Internet Engineering Task Force (IETF)
Request for Comments: 6480
Category: Informational
ISSN: 2070-1721

M. Lepinski
S. Kent
BBN Technologies

February 2012

Инфраструктура для поддержки защищенной маршрутизации в Internet

An Infrastructure to Support Secure Internet Routing

Тезисы

Этот документ описывает архитектуру системы для поддержки улучшенной защиты маршрутизации в сети Internet. Основой этой архитектуры является инфраструктура открытых ключей ресурсов (RPKI[1]), которая представляет иерархию выделения адресов IP и номеров автономных систем (AS[2]), а также распределенную систему репозиториев для хранения и распространения объектов данных, составляющих RPKI, а также других подписанных объектов, требуемых для повышения безопасности маршрутизации. В качестве первого применения этой архитектуры данный документ описывает, как законный владелец адресного пространства IP может явно и проверяемо уполномочить одну или множество AS порождать маршруты в его адресное пространство. Такие проверяемые полномочия могут использоваться, например, для более защищенных маршрутных фильтров BGP.

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/rfc6480.

Оглавление

1. Введение....2
1.1. Терминология....2
2. Инфраструктура открытых ключей для INR....2
2.1. Роль в архитектуре....3
2.2. Сертификаты CA....3
2.3. Сертификаты конечных элементов (EE)....4
2.4. Доверенные привязки....4
3. Полномочия на создание маршрутов....4
3.1. Роль в архитектуре....4
3.2. Синтаксис и семантика....5
4. Репозитории....5
4.1. Роль в архитектуре....6
4.2. Содержимое и структура....6
4.3. Протоколы доступа....7
4.4. Управление доступом....7
5. Манифесты....7
5.1. Синтаксис и семантика....7
6. Поддержка локального кэша....7
7. Основные операции....8
7.1. Издание сертификатов....8
7.2. Смена ключа CA....8
7.3. Управление ROA....8
7.3.1. Абоненты с одним подключением....9
7.3.2. Абоненты с множеством подключений....9
7.3.3. Провайдеро-независимые адреса....9

[1]Resource Public Key Infrastructure.
[2]Autonomous System.
[3]Internet Engineering Task Force.
[4]Internet Engineering Steering Group.

8. Вопросы безопасности....9
9. Взаимодействие с IANA....9
10. Благодарности....9
11. Литература....10
11.1. Нормативные документы....10
11.2. Дополнительная литература....10

1. Введение

Этот документ описывает архитектуру системы для поддержки улучшенной защиты маршрутизации BGP [RFC4271] в сети Internet. Архитектура включает три основных элемента:

- инфраструктура открытых ключей ресурсов (RPKI[1]);
- подписанные объекты маршрутизации для поддержки защиты маршрутизации;
- распределенная система репозиториев для хранения объектов PKI и подписанных объектов маршрутизации.

Описанная в этом документе архитектура позволяет объекту достоверно заявлять свое законное владение множеством адресов IP или номеров AS. В качестве начального применения этой архитектуры документ описывает как законный владелец адресного пространства IP может явно и достоверно предоставить одной или множеству AS полномочия на создание (originate) маршрутов в это адресное пространство. Такая проверяемая передача полномочий может применяться, например, для создания более защищенных фильтров маршрутов BGP. В дополнение к такому применению определенная этой архитектурой инфраструктура также предназначена для обеспечения в будущем поддержки защищенных протоколов типа Secure BGP [S-BGP] или Secure Origin BGP [soBGP]. Эта архитектура применима для маршрутизации дейтаграмм как IPv4, так и IPv6. В настоящее время архитектура поддерживает только адреса семейств IPv4 и IPv6. Таким образом, например, использование этой архитектуры с метками MPLS выходит за рамки этого документа.

Для облегчения развертывания архитектура использует преимущества существующих технологий и опыта. Структура элемента PKI в архитектуре соответствует структуре существующего распределения ресурсов. Управление этой PKI является естественным расширением функций управления ресурсами в организациях, которые уже отвечают за распределение адресов IP и номеров AS. Имеющийся опыт выделения и отзыва ресурсов также нашел свое отражение в этой архитектуре. Отметим, что несмотря на то, что изначально архитектура нацелена на обеспечение защиты маршрутизации, описанная в этом документе PKI может также применяться для решения других задач, связанных с аттестацией владения адресами IP или номерами AS.

Для упрощения реализации везде, где было возможно, использованы существующие стандарты IETF — например, широко используется профиль сертификатов X.509, определенный для инфраструктуры открытых ключей с использованием X.509 (PKIX[2]) [RFC5280] и расширения для представления адресов IP и номеров AS, определенные в RFC 3779 [RFC3779]. Используется также синтаксис криптографических сообщений (CMS[3]) [RFC5652] для вновь определенных подписанных объектов [RFC6488], требуемых этой инфраструктурой.

Как отмечено выше, архитектура включает три основных компоненты - X.509 PKI, в которой сертификатами аттестуются владение адресами IP и номерами AS; подписанные объекты, которые не являются сертификатами (включая манифесты и полномочия по созданию маршрутов) и используются инфраструктурой; распределенная система репозиториев, которая делает все эти подписанные объекты доступными для использования ISP в процессах принятия решений о маршрутизации. Эти три базовых компоненты обеспечивают некоторые функции защиты, наиболее заметной из которых является криптографическая проверка полномочий автономной системы на порождение маршрутов для данного префикса [RFC6483].

