Network Working Group
Request for Comments: 3779
Category: Standards Track

C. Lynn
S. Kent
K. Seo
BBN Technologies

June 2004

Расширения X.509 для адресов IP и номеров AS

X.509 Extensions for IP Addresses and AS Identifiers

Статус документа

Этот документ задаёт проект стандартного протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития этого протокола. Текущий статус стандартизации протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Распространение документа не ограничивается.

Авторские права

Аннотация

Этот документ определяет два расширения для сертификатов X.509 v3. Первое расширение привязывает список адресных блоков IP или префиксов к субъекту сертификата. Второе привязывает к субъекту сертификата список идентификаторов автономных систем. Эти расширения могут служить для передачи полномочий субъекта на использование содержащихся в расширениях адресов IP и идентификаторов автономных систем.

Оглавление

1. Введение....2
1.1. Терминология....2
2. Расширение IP Address Delegation....3
2.1. Контекст....3
2.1.1. Представление адресов и префиксов IP....3
2.1.2. Представление диапазонов адресов IP....3
2.2. Спецификация....4
2.2.1. OID....4
2.2.2. Критичность....4
2.2.3. Синтаксис....4
2.2.3.1. Тип IPAddrBlocks....4
2.2.3.2. Тип IPAddressFamily....4
2.2.3.3. Элемент addressFamily....5
2.2.3.4. Элемент ipAddressChoice и тип IPAddressChoice....5
2.2.3.5. Элемент inherit....5
2.2.3.6. Элемент addressesOrRanges....5
2.2.3.7. Тип IPAddressOrRange....5
2.2.3.8. Элемент addressPrefix и тип IPAddress....5
2.2.3.9. Элемент addressRange и тип IPAddressRange....5
2.3. Проверка пути сертификации расширения IP Address Delegation....6
3. Расширение AS Identifier Delegation....6
3.1. Контекст....6
3.2. Спецификация....6
3.2.1. OID....6
3.2.2. Критичность....6
3.2.3. Синтаксис....6
3.2.3.1. Тип ASIdentifiers....7
3.2.3.2. Элементы asnum, rdi и тип ASIdentifierChoice....7
3.2.3.3. Элемент inherit....7
3.2.3.4. Элемент asIdsOrRanges....7
3.2.3.5. Тип ASIdOrRange....7
3.2.3.6. Элемент id....7
3.2.3.7. Элемент range....7
3.2.3.8. Тип ASRange....7
3.2.3.9. Элементы min и max....7
3.2.3.10. Тип ASId....7
3.3. Проверка пути сертификации расширения AS Identifier Delegation....7
4. Вопросы безопасности....7
5. Благодарности....8
Приложение A. Модуль ASN.1....8
Приложение B. Примеры расширения IP Address Delegation....8
Приложение C. Пример расширения AS Identifier Delegation....10
Приложение D. Использование сертификатов атрибутов X.509....10
Литература....11
Нормативные документы....11
Дополнительная литература....11

1. Введение

В этом документе описаны два расширения сертификатов X.509 v3, которые подтверждают передачу прав на использование адресов IP и номеров автономных систем от IANA через региональных регистраторов (RIR[1]) провайдерам Internet (ISP[2]) и организациям-пользователям. Первое расширение связывает список адресных блоков IP, зачастую представленных адресными префиксами IP, с субъектом (держателю секретного ключа) сертификата. Второе расширение связывает список идентификаторов автономных систем (AS[3]) с субъектом (держателю секретного ключа) сертификата. Эмитентом сертификата является организация (например, IANA, региональный регистратор Internet или ISP), которая имеет полномочия передавать право использования (выделять) наборов адресных блоков IP и номеров AS субъектам сертификатов. Эти сертификаты обеспечивают расширяемую систему проверки прав на использование (right-to-use) для наборов адресных префиксов IP и номеров AS. Это может применяться протоколами маршрутизации (например, Secure BGP [S-BGP]) для проверки правомочности и корректности маршрутной информации или реестрами маршрутизации Internet для проверки получаемых данных.

В разделах 2 и 3 указаны несколько правил кодирования расширений, которые определены в данной спецификации и **должны** выполняться. Эти правила служат нескольким целям. Во-первых, они обеспечивают уникальность представления значения расширения - два экземпляра расширения можно пооктетно сравнить. Во-вторых, обеспечивается минимальный размер представления данных. В-третьих, правила позволяют зависимым сторонам использовать однопроходные алгоритмы при проверке пути сертификации, что позволяет избавиться от сортировки или разработки дополнительного кода в подмножестве алгоритмов проверки для обработки некоторых граничных случаев (смежность, наложение или вхождение диапазонов).

1.1. Терминология

Предполагается знакомство читателя с терминами и концепциями, описанными в документах «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» [RFC3280], «INTERNET PROTOCOL" [RFC791], "Internet Protocol Version 6 (IPv6) Addressing Architecture» [RFC3513], «INTERNET REGISTRY IP ALLOCATION GUIDELINES» [RFC2050] и связанных с ними документах в части политики распределения адресов региональными регистраторами Internet. Ниже приведены определения некоторых терминов.

Allocate - выделение, распределение
Передача хранения (содержания) ресурса промежуточной организации (см. [RFC2050]).

Assign - назначение, присвоение
Передача хранения (содержания) ресурса конечному владельцу (см. [RFC2050]).

Autonomous System (AS) - автономная система
Множество маршрутизаторов с общим техническим администрированием и однородной политикой, использующих один или множество протоколов внутренней маршрутизации и метрик для определения путей маршрутизации пакетов внутри автономной системы, а также протокол внешней маршрутизации для определения путей маршрутизации пакетов в другие автономные системы.

Autonomous System number - номер автономной системы
32-битовое значение, идентифицирующее автономную систему.

Delegate - передача полномочий, делегирование
Передача хранения (т. е. права использования) блока адресов IP или идентификатора AS путём выпуска сертификата для объекта.

initial octet - начальный октет
Первый октет битовой строки (BIT STRING) в представлении DER [X.690].

