Network Working Group   A. Azimov
Internet-Draft   Yandex
Intended status: Standards Track   E. Uskov
Expires: May 6, 2021   JetLend
                                                          R. Bush
                                        Internet Initiative Japan
                                                         K. Patel
                                                           Arrcus
                                                      J. Snijders
                                                              NTT
                                                       R. Housley
                                                  Vigil Security
                                                 November 2, 2020

        A Profile for Autonomous System Provider Authorization
                draft-ietf-sidrops-aspa-profile-04

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 verifying that a Customer Autonomous System
   holder has authorized members of Provider set to be its upstream
   providers and for the Providers 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

   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 May 6, 2021.

Copyright Notice

Table of Contents

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 verify 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
verification 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-cct-ASPA, which 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 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. If customer has
multiple providers they MUST be registered in a single ASPA object.
This rule is important to avoid possible race conditions during
updates. An ASPA is formally defined as:

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

    id-ct-ASPA OBJECT IDENTIFIER ::= { id-ct TBD }

    ASProviderAttestation ::= SEQUENCE {
        version [0] ASPAVersion DEFAULT v0,
        AFI  AddressFamilyIdentifier,
        customerASID  ASID,
        providerASSET  SEQUENCE (SIZE(1..MAX)) OF ASID }

    ASPAVersion ::= INTEGER  { v0(0) }

    AddressFamilyIdentifier ::= OCTET STRING (SIZE (2..3))

    ASID ::= INTEGER
```

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. AFI

The AFI field contains Address Family Identifier for which the
relation between customer and provider ASes is authorized. Presently
defined values for the Address Family Identifier field are specified
in the IANA's Address Family Numbers registry [IANA-AF].

3.3. customerASID

The customerASID field contains the AS number of the Autonomous
System that authorizes an upstream providers (listed in the
providerASSET) to propagate prefixes in the specified address family
other ASes.

3.4. providerASSET

The providerASSET contains the sequence (set) of AS numbers that are
authorized to further propagate announcements in the specified
address family received from the customer.

[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.

   o 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](#). ASN.1 Module for the ASPA Content Type

```
RPKI-ASPA-2018
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
        pkcs-9(9) smime(16) modules(0) id-mod-rpki-aspa-2018(TBD2) }
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) } ;

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

--
-- ASPA Content Type
--

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

id-ct OBJECT IDENTIFIER ::= { id-smime 1 }

id-ct-ASPA OBJECT IDENTIFIER ::= { id-ct TBD }

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

ASProviderAttestation ::= SEQUENCE {
    version [0] ASPAVersion DEFAULT v0,
    AFI  AddressFamilyIdentifier,
    customerASID  ASID,
    providerASSET  SEQUENCE (SIZE(1..MAX)) OF ASID }

ASPAVersion ::= INTEGER  { v0(0) }

AddressFamilyIdentifier ::= INTEGER

ASID ::= INTEGER

END
```

6. IANA Considerations

Please add the id-mod-rpki-aspa-2018 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-2018       | [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
      -------------------------------------------------------------
      TBD       | id-ct-ASPA                  | [ThisRFC]
```

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

```
      Name      | OID                         | Specification
      -------------------------------------------------------------
      ASPA      | 1.2.840.113549.1.9.16.1.TBD  | [ThisRFC]
```

7. Security Considerations

   While it's not restricted, but it's highly recommended maintaining
   for selected Customer AS a single ASPA object that covers all its
   providers. 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.

8. Acknowledgments

9. References

9.1. Normative References

   [IANA-AF] IANA, "Address Family Numbers",
              <http://www.iana.org/numbers.html>.

   [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>.

   [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

   [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>.

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

Keyur Patel
Arrcus, Inc.

Email: keyur@arrcus.com

Job Snijders
NTT Communications
Theodorus Majofskistraat 100
Amsterdam 1065 SZ
The Netherlands

Email: job@ntt.net

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

Email: housley@vigilsec.com