1.1. Терминология

Предполагается, что читатель знаком с терминами и концепциями, описанными в документах «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» [RFC5280] и «X.509 Extensions for IP Addresses and AS Identifiers» [RFC3779].

В этом документе слова «держатель адресного пространства» (address space holder) и «держатель адресного пространства IP» (holder of IP address space) указывают законного владельца адресного блока IP, который получил эти адреса через стандартную иерархию распределения IP-адресов. Т. е. владелец (держатель) адресного пространства получил этот блок адресов непосредственно от IANA или регионального регистратора (RIR[4]) или путем вторичного распределения от национального (NIR[5]) или местного (LIR[6]) регистратора. Слова «держатель (владелец) ресурса» обозначают законного владельца ресурса адресов IP или номеров AS.

В этом документе термины «регистратор» (registry) и ISP указывают организацию, которая имеет ресурсы адресов IP и/или номеров AS для последующего распределения (sub-allocate).

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. Инфраструктура открытых ключей для INR

Поскольку держатель блока адресов IP имеет право определять топологическое назначение (цель) дейтаграмм IP, адресованных в этот блок, решения о междоменной маршрутизации традиционно основываются на информации о

[1]Resource Public Key Infrastructure.
[2]Public Key Infrastructure using X.509.
[3]Cryptographic Message Syntax.
[4]Regional Internet Registry.
[5]National Internet Registry.
[6]Local Internet Registry.

распределении адресного пространства IP. Таким образом, базовая функция этой архитектуры заключается в обеспечении криптографически проверяемой аттестации выделения адресов. В современной практике распределение адресов IP происходит по иерархической модели. Вершиной иерархии является агентство IANA. Ниже IANA размещается 5 региональных регистраторов (RIR), каждый из которых управляет распределением адресов и номеров AS в своем географическом регионе. В некоторых регионах имеется третий уровень иерархии, включающий национальных (NIR) и местных (LIR[1]) регистраторов, а также абонентов с так называемыми «провайдеро-независимыми» (переносимыми) блоками адресов. В остальных регионах третий уровень состоит только из LIR/ISP и абонентов с переносимыми блоками.

В общем случае владелец блока адресов IP может выделять части этого блока для себя (т. е. отдельного подразделения в рамках одной организации) или другой организации в зависимости от контрактных ограничений, задаваемых регистраторами. В результате этого распределение адресного пространства IP можно естественным образом описать с помощью иерархической инфраструктуры открытых ключей, в которой каждый сертификат удостоверяет выделение адресов IP, а выпуск подчиненных (subordinate) сертификатов соответствует выделению фрагментов этого блока адресов IP. Сказанное выше относится и к распределению номеров AS, но правом «вторичного» выделения номеров AS наделены только RIR и NIR. Таким образом, распределение адресов IP и номеров AS можно выразить в рамках одной инфраструктуры PKI. Эта PKI, которую в дальнейшем будем называть инфраструктурой открытых ключей ресурсов (RPKI), является центральной компонентой этой архитектуры.

2.1. Роль в архитектуре

Сертификаты в PKI называют сертификатами ресурсов и они соответствуют профилю, заданному в [RFC6487]. Сертификаты ресурсов удостоверяют выделение субъекту адресов IP или номеров AS эмитентом (сертификата). Это нужно для привязки открытого ключа в сертификате ресурса к адресам IP или номерам AS, включенным в расширения сертификата IP Address Delegation или AS Identifier Delegation, как указано в RFC 3779 [RFC3779].

Важной особенностью этой PKI является то, что сертификаты не удостоверяют отождествление субъекта. Следовательно, имена субъектов в сертификатах не обязаны быть описательными. Т. е. PKI ресурсов предназначена для проверки полномочий, а не подлинности субъекта. Этим она отличается от большинства других PKI, где эмитент гарантирует, что описательное имя субъекта сертификата надежно связано с объектом, который владеет секретным ключом, соответствующим открытому ключу в сертификате. Поскольку от эмитентов не требуется проверка права объекта на использование указанного в сертификате имени субъекта, это позволяет устранить связанные с такой проверкой издержки и ответственность. В результате исполнение функций органа сертификации (CA[2]) существенно упрощается.

Большинство сертификатов этой PKI подтверждают базовые факты, на основе которых работает остальная инфраструктура. Сертификаты CA в PKI удостоверяют обладание адресными блоками IP и номерами AS. Сертификаты конечных элементов (EE[3]) выпускаются CA владельца ресурса для передачи полномочий, подтверждаемых этими сертификатами. Основным назначением сертификатов EE является проверка пригодности полномочий генерации маршрутов (ROA[4]), подписанных объектов, которые явно подтверждают передачу владельцем ресурса прав генерации маршрутов в указанный блок адресов данной AS (см. раздел 3). Сертификаты конечных элементов используются также для проверки других подписанных объектов типа манифестов, которые будут использоваться для обеспечения целостности системы репозиториев (см. раздел 5).

2.2. Сертификаты CA

Любой держатель ресурса, имеющий полномочия дальнейшего распределения этого ресурса, должен иметь возможность выпускать сертификаты ресурсов в соответствии с выделением. Например, сертификаты CA будут связаны с IANA и каждым из регистраторов RIR, NIR и LIR/ISP. Сертификат CA требуется также для обеспечения держателю ресурса возможности выпуска ROA, поскольку он должен выпустить соответствующий сертификат конечного элемента для проверки пригодности каждого ROA. Таким образом, некоторые объекты, которые не распределяют свои ресурсы между другими объектами, также должны иметь сертификаты CA для своих ресурсов (например, абоненту с несколькими подключениями и провайдеро-независимым болком адресов потребуется сертификат для выпуска ROA). Абонентам с одним подключением и адресами от LIR/ISP, если они не переходят к другому LIR/ISP, не потребуется участие в PKI. Абонентам с несколькими подключениями и адресами от LIR/ISP в некоторых случаях может потребоваться участие в PKI (см. параграф 7.3.2).

