Secure Inter-Domain Routing (SIDR)	T. Manderson	
Internet-Draft	May 26, 2009	
Intended status: Standards Track		
Expires: November 27, 2009		

TOC

A Profile for Bogon Origin Attestations (BOAs)
draft-ietf-sidr-bogons-03.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a standard profile for Bogon Origin Attestations (BOAs). A BOA is a digitally signed object that provides a means of verifying that an IP address block holder has not authorised any Autonomous System (AS) to originate routes that are equivalent to any of the addresses listed in the BOA. A BOA also provides a means of verifying that a BGP speaker is not using an AS without appropriate

authority. The proposed application of BOAs is intended to fit within the requirements for adding security measures to inter-domain routing, including the ability to support incremental and piecemeal deployment of such measures, and does not require any changes to the specification of the Border Gateway Protocol.

Table of Contents

---

1. Introduction

TOC

This document defines an application of the Resource Public Key Infrastructure (RPKI) to validate the attestations of resource holders and Internet Registries that certain addresses are currently neither allocated to any party, nor in use by any party, and any appearance of such addresses or AS's in a routing advertisement in the Border Gateway Protocol (BGP) [RFC4271] (Rekhter, Y., Li, T., and S. Hares, “A Border Gateway Protocol 4 (BGP-4),” January 2006.) should be considered an invalid use of such addresses or Autonomous System Numbers.
The RPKI is based on Resource Certificates. Resource Certificates are X.509 certificates that conform to the PKIX profile [RFC5280] (Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” May 2008.), and to the extensions for IP addresses and AS identifiers [RFC3779] (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” June 2004.). A Resource Certificate describes an action by an Issuer

that binds a list of IP address blocks and Autonomous System (AS) numbers to the Subject of a certificate, identified by the unique association of the Subject's private key with the public key contained in the Resource Certificate. The RPKI is structured such that each current Resource Certificate matches a current resource allocation or assignment. This is described in [I-D.ietf-sidr-arch] (Lepinski, M. and S. Kent, “An Infrastructure to Support Secure Internet Routing,” March 2009.).

BOAs can be regarded as a logical opposite of a Route Origin Authorization (ROA) [I-D.ietf-sidr-roa-format] (Lepinski, M., Kent, S., and D. Kong, “A Profile for Route Origin Authorizations (ROAs),” November 2008.), however are not contradictory to a ROA and allows a resource holder to explicitly list those IP addresses and AS's that are denoted by the holder as not validly appearing in any routing advertisement, and to make this attestation in a manner that a relying party can unambiguously validate under the framework of the RPKI.

A BOA is a digitally signed object that makes use of Cryptographic Message Syntax (CMS) [RFC3852] (Housley, R., “Cryptographic Message Syntax (CMS),” July 2004.) as a standard encapsulation format. CMS was chosen to take advantage of existing open source software available for processing messages in this format.

---

2. Basic Format

TOC

Using CMS syntax, a BOA is a type of signed-data object. The general format of a CMS object is:

```
ContentInfo ::= SEQUENCE {
  contentType ContentType,
  content [0] EXPLICIT ANY DEFINED BY contentType }

ContentType ::= OBJECT IDENTIFIER
```

2.1. Signed-Data Content Type

TOC

According to the CMS specification, The signed-data content type shall have ASN.1 type SignedData:

```
SignedData ::= SEQUENCE {
  version CMSVersion,
  digestAlgorithms DigestAlgorithmIdentifiers,
  encapContentInfo EncapsulatedContentInfo,
  certificates [0] IMPLICIT CertificateSet OPTIONAL,
  crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
  signerInfos SignerInfos }

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

SignerInfos ::= SET OF SignerInfo
```

2.1.1. version

TOC

The version is the syntax version number. It MUST be 3, corresponding to the signerInfo structure having version number 3.

2.1.2. digestAlgorithms

TOC

The digestAlgorithms set MUST include only SHA-256, the OID for which is 2.16.840.1.101.3.4.2.1. [RFC4055] (Schaad, J., Kaliski, B., and R. Housley, “Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” June 2005.). It MUST NOT contain any other algorithms.