IP v4 address - адрес IPv4
32-битовый идентификатор, записываемый в форме четырёх десятичных чисел из диапазона 0 - 255, разделённых точками. Примером адреса IPv4 может служить 10.5.0.5.

IP v6 address - адрес IPv6
128-битовый идентификатор, записываемый в форме восьми шестнадцатеричных чисел от 0 до ffff, разделённых двоеточиями (:). Примером адреса IPv6 может служить 2001:0:200:3:0:0:0:1. Последовательность :0: может быть заменена двумя символами двоеточия (::) и запись 2001:0:200:3::1 эквивалентна приведённому выше примеру адреса (см. [RFC3513]).

Prefix - префикс
Битовая строка, содержащая некоторое число начальных битов адреса и записанная в форме адреса, за которым следует символ дробной черты (/) и число начальных битов. Примерами префиксов могут служить 10.5.0.0/16 и 2001:0:200:3:0:0:0:0/64 (или 2001:0:200:3::/64). Префиксы часто сокращают, отбрасывая нули в младших полях так, чтобы число оставшихся битов было не меньше размера префикса. 10.5/16 и 2001:0:200:3/64 являются сокращёнными записями приведённых выше префиксов.

Regional Internet Registry (RIR) - региональный регистратор Internet
Любая организация, признанная IANA в качестве регионального уполномоченного по управлению адресами IP и номерами AS. На момент подготовки документа их было 5 - AfriNIC, APNIC, ARIN, LACNIC и RIPE NCC.

Right-to-use - право использования
Для адресного префикса IP это полномочия указывать AS, которая может создавать анонсы для этого префикса в Internet. Для номеров AS это полномочия сети представлять себя с этим идентификатором сетям из других AS.

subsequent octets - последующие октеты
Октеты со второго и до последнего в форме битовой строки (BIT STRING) с представлением DER [X.690].

trust anchor - доверенная привязка
Сертификат, которому доверяют при проверке пригодности пути сертификации (см. [RFC3280]).

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 [RFC2119].

[1]Regional Internet registry.
[2]Internet service provider.
[3]Autonomous system.

2. Расширение IP Address Delegation

Это расширение показывает выделение адресов IP объекту путём привязки адресов к открытому ключу объекта.

2.1. Контекст

Адресное пространство IP в настоящее время поддерживается иерархией с номинальным корнем в IANA, но реально обслуживается RIR. IANA выделяет блоки адресов RIR, а те, в свою очередь, распределяют их между провайдерами (ISP), которые могут выделять адреса IP нижестоящим провайдерам, заказчикам и т. п. RIR также могут выделять адреса организациям, являющимся конечными абонентами, т. е. не распределяют полученных адресов между другими организациями (см. [RFC2050] и соответствующие документы RIR с рекомендациями и описанием процесса выделения адресов.

Расширение IP Address Delegation предназначено для обеспечения возможности проверки корректности передачи полномочий на блоки адресов IP (т. е. полномочий на использование или последующее выделение адресных блоков IP). Соответственно, имеет смысл использовать преимущества имеющейся административной модели распределения адресного пространства IP. Как описано выше в разделе 1, это может быть реализовано путём выпуска сертификатов, сопровождающих описанное в разделе 1 выделение адресов. Примером использования информации из этого расширения может служить объект, применяющий эти данные для проверки полномочий организации в части создания сообщений BGP UPDATE, анонсирующих путь к конкретному блоку адресов IP (см., например, [RFC1771], [S-BGP]).

2.1.1. Представление адресов и префиксов IP

Имеется два семейства адресов IP - IPv4 и IPv6.

Адрес IPv4 представляет собой 32-битовое значение, которое записывается в форме 4 десятичных чисел от 0 до 255, разделённых точками. Примером адреса IPv4 может служить 10.5.0.5.

Адрес IPv6 представляет собой 128-битовое значение, которое записывается в форме 8 шестнадцатеричных значений от 0 до ffff, разделённых двоеточием (:). Примером адреса IPv6 может служить 2001:0:200:3:0:0:0:1. В адресах IPv6 часто встречаются смежные поля со значением 0. Группу таких полей можно обозначить последовательностью «::». Приведённый выше пример адреса можно представить в виде 2001:0:200:3::1.

Адресный префикс представляет собой блок из 2^k адресов, образующих непрерывную последовательность, в которой старшие биты адресов одинаковы. Например, 512 адресов IPv4 от 10.5.0.0 до 10.5.1.255 будут иметь одинаковые значений 23 старших битов. Блок адресов указывается путём добавления символа дробной черты (/) и числа неизменных старших битов. Префикс из приведённого выше примера имеет вид 10.5.0.0/23 и содержит $2^{(32-23)} = 2^9$ адресов. Блок адресов IPv6 от 2001:0:200:0:0:0:0:0 до 2001:0:3ff:ffff:ffff:ffff:ffff:ffff (2^{89} адресов) представляется в виде 2001:0:200:0:0:0:0:0/39 или 2001:0:200::/39. Префиксы можно сократить, опуская нули в младших полях, не входящих в число неизменных. Сокращённые формы приведённых выше префиксов имеют вид 10.5.0/23 и 2001:0:200/39.

Адрес или префикс IP кодируется в расширении IP Address Delegation как DER-представление ASN.1 BIT STRING, содержащие неизменные старшие биты. В соответствии с [X.690] DER-представление битовой строки состоит из типа BIT STRING (0x03), за которым следует представление числа октетов значения и само значение. Это значение состоит из «начального октета», который указывает число неиспользуемых битов с последнем октете, и «последующих октетов», содержащих саму строку (для адресов IP представление размера совпадает с размером).