В отличие от большинства других PKI, здесь отличительные имена субъектов в сертификатах CA выбираются эмитентом сертификата. Отличительные имена субъектов не пытаются описать эти субъекты. Отличительное имя субъекта должно включать атрибут CommonName и может дополнительно включать атрибут serial.

В этой PKI эмитенты сертификатов, являясь регистраторами RIR, NIR или LIR/ISP, не занимаются проверкой юридических прав субъекта на заявленное им отождествление. Следовательно, выбор отличительного имени, не пытающегося описать этот субъект, минимизирует возможности субъектов злоупотреблять сертификатами для отождествления себя и минимизирует юридическую ответственность эмитентов. Поскольку все сертификаты CA выпускаются для субъектов, с которыми эмитент имеет реальное взаимодействие, эмитентам рекомендуется выбирать для субъектов имена, которые позволят связать сертификат с имеющимися в его базе данных записями для этого субъекта. Например, регистратор может использовать ключи своей базы данных или идентификаторы абонентов в качестве атрибута CommonName выпускаемых для субъекта сертификатов.

Хотя общая часть имен субъектов в сертификатах не идентифицирует эти субъекты, такие имена должны быть уникальными для каждого субъекта, которому данный CA выпускает сертификаты. Т. е. для CA недопустимо выпускать для разных субъектов сертификаты с совпадающей общей частью имени.

Каждый сертификат ресурса удостоверяет выделение ресурса его держателю (владельцу), поэтому объекты, получившие ресурсы из разных источников, будут иметь множество сертификатов CA. Отметим, что в сертификатах,

[1]Термин LIR в некоторых регионах используется для обозначения ISP. Поэтому в оставшейся части документа применяется обозначение LIR/ISP в целях упрощения.
[2]Certification Authority — агентство по сертификации.
[3]End-entity.
[4]Route Origination Authorization.

полученных одним элементом (объектом) из разных источников, имена субъектов в общем случае будут различаться. CA может также выпускать разные сертификаты для каждого выделения одному объекту, если данный CA и держатель ресурса считают, что это будет облегчать управление и использование сертификатов. Например, LIR/ISP может иметь несколько сертификатов, выпущенных одним регистратором, каждый из которых описывает отдельный блок адресов, поскольку LIR/ISP считает нужным рассматривать выделение этих блоков порознь.

2.3. Сертификаты конечных элементов (EE)

Секретный ключ, соответствующий открытому ключу в сертификате EE, не применяется для подписи других сертификатов в PKI. Основным назначением сертификатов EE в этой PKI является проверка подписанных объектов, которые относятся к использования описанных в сертификатах ресурсов (например, ROA и манифестов).

Для ROA и манифестов имеется взаимно-однозначное соответствие между сертификатами конечных элементов и подписанными объектами, т. е. секретный ключ, соответствующий каждому сертификату конечного элемента, используется для подписи единственного объекта и каждый объект подписывается только с одним ключом. Это свойство позволяет использовать PKI для отзыва этих подписанных объектов без создания отдельного нового механизма отзыва. Когда сертификат конечного элемента, использованный для подписи данного объекта, отзывается подпись этого объекта (и все соответствующие утверждения) будет считаться непригодной, что эффективно означает отзыв подписанного объекта путем отзыва сертификата конечного элемента, использованного для подписи объекта.

Второе преимущество этого взаимно-однозначного соответствия заключается в том, что секретный ключ, соответствующий открытому ключу в сертификате, используется единственный раз и может быть уничтожен после его использования для подписи одного объекта. Это существенно упрощает поддержку ключей, поскольку не требуется обеспечивать защиту секретных ключей в течение долгого времени.

Сертификат EE, используемый для проверки подписанного объекта инкапсулируется CMS[1] (см. [RFC6488]) подписанного объекта. Следовательно, не требуется передавать сертификат EE отдельно от подписанного объекта. Подобно этому, не требуется присутствия сертификата EE в системе репозиториев RPKI иначе, чем в виде части соответствующего подписанного объекта.

Хотя в этом документе описаны лишь два варианта применения сертификатов конечных элементов, в будущем могут быть определены и другие приложения. Например, сертификаты EE могут применяться в качестве более обобщенной проверки полномочий их субъектов для использования от имени владельца заданного ресурса. Это может упростить проверку подлинности при взаимодействиях между ISP, или с системой репозиториев. Эти дополнительные варианты использования сертификатов конечных элементов могут потребовать сохранения соответствующих секретных ключей, хотя этого не требуется для ключей, применяемых для подписи манифестов и ROA.

2.4. Доверенные привязки

В любой PKI каждая зависимая от нее сторона (RP[2]) выбирает свой комплект доверенных привязок (TA[3]). Это общее свойство систем PKI применимо и здесь. Имеется иерархия выделения адресов IP и номеров AS и, таким образом IANA и,или пять регистраторов RIR являются очевидными кандидатами на роль TA. Тем не менее, каждый RP самостоятельно выбирает для себя множество доверенных привязок, которые будут применяться для проверки пригодности сертификатов.

