Internet Engineering Task Force (IETF)
Request for Comments: 6482
Category: Standards Track
ISSN: 2070-1721

M. Lepinski
S. Kent
D. Kong
BBN Technologies

February 2012

Профиль полномочий на создание маршрутов (ROA)

A Profile for Route Origin Authorizations (ROAs)

Аннотация

Этот документ определяет стандартный профиль для ROA[1]. Объекты ROA имеют цифровую подпись и обеспечивают способ проверки того, что держатель адресного блока IP уполномочил автономную систему (AS[2]) создавать маршруты к одному или множеству префиксов из этого блока адресов.

Статус документа

Этот документ не является проектом стандарта (Internet Standards Track) и публикуется с информационными целями.

Документ является результатом работы IETF[3] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[4]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc6482.

Оглавление

1. Введение....1
1.1. Уровни требований....2
2. ROA Content-Type....2
3. ROA eContent....2
3.1. version....2
3.2. asID....2
3.3. ipAddrBlocks....2
4. Проверка пригодности ROA....3
5. Вопросы безопасности....3
6. Взаимодействие с IANA....3
7. Благодарности....3
8. Литература....3
8.1. Нормативные документы....3
8.2. Дополнительная литература....3
Приложение A. Модуль ASN.1....3

1. Введение

Основным назначением инфраструктуры открытых ключей ресурсов (RPKI[5]) является повышение уровня защиты маршрутизации (см. [RFC6480]). Для этой системы нужен механизм, который позволит элементам проверить наличие у данной AS полномочий анонсировать маршруты для одного или нескольких префиксов и блока адресов IP. Эта функция обеспечивается с помощью ROA.

ROA использует шаблон для объектов RPKI с цифровой подписью [RFC6488], который определяет синтаксис инкапсуляции CMS[6] [RFC5652] для содержимого ROA, а также базовую процедуру проверки пригодности для подписанных объектов RPKI. Поэтому для завершения спецификации ROA (см. раздел 4 в [RFC6488]) данный документ включает перечисленные ниже определения.

1. OID для идентификации подписанного объекта, каковым будет ROA (OID присутствует в поле eContentType объекта encapContentInfo, а также в качестве content-type подписанного атрибута в объекте signerInfo).

[1]Route Origin Authorization - полномочия создания маршрутов.
[2]Autonomous System.
[3]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[5]Resource Public Key Infrastructure.
[6]Crytopgraphic Message Syntax - синтаксис криптографических сообщений.

2. Синтаксис ASN.1 для ROA eContent (эта информация указывает AS, которое даются полномочия на создание маршрутов, а также префиксы, к которым AS может создавать маршруты). ASN.1 для ROA eContent использует правила отличительного кодирования (DER[1]) [X.690].

3. Для проверки пригодности ROA требуется дополнительный этап (в дополнение к этапам проверки, заданным в [RFC6488]).

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

2. ROA Content-Type

Тип содержимого (content-type) для ROA определяется как routeOriginAuthz и имеет значение 1.2.840.113549.1.9.16.1.24.

Этот идентификатор OID **должен** присутствовать в поле eContentType объекта encapContentInfo и в content-type подписанного атрибута объекта signerInfo (см. [RFC6488]).

3. ROA eContent

Содержимое ROA указывает AS, которой держатель блока адресов предоставил полномочия создавать маршруты, а также один или множество адресных префиксов IP, для которых будут анонсироваться маршруты. Если держателю блока адресов требуется предоставить такие полномочия множеству AS, ему нужно выпустить соответствующее число ROA (по одному на каждую AS). Формальное определение ROA приведено ниже.

```
RouteOriginAttestation ::= SEQUENCE {
   version [0] INTEGER DEFAULT 0,
   asID  ASID,
   ipAddrBlocks SEQUENCE (SIZE(1..MAX)) OF ROAIPAddressFamily }

ASID ::= INTEGER

ROAIPAddressFamily ::= SEQUENCE {
   addressFamily OCTET STRING (SIZE (2..3)),
   addresses SEQUENCE (SIZE (1..MAX)) OF ROAIPAddress }

ROAIPAddress ::= SEQUENCE {
   address IPAddress,
   maxLength INTEGER OPTIONAL }

IPAddress ::= BIT STRING
```

Отметим, что это содержимое появляется поле eContent объекта encapContentInfo (см. [RFC6488]).

3.1. version

Номер версии в поле version для RouteOriginAttestation **должен** иметь значение 0.

3.2. asID

Поле asID содержит номер AS, которой предоставлены полномочия создавать маршруты для данных префиксов IP.

3.3. ipAddrBlocks

Поле ipAddrBlocks представляет набор адресных префиксов IP, для которых AS уполномочена создавать маршруты. Отметим, что для этого поля используется более строгий синтаксис по сравнению с расширением передачи полномочий на адреса IP, определенным в RFC 3779. Указанное расширение позволяет представлять произвольные диапазоны адресов, а в ROA могут указываться только префиксы.

В структуре ROAIPAddressFamily поле addressFamily содержит идентификатор семейства адресов (AFI2) адресного семейства IP. Данная спецификация поддерживает адреса IPv4 и IPv6. Следовательно, поле addressFamily **должно** иметь значение 0001 или 0002.