Для одного адреса неизменны все биты и битовая строка для адреса IPv4 содержит 32 бита. Последующие октеты в DER-представлении адреса 10.5.0.4 будут иметь значения 0x0a 0x05 0x00 0x04. Поскольку в последнем октете используются все биты, начальный октет имеет значение 0x00. Октеты DER-представления BIT STRING показаны ниже

```
Тип  Разм. Неисп. битов ...
0x03 0x05  0x00  0x0a 0x05 0x00 0x04
```

DER-представление префикса 10.5.0/23 будет иметь вид

```
Тип  Разм. Неисп. битов ...
0x03 0x04  0x01  0x0a 0x05 0x00
```

В этом случае три последующих октета включают 24 бита, но префикс имеет размер 23, поэтому в последнем октете 1 бит не используется и начальный октет имеет значение 1 (в соответствии с DER все неиспользуемые биты **должны** иметь значение 0).

DER-представление адреса IPv6 2001:0:200:3:0:0:0:1 будет иметь вид

```
Тип  Разм. Неисп. битов ...
0x03 0x11  0x00  0x20 0x01 0x00 0x00 0x02 0x00 0x00 0x03
                 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x01
```

DER-представление префикса 2001:0:200/39 с одним неиспользуемым битом в последнем октете будет иметь вид

```
Тип  Разм. Неисп. битов ...
0x03 0x06  0x01  0x20 0x01 0x00 0x00 0x02
```

2.1.2. Представление диапазонов адресов IP

Хотя любой непрерывный диапазон адресов IP можно представить набором смежных префиксов, более компактным будет представление диапазона в форме SEQUENCE (последовательность) с указанием младшего и старшего адреса в форме BIT STRING. В SEQUENCE битовая строка с младшим адресом формируется путём удаления всех младших битов со значением 0, а строка со старшим адресом путём удаления всех младших битов со значением 1. в DER-представлении BIT STRING все неиспользуемые биты последнего октета **должны** иметь значение 0. Отметим, что префикс всегда можно выразить в форме диапазона, но диапазон не всегда выражается одним префиксом.

Диапазон адресов префикса 10.5.0/23 будет от 10.5.0.0 до 10.5.1.255. Младший адрес содержит 16 младших битов со значением 0 и DER-представление 16-битовой строки будет иметь вид

```
Тип  Разм. Неисп. битов ...
0x03 0x03  0x00  0x0a 0x05
```

Старший адрес завершается 9 единицами, которые удаляются. DER-представление оставшейся 23-битовой строки имеет вид

```
Тип  Разм. Неисп. битов ...
0x03 0x04  0x01  0x0a 0x05 0x00
```

Префикс 2001:0:200/39 можно представить диапазоном и DER-представлением младшего адреса (2001:0:200::) будет

```
Тип  Разм. Неисп. битов ...
0x03 0x06  0x01  0x20 0x01 0x00 0x00 0x02
```

Старший адрес 2001:0:3ff:ffff:ffff:ffff:ffff:ffff после удаления 90 младших битов со значением 1 будет включать 38 битов с представлением

```
Тип  Разм. Неисп. битов ...
0x03 0x06  0x02  0x20 0x01 0x00 0x00 0x00
```

Специальный случай «всех адресов IP» (префикс 0/0) **должен** кодироваться в DER с октетом размера 1, начальным октетом 0 и без последующих октетов

```
Тип  Разм. Неисп. битов ...
0x03 0x01  0x00
```

Отметим, что для адресов IP число нулей в конце имеет значение. Например DER-представлением 10.64/12 будет

```
Тип  Разм. Неисп. битов ...
0x03 0x03  0x04  0x0a 0x40
```

А DER-представлением 10.64.0/20 будет

```
Тип  Разм. Неисп. битов ...
0x03 0x04  0x04  0x0a 0x40 0x00
```

2.2. Спецификация

2.2.1. OID

Идентификатор OID для этого расширения имеет значение id-pe-ipAddrBlocks.

```
id-pe-ipAddrBlocks  OBJECT IDENTIFIER ::= { id-pe 7 }
```

В [RFC3280] дано определение

```
id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }
```

2.2.2. Критичность

Расширение **следует** обозначать критическим (CRITICAL). Предназначение этого расширения является обозначение права использования указанных в нем блоков адресов IP. CA помечает это расширение критическим для уведомления зависимых сторон о том, что они **должны** понимать семантику расширения для использования сертификата в целях, для которых он был выпущен. Предполагается, что новые приложения, использующие сертификаты с таким расширением, будут понимать его.

2.2.3. Синтаксис

```
id-pe-ipAddrBlocks      OBJECT IDENTIFIER ::= { id-pe 7 }

IPAddrBlocks        ::= SEQUENCE OF IPAddressFamily

IPAddressFamily     ::= SEQUENCE {    -- AFI и необязательный SAFI --
   addressFamily        OCTET STRING (SIZE (2..3)),
   ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOICE {
   inherit              NULL, -- наследуется от эмитента --
   addressesOrRanges    SEQUENCE OF IPAddressOrRange }

IPAddressOrRange    ::= CHOICE {
   addressPrefix        IPAddress,
   addressRange         IPAddressRange }

IPAddressRange      ::= SEQUENCE {
   min                  IPAddress,
   max                  IPAddress }

IPAddress           ::= BIT STRING
```

2.2.3.1. Тип IPAddrBlocks

Тип IPAddrBlocks представляет собой последовательность (SEQUENCE OF) типов IPAddressFamily.

2.2.3.2. Тип IPAddressFamily

Тип IPAddressFamily представляет собой последовательность (SEQUENCE), содержащую элементы addressFamily и ipAddressChoice.

2.2.3.3. Элемент addressFamily

Элемент addressFamily представляет собой строку октетов (OCTET STRING) содержащую 2-октетный идентификатор семейства адресов (AFI[1]) с сетевым порядком байтов, за которым может следовать октет идентификатора последующего семейства адресов (SAFI[2]). AFI и SAFI определены в [IANA-AFI] и [IANA-SAFI], соответственно.

Если не было предоставлено полномочий для конкретного AFI и дополнительного SAFI, **недопустимо** включать IPAddressFamily для этого AFI/SAFI в последовательность IPAddrBlocks.