Например, RP (пусть это будет LIR/ISP) может создать доверенную привязку применительно ко всему адресному пространству и/или всем номерам AS, для которой RP имеет соответствующий секретный ключ. После этого RP может выпускать сертификаты с этой доверенной привязкой для любого желаемого объекта в PKI и это приведет к тому, что все пути сертификации, завершающиеся в этой заданной локально привязке, будут соответствовать требованиям по проверке пригодности, указанным в RFC 3779. Крупным ISP, которые используют блоки приватных адресов IP (см. RFC 1918) и применяют внутри себя протокол BGP, потребуется создать такой тип доверенной привязки чтобы организовать CA, которому выделено все пространство приватных адресов. После этого RP может в рамках этого CA выпускать сертификаты, которые будут соответствовать внутреннему использованию приватных адресов.

Отметим, что RP выбравшие создание и поддержку собственного набора доверенных привязок, могут не заметить ошибок выделения ресурсов, которые возникают при таких обстоятельствах, но создают проблемы лишь для этого RP.

Предполагается, что некоторые элементы существующей иерархии распределения адресов IP и номеров AS могут опубликовать материал о доверенных привязках для использования от инфраструктуры зависимыми сторонами (RP). Стандартный профиль для публикации такого материала можно найти в [RFC6490].

3. Полномочия на создание маршрутов

Информации о распределении адресов IP, предоставляемой инфраструктурой PKI, самой по себе недостаточно для управления решениями о маршрутизации. В частности, протокол BGP работает на основе допущения о том, что AS, создающая маршруты для конкретного префикса, имеет на это полномочия от владельца этого префикса (или блока адресов, включающего данный префикс), однако PKI не имеет информации о таких полномочиях. ROA позволяют явно выразить такие полномочия и предоставляют владельцам адресных блоков IP возможность создания объектов, которые явно и проверяемо указывают, что AS уполномочена на создание маршрутов к данному набору префиксов.

3.1. Роль в архитектуре

ROA подтверждают факт передачи владельцем префиксов полномочий по созданию маршрутов к этим префиксам автономной системе. Структура ROA соответствует формату, описанному в [RFC6482]. Действительность полномочий зависит от того, является ли подписавшая ROA сторона держателем префикса в ROA, - это удостоверяется сертификатом конечного элемента из PKI, чей секретный ключ соответствует использованному для подписи ROA.

ROA могут использоваться зависимыми сторонами для проверки того, что AS, создавшая маршрут для данного префикса IP, имеет полномочия от владельца данного префикса. Например, ISP может использовать действительные

[1]Cryptographic Message Syntax — синтаксис криптографических сообщений.
[2]Relying party — зависимая сторона, потребитель.
[3]Trust anchor.

ROA в качестве входных данных при создании маршрутных фильтров для своих маршрутизаторов BGP (см. [RFC6483], где описано использование ROA в целях проверки полномочий на создание маршрутов BGP).

Изначально система репозиториев будет основным механизмом распространения ROA, поскольку эти репозитории будут содержать сертификаты и CRL, требуемые для проверки ROA. В дополнение к этому ROA могут распространяться также в сообщениях UPDATE или по иным коммуникационным каналам, если этот требуется для своевременной доставки.

3.2. Синтаксис и семантика

ROA представляет собой явное разрешение для одной AS создавать маршруты к одному или множеству префиксов и подписывается владельцем этих префиксов. Концептуально ROA состоит из двух частей — общего шаблона CMS, одинакового для всех подписанных объектов RPKI [RFC6488] и инкапсулированного содержимого ROA, которое указывает наличие полномочий [RFC6482].

На высоком уровне ROA содержит (1) номер AS и (2) список адресных префиксов IP, дополнительно может включаться (3) максимальный размер наиболее конкретных префиксов, которые AS имеет право анонсировать для каждого префикса (этот элемент упрощает компактную передачу полномочий на анонсирования, например, любых префиксов длиной от 20 до 24 битов, содержащихся внутри данного 20-битового префикса).

Отметим, что ROA содержит единственный номер AS. Таким образом, если ISP имеет множество номеров AS, которым разрешено создавать маршруты для префиксов из этой ROA, владельцу адресного блока придется выпустить множество ROA для передачи ISP полномочий по созданию маршрутов для множества автономных систем.

ROA подптсывается с использованием секретного ключа, соответствующего открытому ключу в сертификате конечного элемента (EE) в инфраструктуре PKI. Для того, чтобы ROA была пригодна, соответствующий ей сертификат конечного элемента должен быть действительным и префиксы адресов IP в ROA должны совпадать с префиксами адресов IP, указанными в расширении (RFC 3779) сертификата EE. Следовательно, срок действия ROA неявно определяется сроком действия соответствующего сертификата. ROA отзываются путем отзыва соответствующих сертификатов EE. Отдельного метода отзыва ROA не задается. Можно подумать, что такая модель отзыва будет приводить к увеличению размера списков CRL для сертификации CA, подписывающих сертификаты EE. Однако маршрутные анонсы в публичной сети Internet используются достаточно долго. Следовательно, поскольку сертификаты EE служащие для проверки ROA действительны несколько месяцев, вероятность отзыва множества ROA в течение этого срока достаточно мала.

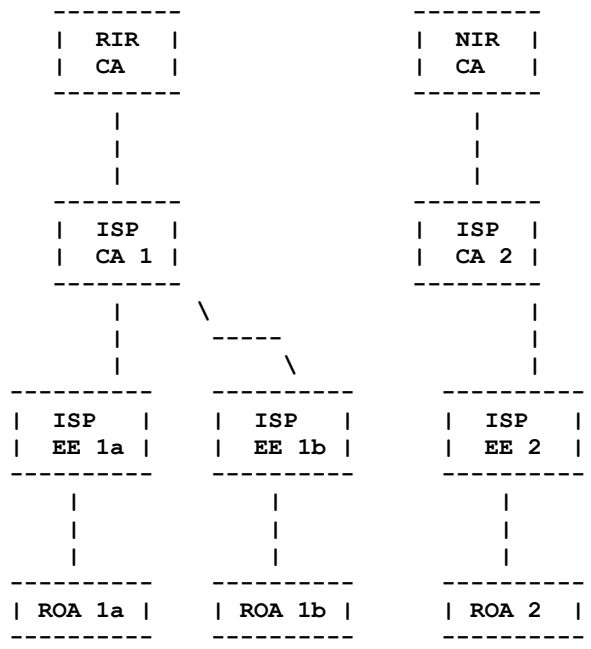

Рисунок 1. ISP, получающий ресурсы от RIR и NIR (требуется два сертификата CA в соответствии с RFC 3779)

Поскольку каждое разрешение ROA связывается с одним сертификатом конечного объекта, набор префиксов IP в ROA должен приниматься из одного источника (т. е. в одном ROA нельзя объединять выделения адресов из разных источников). Владельцы адресных блоков из разных источников, которым нужно передать AS полномочия по созданию маршрутов в эти блоки, должны выпускать множество ROA для такой AS.

4. Репозитории

Изначально LIR/ISP будут использовать ресурсы PKI путем получения и проверки каждого разрешения ROA для создания таблицы префиксов, к которым AS уполномочена создавать маршруты. Для проверки пригодности ROA провайдерам (LIR/ISP) потребуется получить все сертификаты и CRL. Основной функцией системы распределенных репозиториев, описанной здесь, является хранение этих подписанных объектов и обеспечение их доступности для загрузки LIR/ISP. Отметим, что эта система репозиториев обеспечивает механизм, с помощью которого зависимые стороны могут получать свежие данные с удобной для себя частотой обновления. Однако не обеспечивается механизмов «выталкивания» свежих данных зависимым сторонам (например, путем включения объектов PKI в сообщения BGP или других протоколов) и такие механизмы выходят за рамки настоящего документа.

Цифровые подписи для всех объектов в репозитории гарантируют обнаружение несанкционированных изменений в объектах зависимыми сторонами. Кроме того, все репозитории используют манифесты (раздел 5) для того, чтобы

гарантировать зависимым сторонам факты удаления действующих объектов или вставки просроченных объектов с действительной подписью.

Система репозиториев является также пунктом контроля доступа к хранящимся в них подписанным объектам (например, предоставляя возможность манипуляций с записями, относящимися к выделению ресурсов, только уполномоченным сторонам). Использование контроля доступа предотвращает атаки, нацеленные на отказ служб, путем удаления или подделки объектов в репозитории). Зависимые от инфраструктуры стороны способны обнаружить подделку объектов в репозитории, однако лучше предотвращать несанционированные изменения на уровне системы репозиториев, насколько это возможно.

4.1. Роль в архитектуре

Система репозиторией является недоверенным «клиринговым центром» для всех подписанных объектов, которые должны быть доступны зависимым сторонам в глобальном масштабе. При создании сертификатов и CRL они размещаются (выгружаются) в этом репозитории, а потом загружаются зависимыми сторонами (в основном LIR/ISP) для использования. ROA и манифесты являются примерами дополнительных объектов в репозитории, а в будущем архитектура может быть дополнена другими элементами. В этом документе кратко описаны способы поддержки подписанных объектов (сертификаты, CRL, ROA и манифесты) в репозитории. По мере добавления в систему репозиториев новых подписанных элементов это описание потребует внесения изменений, но предполагается, что основные принципы устройства сохранятся неизменными. Полное описание системы репозиториев дано в [RFC6481].

4.2. Содержимое и структура

Хотя репозиторий представляет собой единую систему, к которой обращаются зависимые стороны, в реальности эта система состоит из множества баз данных. Эти базы распределены между регистраторами (RIR, NIR, LIR/ISP). По минимуму база данных, поддерживаемая каждым из регистраторов, будет включать все сертификаты CA и EE, списки CRL и манифесты, подписанные CA, которые связаны с этим регистратором. Репозитории LIR/ISP будут включать также ROA. Регистраторам также настоятельно рекомендуется хранить копии данных из репозиториев их клиентов и клиентв этих клиентов (и . д.) для облегчения доступа зависимых сторон ко всему содержимому репозитория. В идеальном случае каждый RIR будет держать у себя данные PKI от всех элементов своего географического региона.

Для каждого сертификата в PKI в файловой системе репозитория будет присутствовать каталог, служащий полномочной точкой публикации для всех объектов (сертификаты, CRL, ROA и манифесты), проверяемых с помощью этого сертификата. Расширение сертификата SIA[1] [RFC5280] содержит идентификатор URI, указывающий этот каталог. Кроме того, расширение сертификата AIA[2] [RFC5280] содержит URI со ссылкой на полномочное место публикации сертификата CA, который применялся для выпуска данного сертификата. Т. е. если сертификат A служит для проверки сертификата B, расширение AIA в сертификате B указывает на сертификат A, а расширение SIA в сертификате A указывает каталог с сертификатом B (см. Рисунок 2).

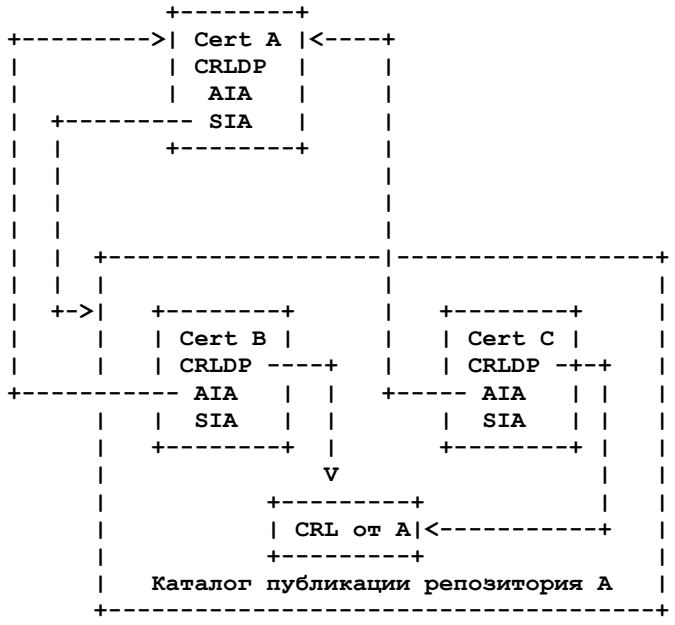

Рисунок 2. Использование расширений SIA и AIA в RPKI.

На рисунке 2 сертификаты B и C выпущены CA A. Следовательно, расширения AIA в сертификатах B и C указывают на (сертификат) A, а расширение SIA в A указывает на точку публикации подчиненной продукции CA A, включающую сертификаты B и C, а также CRL, выпущенные A. Расширение CRLDP[3] в сертификатах B и C указывает на CRL, выпущенные A.

Если сертификат CA выпускается заново с тем же открытым ключом, нет необходимости заново выпускать (с обновленными AIA URI) все сертификаты, подписанные с помощью обновляемого сертификата. Поэтому CA **следует** использовать постоянную схему именования URI для выпускаемых сертификатов. Т. е. в выпущенных повторно сертификатах следует применять ту же точку публикации, которая была указана в ранее выпущенных сертификатам для того же субъекта с использованием того же открытого ключа. Прежние варианты сертификата заменяются новыми.

[1]Subject Information Access — доступ к информации о субъекте.
[2]Authority Information Access — доступ к информации об агентстве.
[3]CRL Distribution Points — точки публикации CRL.

4.3. Протоколы доступа

Операторы репозиториев могут выбрать один или несколько протоколов доступа, с помощью которых зависимые от инфраструктуры стороны будут получать доступ к системе репозиториев. Эти протоколы будут использоваться множеством участников инфраструктуры (например, все регистраторы, ISP и абоненты с множественными подключениями) для поддержки соответствующих частей репозитория. Для этого требуется обеспечить некую базовую функциональность с набором протоколов доступа, как описано ниже. Для реализации всех этих функций не требуется единственный протокол (хотя такой вариант возможен), но каждая функция **должна** быть реализована на базе по крайней мере одного протокола, поддерживаемого оператором репозитория.

Загрузка (download). Протоколы доступа должны поддерживать загрузку больших объемов данных из репозитория, а также последующую загрузку изменений и это будет основным типом взаимодействия зависимых сторон с репозиторием. Могут также поддерживаться другие типы взаимодействия с репозиторием (например, загрузка одного объекта).

Выгрузка, обновление, удаление (upload/change/delete). Протоколы доступа должны также поддерживать для издателей сертификатов, CRL и других подписанных объектов возможность добавления и удаления таких объектов. Должны обеспечиваться также механизмы изменения объектов в репозитории. Все протоколы доступа, позволяющие вносить изменения в репозиторий (путем добавления, удаления или изменения его содержимого), должны поддерживать проверку полномочий вносящей изменения стороны и использованием подходящего контроля доступа (см. параграф 4.4).

Для обеспечения всем зависимым сторонам возможности получать все подписанные объекты RPKI все точки публикации **должны** быть доступны по протоколу rsync (см. [RFC5781] и [RSYNC]), хотя **могут** применяться и другие протоколы загрузки. Точки публикации репозитория могут обеспечивать функциональность добавления, удаления и изменения объектов с помощью желаемого набора протоколов доступа, при условии того, что все такие протоколы подходят для коммуникаций всем сертификационным органам, содержащим данные в этой точке публикации.

4.4. Управление доступом

Для поддержки целостности данных в репозитории должны быть организованы средства контроля, предотвращающие несанкционированное добавление, изменение и удаление объектов. Отождествление сторон, пытающихся внести изменения, может проверяться с помощью подходящих протоколов доступа. Хотя конкретные правила доступа определяются операторами репозитория, **рекомендуется** разрешать добавление, изменение и удаление подписанных объектов только их эмитентам. Дополнительно в будущем может оказаться полезным определение формального механизма передачи полномочий, чтобы позволить держателям ресурсов передавать другим сторонам право действий от своего имени, как предложено в параграфе 2.3.

5. Манифесты

Манифест представляет собой подписанный объект со списком всех подписанных объектов (кроме самого манифеста), выпущенных органом, ответственным за публикацию в системе репозитория. Для каждого действующего сертификата, CRL или ROA, выпущенного агентством, манифест содержит имя файла с объектом и хэш содержимого этого файла.