В структуре ROAIPAddress поле addresses представляет префиксы в форме последовательности типа IPAddress (см. [RFC3779]). При наличии поля maxLength **оно** должно содержать целое число, значение которого не меньше размера сопровождающего префикса и не больше (в битах) размера адреса IP для данного семейства (32 для IPv4 и 128 для IPv6). При наличии поля maxLength оно задаёт максимальный размер адресного префикса IP, который разрешено анонсировать AS (например, если задан префикс IP 203.0.113/24 и maxLength = 26, AS уполномочена анонсировать любой более конкретный префикс, размер которого не превышает 26, т. е. AS может анонсировать префиксы 203.0.113/24, 203.0.113.128/25 или 203.0.113.0/25, но не 203.0.113.0/27). Если поле maxLength не задано, AS может анонсировать только точный префикс, заданный ROA.

Отметим, что действительное разрешение ROA может содержать адресный префикс IP (в элементе ROAIPAddress), охватываемый другим адресным префиксом IP (в отдельном элементе ROAIPAddress). Например, ROA может содержать префикс 203.0.113/24 с maxLength = 26, а также префикс 203.0.113.0/28 с maxLength = 28 (ROA будет разрешать указанной AS анонсировать любой префикс, начинающийся с 203.0.113 и имеющим минимальный размер 24, а максимальный - 26, а также префикс 203.0.113.0/28). Кроме того ROA **может** содержать два элемента ROAIPAddress с одинаковыми префиксами IP. Однако это **не рекомендуется**, поскольку в таком случае ROAIPAddress

[1]Distinguished Encoding Rules.

с меньшим maxLength не будет давать указанной AS дополнительных прав и может быть опущена без изменения смысла ROA.

4. Проверка пригодности ROA

До того, как зависимая от инфраструктуры сторона сможет применять ROA для проверки пригодности маршрутных анонсов, она **должна** будет проверить пригодность ROA. Для проверки пригодности ROA зависимая сторона **должна** выполнить все проверочные операции, указанные в [RFC6488], а также приведённый ниже дополнительный шаг проверки.

- Убедиться в наличии расширения IP Address Delegation [RFC3779] в сертификате конечного элемента (EE[1]), содержащемся в ROA, а также проверить вхождение всех адресных префиксов IP, содержащихся в ROA, в набор адресов IP, заданных расширением IP Address Delegation в сертификате EE.

5. Вопросы безопасности

Не принимается каких-либо допущений о конфиденциальности данных в ROA и предполагается, что ROAs будут храниться в репозиториях, доступных всем ISP и, возможно, всем пользователям Internet. С ROA не связано явной проверки подлинности, поскольку PKI, используемая для проверки пригодности ROA, обеспечивает проверку полномочий, но не подлинности. Хотя для ROA представляют собой подписанные объекты прикладного уровня, они не предназначены для передачи информации, от которой невозможно отказаться.

Целью ROA является передача полномочий AS на создание маршрутов к указанным в ROA префиксам. Поэтому **должна** обеспечиваться целостность ROA. Спецификация ROA использует формат подписанных объектов RPKI, поэтому все вопросы безопасности,, рассмотренные в [RFC6488], применимы и для ROA. Кроме того, профиль подписанного объекта использует формат подписанных сообщений CMS для обеспечения целостности, поэтому ROA наследуют все аспекты защиты, связанные с этой структурой данных.

Право подписавшей ROA стороны предоставлять AS полномочия создания маршрутов к адресным префиксам подтверждается с помощью инфраструктуры открытых ключей для адресов IP и номеров AS, описанной в [RFC6480]. В частности, подписи ROA **должны** проверяться с использованием сертификатов X.509, выпущенный в рамках этой PKI, а также должно проверяться соответствие адресных префиксов из ROA адресам, указанным в расширении сертификата.

6. Взаимодействие с IANA

Агентство IANA зарегистрировало показанный ниже подписанный объект (RPKI Signed Object).

```
ROA    1.2.840.113549.1.9.16.1.24    [RFC6482]
```

7. Благодарности

Авторы благодарят Charles Gardiner и Russ Housley за помощь и вклад в работу. В дополнение к этому авторы выражают благодарность Rob Austein, Roque Gagliano, Danny McPherson и Sam Weiler за внимательное рецензирование и полезные комментарии.

8. Литература

8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[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.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, February 2012.

[X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

8.2. Дополнительная литература

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

Приложение A. Модуль ASN.1

Это нормативное приложение содержит модуль ASN.1, задающий содержимое ROA в синтаксисе ASN.1.

```
RPKI-ROA { iso(1) member-body(2) us(840) rsadsi(113549)
   pkcs(1) pkcs9(9) smime(16) mod(0) 61 }

DEFINITIONS EXPLICIT TAGS ::= BEGIN

RouteOriginAttestation ::= SEQUENCE {
```

[1]End-entity.

```
      version [0] INTEGER DEFAULT 0,
      asID  ASID,
      ipAddrBlocks SEQUENCE (SIZE(1..MAX)) OF ROAIPAddressFamily }

   ASID ::= INTEGER

   ROAIPAddressFamily ::= SEQUENCE {
      addressFamily OCTET STRING (SIZE (2..3)),
      addresses SEQUENCE (SIZE (1..MAX)) OF ROAIPAddress }

   ROAIPAddress ::= SEQUENCE {
      address IPAddress,
      maxLength INTEGER OPTIONAL }

   IPAddress ::= BIT STRING

   END
```

Адреса авторов

Matt Lepinski

BBN Technologies

10 Moulton Street

Cambridge MA 02138

EMail: mlepinski@bbn.com

Stephen Kent

BBN Technologies

10 Moulton Street

Cambridge MA 02138

EMail: skent@bbn.com

Derrick Kong

BBN Technologies

10 Moulton Street

Cambridge MA 02138

EMail: dkong@bbn.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru