.2. customerASID
  3.3. providers
    3.3.1. ProviderAS
      3.3.1.1. providerASID
      3.3.1.2. afiLimit
4. ASPA Validation
5. IANA Considerations
6. Security Considerations
7. Implementation status
8. Acknowledgments
9. References
  9.1. Normative References
  9.2. Informative References
Authors' Addresses

1. Introduction

The primary purpose of the Resource Public Key Infrastructure (RPKI) is to improve routing security. (See [RFC6480] for more information.) As part of this infrastructure, a mechanism is needed to validate that a AS has permission from a Customer AS (CAS) holder to send routes in all directions. The digitally signed Autonomous System Provider Authorization (ASPA) object provides this validation mechanism.

The ASPA uses the template for RPKI digitally signed objects [RFC6488], which defines a Cryptographic Message Syntax (CMS) [RFC5652] wrapper for the ASPA content as well as a generic validation procedure for RPKI signed objects. As ASPAs need to be validated with RPKI certificates issued by the current infrastructure, we assume the mandatory-to-implement algorithms in [RFC6485], or its successor.

To complete the specification of the ASPA (see 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 [X680] Distinguished Encoding Rules (DER) [X690].

3. The steps required to validate an ASPA beyond the validation steps specified in [RFC6488]).

2. The 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. The ASPA eContent

The content of an ASPA identifies the Customer AS (CAS) as well as the Set of Provider ASes (SPAS) that are authorized to further propagate announcements received from the customer.

Not all route servers at internet exchange points are transparent, e.g. in some cases they are present in the ASPATH. In this case route server AS is acting as a provider AS, which propagates routes between its customers. Thus, a customer MUST add both upstream providers and non-transparent route sever AS it is connected to its SPAS.

If customer is connected to multiple transit providers/non-transparent route servers they MUST be registered in a single ASPA object. This rule is important to avoid possible race conditions during updates.

The eContent of an ASPA is an instance of ASProviderAttestation, formally defined by the following ASN.1 [X680] module:

```
RPKI-ASPA-2022
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-9(9) smime(16) modules(0) id-mod-rpki-aspa-2020(TBD) }

DEFINITIONS IMPLICIT 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) 49 }

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

ASProviderAttestation ::= SEQUENCE {
  version [0]   ASPAVersion DEFAULT v0,
  customerASID  ASID,
  providers     ProviderASSet }

ASPAVersion ::= INTEGER  { v0(0) }

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

ProviderAS ::= SEQUENCE {
  providerASID  ASID,
  afiLimit      AddressFamilyIdentifier OPTIONAL }

ASID ::= INTEGER

AddressFamilyIdentifier ::= OCTET STRING (SIZE (2))

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 MUST be v0.

3.2. customerASID

The customerASID field contains the AS number of the Autonomous System (AS) that authorizes a collection of provider ASes (as listed in the providerASSet) to propagate prefixes in the specified address family to other ASes.

3.3. providers

The providers field contains the listing of ASes that are authorized to further propagate announcements in the specified address family received from the customer.

Each element contained in the providers field is an instance of ProviderAS.

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

- The elements of providers MUST be ordered in ascending numerical order by the value of the providerASID field.

- Each value of providerASID MUST be unique (with respect to the other elements of providers).

3.3.1. ProviderAS

3.3.1.1. providerASID

The providerASID field contains the AS number of an AS that has been authorized by the customer AS to propagate prefixes in the specified address family to other ASes.

3.3.1.2. afiLimit

The afiLimit field optionally constrains the authorization given to the provider AS to a single address family.

If present, it contains the two-octet Address Family Identifier (AFI) for which the relation between the customer and provider is authorized. Only permitted AFI values are the IPv4 and IPv6 AFI values as specified in [IANA-AF].

If omitted, the authorization is valid for both IPv4 and IPv6 announcements.

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 step.

- The autonomous system identifier delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the ASPA), and the customer AS number in the ASPA is contained within the set of AS numbers specified by the EE certificate's autonomous system identifier delegation extension.

5. IANA Considerations

Please add the id-mod-rpki-aspa-2022 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-2022	[ThisRFC]

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	[ThisRFC]

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
Autonomous System Provider Authorization	1.2.840.113549.1.9.16.1.4

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	[draft-ietf-sidr

6. Security Considerations

While it's not restricted, but it's highly recommended maintaining for selected Customer AS a single ASPA object that covers all connected providers/route servers. Such policy should prevent race conditions during ASPA updates that might affect prefix propagation. The software that provides hosting for ASPA records SHOULD support enforcement of this rule. In the case of the transition process between different CA registries, the ASPA records SHOULD be kept identical in all registries.

7. 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] written in C based on the OpenBSD RPKI Validator was provided by Job Snijders from Fastly.

*A signer and decoder implementation [rpkimancer] written in Python was provided by Ben Maddison from Workonline.

- *A signer implementation [krill] written in Rust was provided by Tim Bruijnzeels from NLnetLabs.

- *At IETF114 Ties de Kock from RIPE NCC shared a signer implementation had been developed internally.

- *Di Ma reported [rpstir2] success in RPSTIR2 validating objects produced by Tim Bruijnzeels.

8. Acknowledgments

The authors would like to thank Keyur Patel for helping kickstart the ASPA profile project; and Ties de Kock & Tim Bruijnzeels for suggesting that the ProviderASSet be in a canonical form.

9. References

9.1. Normative References

[IANA-AF] IANA, "Address Family Numbers", <https://www.iana.org/assignments/address-family-numbers/address-family-numbers.xhtml>.

[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>.

[X680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 2015.

[X690] 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, 2015.

9.2. Informative References

[krill] Bruijnzeels, T., "Krill", 2022, <https://github.com/NLnetLabs/krill>.

[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>.

[rpki-client] Snijders, J., "rpki-client", 2022, <https://mailarchive.ietf.org/arch/msg/sidrops/Jdowj_bDhN_T993SN4bbsWeDgGA/>.

[rpkimancer] Maddison, B., "rpkimancer-aspa", 2022, <https://github.com/benmaddison/rpkimancer-aspa>.

[rpstir2] Ma, D., "RPSTIR2", <https://mailarchive.ietf.org/arch/msg/sidrops/pxqAGPmR0MA3NMe-NxYyiEZ7RXw>.

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
Fastly
Amsterdam

Email: job@fastly.com

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