2.1.3. encapContentInfo

TOC

encapContentInfo is the signed content, consisting of a content type identifier and the content itself.

```
EncapsulatedContentInfo ::= SEQUENCE {
  eContentType ContentType,
  eContent [0] EXPLICIT OCTET STRING OPTIONAL }

ContentType ::= OBJECT IDENTIFIER
```

2.1.3.1. eContentType

TOC

The ContentType for a BOA is defined as id-ct-rpkiBOA, and has the numerical value of 1.2.840.113549.1.9.16.1.[TBD]. [This value needs to be assigned via an OID registration.]

```
id-smime OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
    rsadsi(113549) pkcs(1) pkcs9(9) 16 }

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

id-ct-rpkiBOA OBJECT IDENTIFIER ::= { id-ct [TBD] }
```

2.1.3.2. eContent

TOC

The content of a BOA identifies a list of one or more AS's and one or more IP address prefixes that are asserted to be "bogons" and, accordingly, BOAs are intended to act as a constraint on the routing system to signal that no route object that that relates to these AS's or IP addresses should be interpreted as representing a valid routing attestation. A BOA is formally defined as:

```
id-ct-rpkiBOA ::= {
   version [0] INTEGER DEFAULT 0,
   asIDs        SEQUENCE OF asIdsOrRange,
   ipAddrBlocks SEQUENCE OF BOAIPAddressFamily }

ASIdOrRange   ::= CHOICE {
   id               ASId,
   range            ASRange }

ASRange       ::= SEQUENCE {
   min              ASId,
   max              ASId }

ASId          ::= INTEGER

BOAIPAddressFamily ::= SEQUENCE {
   addressFamily OCTET STRING (SIZE (2..3)),
   addresses SEQUENCE OF IPAddress }

IPAddress ::= BIT STRING
```

2.1.3.2.1. version

TOC

The version number of the BogonOriginAttestation MUST be 0.

2.1.3.2.2. asIDs

TOC

The asIDs field contains the AS numbers that are to be regarded as Bogon AS's. The set of AS numbers may be explicitly listed, or specified as a continuous range of values. The field is to be formatted as per the canonical format specified in [RFC3779] (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” June 2004.).

2.1.3.2.3. BOAIPAddressFamily

TOC

The BOAIPAddressFamily field encodes the set of IP address prefixes that are to be regarded as Bogon IP addresses that are to be constrained from appearing in any routing advertisement. The intended semantics of an address prefix in a BOA is that any route object that has the same address prefix as that listed as a Bogon IP address, or is a more specific prefix of a Bogon IP address can be regarded as a Bogon route object.

The syntax of the address prefixes listed in a BOA uses a subset of the IP Address Delegation extension defined in [RFC3779] (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” June 2004.). The BOAIPAddressFamily cannot contain arbitrary address ranges, but in all other respects uses the same canonical format as the IP Address Delegation Extension.

Within the BOAIPAddressFamily structure, addressFamily contains the Address Family Identifier (AFI) of an IP address family. This specification only supports IPv4 and IPv6. Therefore, addressFamily MUST be either 0001 or 0002. The addresses field represents prefixes as a sequence of type IPAddress, as defined in[RFC3779] (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” June 2004.).

2.1.4. certificates

TOC

The certificates field MUST be included, and MUST contain only the end entity (EE) certificate needed to validate this BOA.

2.1.5. crls

TOC

The crls field MUST be omitted.

2.1.6. signerInfo

TOC

SignerInfo is defined under CMS as:

```
SignerInfo ::= SEQUENCE {
  version CMSVersion,
  sid SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature SignatureValue,
  unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }
```

2.1.6.1. version

TOC

The version number MUST be 3, corresponding with the choice of SubjectKeyIdentifier for the sid.