Должна присутствовать только одна последовательность IPAddressFamily для уникальной комбинации AFI и SAFI. Каждая последовательность (SEQUENCE) **должна** быть упорядочена по возрастанию значений addressFamily (октеты считаются значениями без знака). addressFamily без SAFI **должны** предшествовать элементам, включающим SAFI. При указании обоих типов адресов IPv4 и IPv6 адреса IPv4 **должны** предшествовать адресам IPv6 (поскольку IPv4 AFI имеет значение 0001, которое меньше IPv6 AFI - 0002).

2.2.3.4. Элемент ipAddressChoice и тип IPAddressChoice

Элемент ipAddressChoice имеет тип IPAddressChoice, который представляет собой выбор (CHOICE) одного из элементов inherit или addressesOrRanges.

2.2.3.5. Элемент inherit

Если выбор IPAddressChoice содержит элемент inherit, набор адресов IP (на которые распространяются полномочия) для указанного AFI и дополнительного SAFI берётся из сертификата эмитента (или сертификата эмитента сертификата эмитента и т. д. рекурсивно, пока не будет найден сертификат, содержащий IPAddressChoice и с элементом addressesOrRanges).

2.2.3.6. Элемент addressesOrRanges

Элемент addressesOrRanges является последовательностью (SEQUENCE OF) типов IPAddressOrRange. Элементы addressPrefix и addressRange **должны** сортироваться с использованием двоичного представления

```
<lowest IP address in range> | <prefix length>
```

где | означает конкатенацию. Отметим, что октеты в этом представлении (a.b.c.d | размер для IPv4 или s:t:u:v:w:x:y:z | размер IPv6) не являются октетами DER-представления битовой строки (BIT STRING). Например, для двух addressPrefix

```
Адрес IP   | разм. DER-представление
-----------------  ------------------------
                   Тип  Разм. Неисп. битов ...
10.32.0.0 | 12     03   03    04   0a 20
10.64.0.0 | 16     03   03    00   0a 40
```

префикс 10.32.0.0/12 **должен** быть впереди префикса 10.64.0.0/16, поскольку 32 меньше 64, тогда как при сортировке по DER-представлениям битовых строк порядок был бы обратным, за счёт октета неиспользуемых битов. Любой паре вариантов IPAddressOrRange в расширении **недопустимо** перекрываться с другой парой. Любые непрерывные префикса или диапазоны **должны** объединяться в один диапазон или (если возможно) в один префикс.

2.2.3.7. Тип IPAddressOrRange

Тип IPAddressOrRange представляет собой выбор (CHOICE) одного из элементов addressPrefix (префикс или адрес IP) или addressRange (диапазон адресов IP).

В соответствии с данной спецификацией любой диапазон адресов, который может быть выражен префиксом, **должен** кодироваться с использованием элемента IPAddress (BIT STRING), а любой диапазон, который невозможно выразить префиксом, **должен** кодироваться с использованием IPAddressRange (SEQUENCE из двух BIT STRING). Приведённый ниже псевдокод иллюстрирует выбор способа кодирования диапазона адресов.

```
LET  N = число совпадающих старших битов в младшем и старшем адресе диапазона
IF   все оставшиеся биты младшего адреса имеют значения 0
 AND все оставшиеся биты старшего адреса имеют значения 1
THEN диапазон ДОЛЖЕН кодироваться как IPAddress размером N битов
ELSE диапазон ДОЛЖЕН кодироваться как IPAddressRange.
```

2.2.3.8. Элемент addressPrefix и тип IPAddress

Элемент addressPrefix имеет тип IPAddress. Этот тип определяет диапазон адресов IP, в котором N старших (слева) битов сохраняется неизменным, а оставшиеся биты (32 - N для IPv4, 128 - N для IPv6) могут принимать разные значения. Например, префикс IPv4 10.64/12 соответствует адресам с 10.64.0.0 до 10.79.255.255, а 10.64/11 - адресам с 10.64.0.0 до 10.95.255.255. Префикс IPv6 2001:0:2/48 представляет адреса 2001:0:2:: - 2001:0:2:ffff:ffff:ffff:ffff:ffff.

Адресный префикс IP представляется в форме строки битов (BIT STRING). DER-представление BIT STRING использует начальный октет строки для указания числа младших битов в младшем октете, которые не используются. В DER-представлении эти биты **должны** иметь значение 0.

Пример

```
          128.0.0.0       = 1000 0000.0000 0000.0000 0000.0000 0000
        - 143.255 255 255 = 1000 1111.1111 1111.1111 1111.1111 1111
      битовая строка для кодирования = 1000
            Тип  Разм. Неисп. битов ...
Кодирование = 0x03 0x02  0x04  0x80
```

2.2.3.9. Элемент addressRange и тип IPAddressRange

Элемент addressRange имеет тип IPAddressRange, который представляет собой последовательность (SEQUENCE), включающую младший (элемент min) и старший (элемент max) IP-адрес диапазона. Каждый из этих адресов

[1]Address Family Identifier.
[2]Subsequent Address Family Identifier

представляется строкой битов (BIT STRING). Все не указанные биты младшего адреса в IPAddressRange (до размера полного адреса) считаются установленными в 0, а для старшего - в 1. Битовая строка младшего адреса образуется путём удаления всех младших битов со значением 0 из младшего адреса, BIT STRING старшего адреса образуется удалением единиц из младших битов старшего адреса.

Пример

```
          129.64.0.0       = 1000 0001.0100 0000.0000 0000.0000 0000
        - 143.255.255.255  = 1000 1111.1111 1111.1111 1111.1111 1111
       мин. битов. строка  = 1000 0001.01
       макс. битов. строка = 1000
Кодирование = SEQUENCE {
            Тип  Разм. Неисп. битов ...
     min    0x03 0x03  0x06  0x81      0x40
     max    0x03 0x02  0x04  0x80
           }
```

Для упрощения операций сравнения адресных блоков IP при проверке пути сертификации старший адрес IP **должен** содержать хотя бы один бит со значением 1, т. е. последующие октеты не могут быть опущены или содержать только 0[1].

2.3. Проверка пути сертификации расширения IP Address Delegation

Для проверки пути сертификации сертификата с расширением IP Address Delegation требуются дополнительная обработка. При проверке каждого сертификата на этом пути адреса IP в расширении IP Address Delegation этого сертификата **должны** быть частью адресного блока IP в расширении IP Address Delegation сертификата эмитента. Если это условие не выполняется, проверка **должна** завершаться отказом. Сертификат, являющийся доверенной привязкой для проверки пути сертификации сертификатов с расширением IP Address Delegation, а также сертификатов на пути проверки **должен** включать расширение IP Address Delegation. Начальный набор разрешённых адресных диапазонов берётся из сертификата доверенной привязки.

3. Расширение AS Identifier Delegation

Это расширение показывает выделение номеров AS объекту путём привязки этих номеров к открытому ключу объекта.

3.1. Контекст

Расширение AS Identifier Delegation в настоящее время поддерживается иерархией с номинальным корнем в IANA, но реально обслуживается RIR. IANA выделяет номера AS регистраторам RIR, которые, в свою очередь, назначают номера AS организациям, являющимся конечными объектами (не распределяющими эти номера между другими организациями). Расширение AS Identifier Delegation предназначено для обеспечения возможности проверки полномочий для идентификаторов AS (т. е. прав объекта на использование данного номера AS). Соответственно, имеет смысл воспользоваться преимуществами имеющейся инфраструктуры поддержки идентификаторов AS. Как описано выше в разделе 1, это реализуется путём выпуска сертификатов, включающих описанное в этом разделе расширение. Примером использования информации из таких расширений может служить объект, применяющий расширение для проверки полномочий организации на управление AS, указанной идентификатором AS в расширении. Применение этого расширения для представления назначений идентификаторов AS не означает изменения процедур поддержки идентификаторов AS или условий, в которых следует использовать AS [RFC1930].

3.2. Спецификация

3.2.1. OID

Идентификатор OID для этого расширения имеет значение id-pe-autonomousSysIds.

```
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }
```

для которого [RFC3280] определяет

```
id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }
```

3.2.2. Критичность

Это расширение **следует** объявлять критичным (CRITICAL). Предполагаемое использование этого расширения состоит в обозначении права использования идентификаторов AS, указанных в нем. CA помечает это расширение как критическое (CRITICAL) для обозначения того, что зависимая сторона должна понимать семантику расширения для того, чтобы использовать сертификат по назначению. Предполагается, что новые приложения, которые используют сертификаты с таким расширением, будут его понимать.

3.2.3. Синтаксис

```
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }

ASIdentifiers       ::= SEQUENCE {
    asnum               [0] EXPLICIT ASIdentifierChoice OPTIONAL,
    rdi                 [1] EXPLICIT ASIdentifierChoice OPTIONAL}
ASIdentifierChoice  ::= CHOICE {
   inherit              NULL, -- наследуется от эмитента --
   asIdsOrRanges        SEQUENCE OF ASIdOrRange }

ASIdOrRange         ::= CHOICE {
    id                  ASId,
```

[1]Этот абзац предложено исключить из спецификации. См. https://www.rfc-editor.org/errata/eid2537. *Прим. перев.*

```
      range               ASRange }

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

   ASId                ::= INTEGER
```

3.2.3.1. Тип ASIdentifiers

Тип ASIdentifiers представляет собой последовательность (SEQUENCE), содержащую одну или множество форм идентификаторов автономных систем - номеров AS (в элементах asnum) или идентификаторов доменов маршрутизации (в элементах rdi). Если ASIdentifiers содержит множество форм идентификаторов, элемент asnum **должен** предшествовать элементу rdi. Номера AS используются BGP, а идентификаторы доменов маршрутизации заданы в IDRP [RFC1142][1].

3.2.3.2. Элементы asnum, rdi и тип ASIdentifierChoice

Элементы asnum и rdi имеют тип ASIdentifierChoice, который представляет собой выбор (CHOICE) из элементов inherit и asIdsOrRanges.

3.2.3.3. Элемент inherit

Если выбор ASIdentifierChoice содержит элемент inherit, множество полномочных идентификаторов AS берётся из сертификата эмитента или эмитента сертификата эмитента (рекурсивно, пока не будет найден сертификат с ASIdentifierChoice, содержащим элемент asIdsOrRanges). Если для конкретной формы идентификатора AS не было предоставлено полномочий, **недопустимо** присутствие соответствующего элемента asnum/rdi в последовательности ASIdentifiers.

3.2.3.4. Элемент asIdsOrRanges

Элемент asIdsOrRanges представляет собой последовательность (SEQUENCE) типов ASIdOrRange. **Недопустимо** перекрытие любой пары элементов в последовательности asIdsOrRanges. Все непрерывные последовательности идентификаторов AS **должны** по возможности объединяться в один диапазон. Идентификаторы AS в элементе asIdsOrRanges **должны** сортироваться в порядке роста числовых значений.

3.2.3.5. Тип ASIdOrRange

Тип ASIdOrRange представляет собой выбор (CHOICE) из одиночного целого числа (ASId) или одиночной последовательности (ASRange).

3.2.3.6. Элемент id

Элемент id имеет тип ASId.

3.2.3.7. Элемент range

Элемент range имеет тип ASRange.

3.2.3.8. Тип ASRange

Тип ASRange представляет собой последовательность (SEQUENCE), содержащую элементы min и max, которые служат для указания диапазона значений идентификаторов AS.

3.2.3.9. Элементы min и max

Элементы min и max относятся к типу ASId. Элемент min служит для задания минимального идентификатора AS в диапазоне, а элемент max - для задания максимального идентификатора AS.

3.2.3.10. Тип ASId

ASId имеет тип INTEGER (целое число).

3.3. Проверка пути сертификации расширения AS Identifier Delegation

Проверка пути сертификации сертификата, содержащего расширение AS Identifier Delegation требует дополнительных операций. Поскольку проверяется каждый сертификат на этом пути, идентификаторы AS в расширении AS Identifier Delegation сертификата **должны** быть частью идентификаторов AS в расширении AS Identifier Delegation сертификата эмитента. При нарушении этого правила проверка **должна** завершаться отказом. Сертификат, являющийся доверенной привязкой для проверки пути сертификации сертификатов, содержащих расширение AS Identifier Delegation, а также все сертификаты на пути проверки **должны** содержать расширение AS Identifier Delegation. Начальный набор разрешённых идентификаторов AS берётся из сертификата доверенной привязки.

4. Вопросы безопасности

Данная спецификация описывает два расширения X.509. Поскольку сертификаты X.509 имеют цифровые подписи, дополнительной защиты целостности не требуется. Сертификаты с этими расширениями не требуется хранить в секрете, поскольку неограниченный и анонимный доступ к ним не создаёт угроз безопасности.

Однако вопросы безопасности, выходящие за рамки данной спецификации, будут влиять на гарантии, предоставляемые пользователям сертификатов. В этом параграфе отмечены важные аспекты, на которые следует обращать внимание разработчикам, администраторам и пользователям.

Эти расширения предоставляют информацию о полномочиях, т. е. праве использовать адреса IP или идентификаторы AS. Расширения разработаны для поддержки защищённой версии протокола BGP [S-BGP], но могут применяться и в

[1] RFC 1142 не содержит спецификации IDRP, она задана в ISO 10747. См. https://www.rfc-editor.org/errata/eid836. *Прим. перев.*

другом контексте. В среде защищённого BGP сертификаты с такими расширениями служат возможностями (capability) - сертификат подтверждает, что владелец секретного ключа (Subject) уполномочен использовать адреса IP или идентификаторы AS, представленные в расширениях. По этой причине поле Subject значительно меньше относится к защите, нежели в обычных инфраструктурах PKI.

5. Благодарности

Авторы признательны Charles Gardiner, Russ Housley, James Manger и Jim Schaad за их вклад в подготовку документа.

Приложение A. Модуль ASN.1

Это нормативное приложение описывает расширения, используемые соответствующими спецификации компонентами PKI в синтаксисе ASN.1.

```
IPAddrAndASCertExtn { iso(1) identified-organization(3) dod(6)
         internet(1) security(5) mechanisms(5) pkix(7) mod(0)
         id-mod-ip-addr-and-as-ident(30) }
    DEFINITIONS EXPLICIT TAGS ::=
BEGIN
     -- Copyright (C) The Internet Society (2004). Эта        --
     -- версия данного модуля ASN.1 является частью RFC 3779. --
     -- Авторские права полностью указаны в этом документе.   --
-- EXPORTS ALL --

IMPORTS
-- специфические для PKIX значения OID и arc --
    id-pe FROM PKIX1Explicit88 { iso(1) identified-organization(3)
               dod(6) internet(1) security(5) mechanisms(5) pkix(7)
               id-mod(0) id-pkix1-explicit(18) };

-- OID расширения IP Address Delegation --
id-pe-ipAddrBlocks  OBJECT IDENTIFIER ::= { id-pe 7 }

-- Синтаксис расширения IP Address Delegation --
IPAddrBlocks        ::= SEQUENCE OF IPAddressFamily

IPAddressFamily     ::= SEQUENCE { -- AFI и необязательный SAFI --
   addressFamily        OCTET STRING (SIZE (2..3)),
   ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOICE {
   inherit              NULL, -- наследуется от эмитента --
   addressesOrRanges    SEQUENCE OF IPAddressOrRange }

IPAddressOrRange    ::= CHOICE {
   addressPrefix        IPAddress,
   addressRange         IPAddressRange }

IPAddressRange      ::= SEQUENCE {
   min                  IPAddress,
   max                  IPAddress }

IPAddress           ::= BIT STRING

-- OID расширения ASystem Identifier Delegation --
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }

-- Синтаксис расширения ASystem Identifier Delegation --
ASIdentifiers       ::= SEQUENCE {
    asnum               [0] ASIdentifierChoice OPTIONAL,
    rdi                 [1] ASIdentifierChoice OPTIONAL }

ASIdentifierChoice  ::= CHOICE {
   inherit              NULL, -- наследуется от эмитента --
   asIdsOrRanges        SEQUENCE OF ASIdOrRange }

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

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

ASId                ::= INTEGER
END
```

Приложение B. Примеры расширения IP Address Delegation

Критическое расширение сертификата X.509 v3, которое задаёт перечисленные ниже адреса.

```
Префиксы индивидуальных адресов IPv4
    1) 10.0.32/20     т. е.  10.0.32.0 - 10.0.47.255
    2) 10.0.64/24     т. е.  10.0.64.0 - 10.0.64.255
    3) 10.1/16        т. е.  10.1.0.0  - 10.1.255.255
    4) 10.2.48/20     т. е.  10.2.48.0 - 10.2.63.255
```

```
      5) 10.2.64/24     т. е.  10.2.64.0 - 10.2.64.255
      6) 10.3/16        т. е.  10.3.0.0  - 10.3.255.255, and
      7) наследуются все адреса IPv6 от эмитента сертификата
```

Будет иметь шестнадцатеричное представление

```
30 46                       Extension {
   06 08 2b06010505070107     extnID        1.3.6.1.5.5.7.1.7
   01 01 ff                   critical
   04 37                      extnValue {
      30 35                     IPAddrBlocks {
         30 2b                    IPAddressFamily {
            04 03 0001  01          addressFamily: IPv4 Unicast
                                    IPAddressChoice
            30 24                     addressesOrRanges {
                                        IPAddressOrRange
               03 04 04 0a0020            addressPrefix 10.0.32/20
                                        IPAddressOrRange
               03 04 00 0a0040            addressPrefix 10.0.64/24
                                        IPAddressOrRange
               03 03 00 0a01              addressPrefix    10.1/16
                                        IPAddressOrRange
               30 0c                      addressRange {
                  03 04 04 0a0230           min        10.2.48.0
                  03 04 00 0a0240           max        10.2.64.255
                                            } -- addressRange
                                        IPAddressOrRange
               03 03 00 0a03              addressPrefix    10.3/16
                                      } -- addressesOrRanges
                                    } -- IPAddressFamily
         30 06                      IPAddressFamily {
            04 02 0002                addressFamily: IPv6
                                      IPAddressChoice
            05 00                       наследуется от эмитента
                                    } -- IPAddressFamily
                                  } -- IPAddrBlocks
                                } -- extnValue
                              } -- расширение
```

Этот пример показывает сортировку префиксов и диапазонов.