Ка и ROA, манифест подписывается с помощью секретного ключа, парный открытый ключ которого указан в сертификате конечного элемента. Этот сертификат EE, в свою очередь, подписывается соответствующим CA. Поскольку секретный ключ в сертификате EE используется для подписи единственного манифеста, этот манифест можно отозвать путем отзыва сертификата EE. В таких случаях для предотвращения неоправданного роста CRL срок действия сертификата EE, используемого для проверки манифеста, **следует** делать таким же как у самого манифеста.

Манифесты могут применяться зависимыми сторонами при создании локального кэша (см. раздел 6) для снижения риска атак с удалением файлов из репозитория или подменой подписанных объектов. Такая защита нужна, поскольку система репозитория не является доверенной, несмотря на подписи во всех объектах.

5.1. Синтаксис и семантика

Манифест содержит список всех файлов (и хэш-значений их содержимого) в точке публикации репозитория на конкретный момент. Подробная спецификация содержимого манифеста приведена в [RFC6486], кратко же можно сказать, что манифест включает (1) порядковый номер, (2) время выпуска, (3) время планового выпуска следующего манифеста, (4) список имен файлов и хэш-значений их содержимого.

Номер манифеста является числом, которое увеличивается при выпуска каждого нового манифеста. Агентству **требуется** выпускать новый манифест по факту изменения содержимого репозитория или наступления заданного момента обновления манифеста. Таким образом, манифест действует до наступления указанного в нем срока обновления или до появления манифеста с большим порядковым номером (до первого из событий). Отметим, что сертификат EE используется для подписи лишь одного манифеста и при выпуске нового манифеста CA **должен** также выпустить новый CRL с включением сертификата EE, соответствующего старому манифесту. Отозванный сертификат EE для старого манифеста будет удален из CRL по истечении срока его действия и списки CRL сильно расти не будут.

6. Поддержка локального кэша

Для использования подписанных объектов, выпущенных в этой PKI, зависимая сторона должна сначала получить локальную копию действующих сертификатов EE для PKI. Для этого нужно выполнить перечисленные ниже действия.

1. Запросить в системе репозиториев копии всех сертификатов, манифестов и CRL, выпущенных в PKI.
2. Для каждого сертификата CA в PKI проверить подпись соответствующего манифеста. Дополнительно убедиться, что текущее время меньше значения, указанного в поле nextUpdate манифеста.
3. Для каждого манифеста проверить, что сертификаты и CRL, выпущенные с помощью соответствующего сертификата CA, соответствуют хэш-значениям в манифесте. Убедиться в том, что манифест не содержит отсутствующих в репозитории сертификатов и манифестов. При несоответствии хэш-значений или отсутствии какого-либо сертификата или CRL следует уведомить администратора репозитория о повреждении данных.

4. Проверить пригодность каждого сертификата EE путем построения и проверки пути сертификации (включая проверку относящихся к нему CRL) до заданных в локальной конфигурации TA (см. [RFC6487]).

Поскольку зависимые стороны будут проводить эти проверки регулярно, эффективней для них будет запрашивать из репозитория лишь объекты, изменившиеся с момента последнего обновления локального кэша зависимой стороны.

Отметим также, что проверка соответствия манифесту всех выпущенных объектов позволяет зависимой стороне быть уверенной в том, что не были пропущены обновления каких-либо объектов.

7. Основные операции

Создание и поддержка описанной выше инфраструктуры потребует дополнительных «побочных» операций при нормальном распределении ресурсов и процедур проверки полномочий маршрутизации. Например, абонент с провайдеро-независимыми (переносимыми) адресами, организующий взаимодействие с ISP, должен будет выпустить одно или множество разрешений ROA, указывающих данного провайдера (ISP), в дополнение к обычным техническим и административным процедурам. Основным современным применением этой инфраструктуры является создание маршрутных фильтров — используя ROA, можно создавать фильтры маршрутов автоматически и с гарантией того, что держатель анонсируемого префикса уполномочил создающую маршруты AS на анонсирование этих маршрутов.

7.1. Издание сертификатов

Выпуск сертификатов требуется в нескольких ситуациях. Для любого выделения, которое может быть разделено по субстратам , требуется сертификат CA - например, для того, чтобы выпускать сертификаты при возникновении необходимости выделения очередного субстрата. Владельцы провайдеро-независимых адресов IP тоже должны иметь сертификаты, чтобы иметь возможность выпуска ROA для каждого ISP, уполномоченного создавать маршрут к этим блокам адресов (поскольку адреса получены не от ISP). Кроме того, обонентам с множественными подключениями тоже нужны сертификаты, если они намерены выпускать ROA для своих адресов (см. параграф 7.3.2). Прочим держателям ресурсов не требуются сертификаты CA в рамках PKI.

В конечном итоге владелец ресурса не будет запрашивать сертификаты ресурса, а получит их в качестве «побочного» эффекта при выделении ресурса. Однако при начальном развертывании RPKI потребуется явный выпуск множества сертификатов для выделенных ранее ресурсов. Отметим, что во всех случаях органом, выпускающим сертификат CA, будет тот, кто выделил ресурс. Это отличается от других PKI, где субъект может запросить сертификат в любом CA.