2.1.6.2. sid

TOC

The sid is defined as:

```
SignerIdentifier ::= CHOICE {
  issuerAndSerialNumber IssuerAndSerialNumber,
  subjectKeyIdentifier [0] SubjectKeyIdentifier }
```

For a BOA, the sid MUST be a SubjectKeyIdentifier.

2.1.6.3. digestAlgorithm

TOC

The digestAlgorithm MUST be SHA-256, the OID for which is 2.16.840.1.101.3.4.2.1. [RFC4055] (Schaad, J., Kaliski, B., and R.

Housley, “Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” June 2005.)

2.1.6.4. signedAttrs

TOC

Signed Attributes are defined as:

```
SignedAttributes ::= SET SIZE (1..MAX) OF Attribute

Attribute ::= SEQUENCE {
  attrType OBJECT IDENTIFIER,
  attrValues SET OF AttributeValue }

AttributeValue ::= ANY
```

The signedAttr element MUST be present and MUST include the content-type and message-digest attributes. The signer MAY also include the signing-time signed attribute, the binary-signing-time signed attribute, or both signed attributes. Other signed attributes that are deemed appropriate MAY also be included. The intent is to allow additional signed attributes to be included if a future need is identified. This does not cause an interoperability concern because unrecognized signed attributes are ignored by the relying party.
The signedAttr MUST include only a single instance of any particular attribute. Additionally, even though the syntax allows for a SET OF AttributeValue, in a BOA the attrValues must consist of only a single AttributeValue.

2.1.6.4.1. Content-Type Attribute

TOC

The ContentType attribute MUST be present. The attrType OID for the ContentType attribute is 1.2.840.113549.1.9.3.
The attrValues for the ContentType attribute in a ROA MUST be 1.2.840.113549.1.9.16.1.[TBD] (matching the eContentType in the EncapsulatedContentInfo).

2.1.6.4.2. Message-Digest Attribute

TOC

The MessageDigest Attribute MUST be present. The attrType OID for the MessageDigest Attribute is 1.2.840.113549.1.9.4.

The attrValues for the MessageDigest attribute contains the output of the digest algorithm applied to the content being signed, as specified in Section 11.1 of[RFC3852] (Housley, R., “Cryptographic Message Syntax (CMS),” July 2004.).

2.1.6.4.3. Signing-Time Attribute

TOC

The SigningTime Attribute MAY be present in a BOA. If it is present it MUST be ignored by the relying party. The presence of absence of the SigningTime attribute in no way affects the validation of the BOA (as specified in Section 3). The attrType OID for the SigningTime attribute is 1.2.840.113549.1.9.5.
The SigningTime attribute is defined as:

```
id-signingTime OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs9(9) 5 }

SigningTime ::= Time

Time ::= CHOICE {
  utcTime UTCTime,
  generalizedTime GeneralizedTime }
```

The Time element specifies the time, based on the local system clock, at which the digital signature was applied to the content.

2.1.6.4.4. BinarySigningTime Attribute

TOC

The BinarySigningTime Attribute MAY be present. If it is present it MUST be ignored by the relying party. The presence of absence of the BinarySigningTime attribute in no way affects the validation of the ROA (as specified in Section 3). The attrType OID for the BinarySigningTime attribute is 1.2.840.113549.1.9.16.2.46.
The BinarySigningTime attribute is defined as:

```
id-aa-binarySigningTime OBJECT IDENTIFIER ::= { iso(1)
    member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    smime(16) aa(2) 46 }

BinarySigningTime ::= BinaryTime

BinaryTime ::= INTEGER (0..MAX)
```

The BinaryTime element specifies the time, based on the local system clock, at which the digital signature was applied to the content.

2.1.6.5. signatureAlgorithm

TOC

The signatureAlgorithm MUST be RSA (rsaEncryption), the OID for which is 1.2.840.113549.1.1.1.

2.1.6.6. signature

TOC

The signature value is defined as:

```
SignatureValue ::= OCTET STRING
```

The signature characteristics are defined by the digest and signature algorithms.

2.1.6.7. unsignedAttrs

TOC

unsignedAttrs MUST be omitted.