- Префикс 1 **должен** предшествовать префиксу 2, хотя число неиспользуемых битов (4) в префиксе 1 больше числа неиспользуемых битов (0) в префиксе 2.
- Префикс 2 **должен** предшествовать префиксу 3, хотя число октетов (4) в представлении BIT STRING для префикса 2 больше числа октетов (3) в BIT STRING префикса 3.
- Префиксы 4 и 5 являются смежными (представляют диапазон адресов 10.2.48.0 - 10.2.64.255), поэтому они **должны** объединяться в диапазон (поскольку одним префиксом выразить из невозможно).
- Отметим, что 6 нулей в конце элемента max значимы для интерпретации значения (поскольку все неиспользуемые биты интерпретируются 1, а не 0). Четыре нуля в конце элемента min не являются значимыми и **должны** быть удалены (это даёт 4 неиспользуемых бита в представлении элемента min). DER-представление **требует** устанавливать значение 0 для всех неиспользуемых битов в последнем из последующих октетов.
- Диапазон, формируемый префиксами 4 и 5, **должен** предшествовать префиксу 6, хотя тег SEQUENCE для представления диапазона (30) больше тега BIT STRING (03) для представления префикса 6.
- Данные IPv4 **должны** предшествовать информации IPv6, поскольку идентификатор семейства адресов для IPv4 (0001) меньше идентификатора для IPv6 (0002).

Ниже показано расширение, задающее префикс IPv6 2001:0:2/48 и префиксы IPv4 10/8 и 172.16/12, а также наследование всех групповых адресов IPv4 из сертификата эмитента (в шестнадцатеричной форме).

```
30 3d                       Extension {
   06 08 2b06010505070107     extnID        1.3.6.1.5.5.7.1.7
   01 01 ff                   critical
   04 2e                      extnValue {
      30 2c                     IPAddrBlocks {
         30 10                    IPAddressFamily {
            04 03 0001 01           addressFamily: IPv4 Unicast
                                    IPAddressChoice
            30 09                     addressesOrRanges {
                                        IPAddressOrRange
               03 02 00 0a                addressPrefix    10/8
                                        IPAddressOrRange
               03 03 04 b010              addressPrefix    172.16/12
                                      } -- addressesOrRanges
                                    } -- IPAddressFamily
         30 07                      IPAddressFamily {
            04 03 0001 02           addressFamily: IPv4 Multicast
                                    IPAddressChoice
            05 00                     наследуется от эмитента
                                    } -- IPAddressFamily
         30 0f                      IPAddressFamily {
            04 02 0002              addressFamily: IPv6
                                    IPAddressChoice
```

```
            30 09                    addressesOrRanges {
                                       IPAddressOrRange
               03 07 00 200100000002     addressPrefix   2001:0:2/47
                                     } -- addressesOrRanges
                                   } -- IPAddressFamily
                                 } -- IPAddrBlocks
                               } -- extnValue
                                } -- расширение
```

Приложение C. Пример расширения AS Identifier Delegation

Ниже приведено расширение, задающее номера AS 135, 3000 - 3999 и 5001, а также наследующее все идентификаторы rdi из сертификата эмитента (в шестнадцатеричной форме).

```
30 2b                       Extension {
   06 08 2b06010505070108     extnID        1.3.6.1.5.5.7.1.8
   01 01 ff                   critical
   04 1c                      extnValue {
      30 1a                     ASIdentifiers {
         a0 14                    asnum
                                    ASIdentifierChoice
            30 12                     asIdsOrRanges {
                                        ASIdOrRange
               02 02 0087               ASId
                                        ASIdOrRange
               30 08                    ASRange {
                  02 02 0bb8              min
                  02 02 0f9f              max
                                        } -- ASRange
                                        ASIdOrRange
               02 02 1389               ASId
                                     } -- asIdsOrRanges
                                   } -- asnum
         a1 02                     rdi {
                                     ASIdentifierChoice
            05 00                      наследуется от эмитента
                                   } -- rdi
                                 } -- ASIdentifiers
                               } -- extnValue
                             } -- расширение
```

Приложение D. Использование сертификатов атрибутов X.509

В этом приложении рассматриваются вопросы, связанные с предложением использовать сертификаты атрибутов (AC, как описано в [RFC3281]) для доставки от региональных регистраторов (RIR[1]) до организаций, являющихся конечными пользователями, «прав на использование» адресных блоков IP и идентификаторов AS.

Ресурсы идентификаторов AS и адресных блоков IP в настоящее время поддерживаются раздельно. Все организации, имеющие право использовать идентификаторы AS, получают эти полномочия напрямую от RIR. Организации, имеющие право использовать блоки адресов IP, получают свои полномочия напрямую от RIR или опосредованно через сервис-провайдеров, которые могут получить свои полномочия от ISP, а те, в свою очередь, от RIR. Отметим, что в будущем для идентификаторов AS также может возникнуть многоуровневое распределение, поэтому механизм не следует строить на базе лишь трёх уровней.

В разделе 1 RFC 3281 приведены две причины, по которым использование AC может быть предпочтительней применения сертификатов открытых ключей (PKC[2]) в расширениях, передающих информацию о полномочиях.

> «Информация о полномочиях может быть помещена в расширение PKC или отдельный сертификат атрибута (AC). Размещение информации о полномочиях в PKC обычно нежелательно по двум причинам. Во-первых, срок действия такой информации обычно отличается от срока действия привязки объекта к открытому ключу. Размещение информации о полномочиях в расширении PKC обычно сокращает полезный срок действия PKC. Во-вторых, эмитенты PKC обычно не обладают информацией о предоставлении полномочий. Это приводит к необходимости дополнительных действий эмитентов PKC по получению такой информации из уполномоченного источника.»