---

3. BOA Validation

TOC

Before a relying party can use a BOA as a constrictor of a routing announcement, the relying party must use the RPKI to validate the BOA. To do this the relying party performs the following steps:

1. Verify that the BOA syntax complies with this specification. In particular, verify the following:

   a. The contentType of the CMS object is SignedData (OID 1.2.840.113549.1.7.2)

   b. The eContentType of the CMS object is id-ct-rpkiBOA (OID 1.2.840.113549.1.9.16.1.[TBD])

   c. The version of the SignedData object is 3.

d. The digestAlgorithm in the SignedData object is SHA-256 (OID 2.16.840.1.101.3.4.2.1).

e. The certificates field in the SignedData object is present and contains an EE certificate whose Subject Key Identifier (SKI) matches the sid field of the SignerInfo object.

f. The crls field in the SignedData object is omitted.

g. The eContentType in the EncapsulatedContentInfo is rid-ct-rpkiBOA (OID 1.2.840.113549.1.9.16.1.[TBD])

h. The version of the BOA is 0.

i. The addressFamily in the BOAIPAddressFamily is either IPv4 or IPv6 (0001 and 0002, respectively).

j. The version of the SignerInfo is 3.

k. The digestAlgorithm in the SignerInfo object is SHA-256 (OID 2.16.840.1.101.3.4.2.1).

l. The signatureAlgorithm in the SignerInfo object is RSA (OID 1.2.840.113549.1.1.1).

m. The signedAttrs field in the SignerInfo object is present and contains both the ContentType attribute (OID 1.2.840.113549.1.9.3) and the MessageDigest attribute (OID 1.2.840.113549.1.9.4). .

n. The unsignedAttrs field in the SignerInfo object is omitted.

2. Use the public key in the EE certificate to verify the signature on the BOA.

3. Verify that the EE certificate has an IP Address Delegation extension [RFC3779] (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” June 2004.) and that the IP address prefixes in that extension cover the IP address prefixes in the BOA, and the AS numbers in that extension cover the AS numbers in the BOA.

4. Verify that no valid ROA exists which also covers any more or less specific prefixes, or any AS numbers. In the case that a

ROA does exist which overlaps the BOA in any way, the BOA MUST be considered invalid.

5. Verify that the EE certificate is a valid end-entity certificate in the resource PKI by constructing a valid certificate path to a trust anchor. (See [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” February 2009.) for more details.)

---

4. BOA Use Practices

TOC

BOAs are intended to allow relying parties a means of validating whether route origination information as described in a route advertisement refers to an IP address or AS number that has not been validly allocated for use in the routing system.
Any party with a validly assigned Internet resource set and a CA certificate that describes this allocation can publish a BOA, independently of the actions of the actions of the party that assigned the resource set.
An Internet Registry SHOULD maintain a single BOA in relation to each parent registry that has assigned resources to this registry.
BOAs are not hierarchically related however they are subordinate to the CA certificate that describes the immediate allocations assigned.
An Internet Registry SHOULD maintain a regular issuance cycle for BOAs. For registries that operate on a day-to-day basis in terms of resource transactions, it is suggested that a local BOA management practice would be that a new BOA should be issued on a regular 24 hour basis. The corresponding EE certificate should have a validity period of no more than 72 hours from the time of issuance. Each time a new EE certificate for a BOA is issued the previous BOA's EE certificate should be revoked and the previous BOA removed from the publication repository.
Parties that operate a local cache of RPKI objects should ensure that they refresh BOA objects at intervals 24 hours to ensure that they have the current BOA in the local cache.

---

5. BOA Interpretation

TOC

A BOA can be used to check an inter-domain routing advertisement ("route") to determine if the origination information in the route object refers to invalid IP addresses or an invalid AS number.