> «По этим причинам зачастую лучше отделить информацию о полномочиях от PKC. Эта информация все равно должна быть привязана к объекту и AC обеспечивает такую привязку - это просто цифровая подпись (или сертификат) для объекта и набор атрибутов.»

В случае адресов IP и идентификаторов AS приведённые выше соображения не применимы. Во-первых, сертификаты открытых ключей выпускаются исключительно в целях предоставления полномочий, поэтому срок их действия в точности совпадает со сроком действия полномочий, который часто привязан к контрактным отношениям между эмитентом и организацией, получившей полномочия. Имена субъекта (Subject) и эмитента (Issuer) нужны лишь для создания цепочек при проверке путей сертификации, поэтому не требуется какого-либо соответствия имён физическим объектам. Значение Subject в PKC может быть произвольно выбранным выпускающим сертификат CA, что позволяет частично скрыть владельца ресурса. Во-вторых, иерархия сертификатов организована так, что эмитент сертификата обладает информацией о полномочиях.

Таким образом, два пункта из первой цитаты не являются корректными для случая распределения номеров AS и адресных блоков IP. Указанное во второй цитате также не применимо, поскольку ресурсы привязываются не к объекту, а к владельцу секретного ключа, соответствующего открытому ключу в PKC.

В RFC 3281 указано несколько требований, которым должны соответствовать сертификаты атрибутов (AC). Применительно к S-BGP наиболее важные требования перечислены ниже.

[1]Regional Internet Registry.
[2]Public key certificate.

1 Раздел 1: «данная спецификация **не рекомендует** использовать цепочки AC. Другие (будущие) спецификации могут включать вопросы использования цепочек AC.»

Распределение ресурсов от IANA через RIR, ISP, DSP и присвоение конечным пользователям (организациям) требует использования цепочек по крайней мере для адресных блоков IP. Требуется описание расположения вышестоящего AC и способа обработки. Читатели могут подумать сами о способах избавления от цепочек.

2 Параграф 4.2.9: «в параграфе 4.3 определены расширения, которые **могут** использоваться с этим профилем, и критерии указания уровня критичности таких расширений. При использовании любых других критических расширений AC не будет соответствовать профилю. Однако использование других некритических расширений не нарушает соответствия AC данному профилю.»

Это означает, что расширения передачи полномочий, определённые в данной спецификации (они являются критическими) просто не могут быть включены в AC. Они могут использоваться в некритическом варианте, но предполагаемое использование требует, чтобы эти расширения были критическими для предотвращения использования сертификатов в качестве отождествлений не понимающими этих расширений приложениями.

3 Параграф 4.5: "эмитенту AC **недопустимо** быть также эмитентом PKC. Т. е. эмитент AC не может быть CA.»

Это означает, что каждому эмитенту AC потребуется отдельный CA для выпуска PKC с открытым ключом держателя AC. Эмитент AC не может выпустить PKC для держателя, а эмитент PKC не может подписывать AC. Таким образом, каждому объекту в PKI потребуется поддерживать эмитента AC в дополнение к CA. Это будет удваивать число эмитентов при использовании сертификатов атрибутов по сравнению с числом эмитентов сертификатов и CRL при использовании PKC. При выдаче сертификатов разными органами возрастает также вероятность несогласованности.

Модель AC из RFC 3281 предполагает, что держатель AC представляет AC проверяющей стороне, когда та желает получить обоснование атрибута или полномочий. Предполагаемое использование определённых здесь расширений не включает прямого взаимодействия между проверяющей AC стороной (NOC[1]) и эмитентами AC (все RIR и NOC). На основе подписи в заявляющем право использования объекте «проверяющая AC сторона» может получить PKC держателя AC, но нет прямого пути для определения субъектов AC.

4 Параграф 5: «4. Эмитент AC **должен** быть непосредственно доверенным издателем AC (по конфигурации или иным способом).»

Это не справедливо для случая прав на использование адресных блоков IP, которые выделяются через иерархию. Проверка пути сертификации AC будет требовать организации цепочек через иерархию передачи полномочий (делегирования). Организация для каждой зависимой от инфраструктуры стороны (NOC) «доверия» к каждому другому NOC не обеспечивает масштабируемости и такое «доверие» приведёт в результате к отказам, которые предлагаемые механизмы должны были предотвращать. В предлагаемой здесь модели используется одна PKI с доверенным корнем, а не тысячи отдельных доверительных отношений между ISP, выпускающими AC.

Объем работы, требуемой для проверки пригодности AC больше , нежели для расширений сертификатов, определённых в этом документе в рамках PKC. Число проверяемых сертификатов для случая AC будет вдвое больше. Это может существенно увеличить издержки, связанные с использованием AC.

Литература

Нормативные документы

[IANA-AFI] http://www.iana.org/assignments/address-family-numbers.

[IANA-SAFI] http://www.iana.org/assignments/safi-namespace.

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

[RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[X.690] ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, "Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

Дополнительная литература

[RFC791] Postel, J., "Internet Protocol -- DARPA Internet Program Protocol Specification", RFC 791, September 1981.

[RFC1142] D. Oran, Ed., "OSI IS-IS Intra-domain Routing Protocol", RFC 1142, February 1990.

[RFC1771] Rekhter, Y. and T. Li, Eds., "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC2050] Hubbard, K., Kosters, M., Conrad, D., Karrenberg, D. And J. Postel, "Internet Registry IP Allocation Guidelines", BCP 12, RFC 2050, November 1996.

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[RFC3281] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[RFC4291] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.[2]

[1] Network operations center. *Прим. перев.*

[2] В оригинале эта ссылка отсутствует (документа ещё не было). См. https://www.rfc-editor.org/errata/eid1887. *Прим. перев.*

[S-BGP] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," IEEE JSAC Special Issue on Network Security, April 2000.

Адреса авторов

Charles Lynn
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA
Phone: +1 (617) 873-3367
EMail: CLynn@BBN.Com

Stephen Kent
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA
Phone: +1 (617) 873-3988
EMail: Kent@BBN.Com

Karen Seo
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA
Phone: +1 (617) 873-3152
EMail: KSeo@BBN.Com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.