If a route has an AS origination that refers to an AS number that is listed in a valid BOA, then the route can be regarded as a Bogon, and local policies that apply to Bogon AS's can be applied to the route. However if the AS number of this route is described in a valid ROA whose EE certificate lists the AS number, the BOA MUST be considered invalid

If a route has an address prefix that is equal to, or is a more specific prefix of an IP address that is included in a valid BOA then the route can be regarded as a Bogon, and local policies that apply to Bogon prefixes can be applied to the route. However if the address prefix of the route is described (either more or less specific) by a valid ROA, the BOA MUST be considered invalid.

BOA interpretation in the context of validation of origination of route objects is described in [I-D.ietf-sidr-roa-validation] (Huston, G. and G. Michaelson, “Validation of Route Origination in BGP using the Resource Certificate PKI,” October 2008.).

---

6. Security Considerations

TOC

There is no assumption of confidentiality for the data in a BOA; it is anticipated that BOAs will be stored in repositories that are accessible to all ISPs, and perhaps to all Internet users. There is no explicit authentication associated with a BOA, since the RPKI used for BOA validation provides authorization but not authentication. Although the BOA is a signed, application layer object, there is no intent to convey non-repudiation via a BOA.

The purpose of a BOA is to convey an attestation by an address holder that there is no authority for the generation of a route that refers to specified addresses or origination from specified AS's. The integrity of a BOA must be established in order to validate the authority of the Bogon Attestation. The BOA makes use of the CMS signed message format for integrity, and thus inherits the security considerations associated with that data structure. The right of the BOA signer to authorize the attestation of specified IP addresses and AS's as Bogons is established through use of the address space and AS number PKI described in [I-D.ietf-sidr-arch] (Lepinski, M. and S. Kent, “An Infrastructure to Support Secure Internet Routing,” March 2009.). Specifically, a relying party must verify the signature on the BOA using an X.509 certificate issued under this PKI, and check that the prefix(es) in the BOA match, or are covered by those in the address space extension in the certificate.

TOC

7. IANA Considerations

It would be anticipated that the IANA maintain a BOA for all unallocated space or reserved space (IPv4, IPv6 and ASNs) not intended for public use.

---

8. Acknowledgments

TOC

The authors are indebted to the authors of Route Origin Authorization (ROA) [I-D.ietf-sidr-roa-format] (Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)," November 2008.), M. Lepinski, S. Kent and D. Kong, as much of the text used to define a BOA has been borrowed from the ROA format specification, and Russ Housley for clarification on the CMS profile.
Further the authors wish to thank many security people, too many to name, for clarifying that negative attestations are a valid and useful security construct.
Lastly, without the orginal thoughts and words from George Michaelson and Geoff Huston this document would not exist. Their hands helped form the concepts of why we need BOAs in the RPKI and historically were two of the original three authors of this document.

---

9. Normative References

TOC

[I-D.ietf-sidr-arch]	Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing," draft-ietf-sidr-arch-06 (work in progress), March 2009 (TXT).
[I-D.ietf-sidr-res-certs]	Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," draft-ietf-sidr-res-certs-16 (work in progress), February 2009 (TXT).
[I-D.ietf-sidr-roa-format]	Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)," draft-ietf-sidr-roa-format-04 (work in progress), November 2008 (TXT).
[I-D.ietf-sidr-roa-validation]	Huston, G. and G. Michaelson, "Validation of Route Origination in BGP using the Resource Certificate PKI," draft-ietf-sidr-roa-validation-01 (work in progress), October 2008 (TXT).
[RFC3779]	Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers," RFC 3779, June 2004 (TXT).
[RFC3852]	Housley, R., "Cryptographic Message Syntax (CMS)," RFC 3852, July 2004 (TXT).

[RFC4055]	Schaad, J., Kaliski, B., and R. Housley, “Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” RFC 4055, June 2005 (TXT).
[RFC4271]	Rekhter, Y., Li, T., and S. Hares, “A Border Gateway Protocol 4 (BGP-4),” RFC 4271, January 2006 (TXT).
[RFC5280]	Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” RFC 5280, May 2008 (TXT).

Author's Address

TOC

	Terry Manderson
Email:	terry@terrym.net