Если владелец ресурса с течением времени получает множество распределений, он может увеличить набор сертификатов для подтверждения этих ресурсов. Если держатель ресурса получает множество распределений из одного источника, множество таких ресурсов может быть объединено в одном сертификате ресурса при согласии на это держателя ресурсов и эмитента. Это реализуется путем объединения множества расширений IP Address Delegation и AS Identifier Delegation в одиночные расширения (каждого типа) нового сертификата. Однако создание комбинированного сертификата для ресурсов с разными сроками действия может вызывать проблемы, поскольку в сертификате может быть только один срок действия.

Если ресурсы выделены из разных источников, они будут подписаны разными CA и не могут быть объединены. Если выделенные ресурсы больше не принадлежат их держателю, подтверждающие это выделение сертификаты **должны** быть отозваны. Держателю ресурса **не следует** применять один и тот же открытый ключ во множестве сертификатов CA от одного или разных эмитентов, поскольку повторное использование пары ключей усложняет создание пути сертификации. Отметим, что отличительные имена субъектов задаются эмитентами и для ресурсов, выделенных одному держателю из разных источников, имена субъекта в сертификатах в общем случае будут разными.

7.2. Смена ключа CA

Когда орган сертификации хочет сменить открытый (и соответствующий секретный) ключ, связанный с сертификатом RPKI CA, он **должен** выполнить процедуру смены ключей. Обычно замена ключей происходит периодически и частота смены задается в заявлении о практике сертификации данного CA. Однако при компрометации ключа может потребоваться незапланированная смена.

Отметим, что процедура смены нужна лишь при реальной замене ключей CA и не требуется при выпуске нового сертификата CA с тем же ключом, который был в предыдущем сертификате для этого CA. Например, требуется выпуск нового сертификата CA, если CA получает или освобождает ресурс, а также при завершении срока действия выделенного ресурса. Однако в таких случаях новый сертификат обычно будет использовать прежний открытый (и секретный) ключ и замена ключей не требуется.

В [RFC6489] задана консервативная процедура смены ключей, которую центрам сертификации следует применять при замене открытого (и секретного) ключа, связанного с его сертификатом RPKI CA. Основные свойства этой процедуры указаны ниже. Во-первых, поскольку данные из подписанных объектов RPKI могут применяться в маршрутизации, процедура гарантирует, что в процессе ее выполнения ни одна из зависимых сторон не получит некорректных заключений о пригодности подписанных объектов. Отметим, в частности, что CA не может предполагать использование зависимыми сторонами какого-либо конкретного алгоритма построения пути сертификации от сертификата EE до одной из доверенных привязок. Следовательно в течение процедуры смены ключей обеспечивается максимально возможная целостность точек SIA и AIA в иерархии RPKI. Во-вторых, процедура смены ключей рассчитана так, что повторный выпуск всех сертификатов, расположенных ниже данного CA в иерархии RPKI, не требуется. Естественно, потребуется заново подписать все сертификаты, выпущенные непосредственно CA, меняющим ключи. Однако указатели SIA и AIA в сертификатах задаются так, что дальнейшего повторного выпуска сертификатов не требуется.

7.3. Управление ROA

Когда держатель адресов IP хочет передать AS полномочия на создание маршрутов к его адресам, он **должен** выпустить сертификат конечного элемента с нужным префиксом в расширении IP Address Delegation. Для подписи ROA с адресным префиксом и номером уполномоченной AS используется соответствующий секретный ключ. Держатель адресов **может** включить в сертификат EE и соответствующее разрешение ROA множество адресных префиксов. Любой держатель адресов, выпускающий ROA для префикса должен иметь сертификат ресурса для включающего этот префикс распределения. Стандартная процедура выпуска ROA описана ниже.

1. Создается сертификат конечного элемента с префиксом (префиксами) для которого ROA дает полномочия.
2. Создается содержимое ROA с префиксами из сертификата EE и номером AS, получающей полномочия.
3. ROA подписывается с использованием секретного ключа, соответствующего сертификату EE (ROA представляется содержимым, инкапсулированным в подписанное сообщение CMS [RFC5652]).
4. Сертификат конечного элемента и ROA выгружаются в систему репозитория.

Стандартная процедура отзыва ROA заключается в отзыве соответствующего сертификата конечного элемента путем выпуска CRL и выгрузки его в репозиторий. Отозванные ROA и сертификаты EE **следует** удалять из репозитория.

При отзыве ROA следует соблюдать осторожность, поскольку такой отзыв может привести к тому, что зависимые стороны сочтут маршрутные анонсы, соответствующих префиксам и номеру AS в ROA, несанкционированными (и это может привести к изменению картины маршрутизации с отказом от пересылки пакетов на основе этих анонсов). В частности, держателю ресурса следует придерживаться описанного ниже принципа «сделать до прерывания». Перед отзывом ROA для префикса, который держатель хочет маршрутизировать в Internet, важно обеспечить для этого ресурса наличие другого действительного разрешения ROA с тем же префиксом (номер AS может быть иным). Кроме того, держателю ресурса следует убедиться в том, что AS, указанная в дополнительном ROA, действительно создает маршруты к соответствующему префиксу. Зависимая от инфраструктуры сторона должна получить новые ROA из системы репозитория до принятия маршрутных решений в ответ на отзыв ROA.

7.3.1. Абоненты с одним подключением

В BGP абонентам с одним подключением и адресами от провайдера (PA[1]) не нужно явно давать разрешение на анонсы маршрутов к используемым префиксам, поскольку его ISP уже анонсирует более общий префикс и маршрутизирует трафик в сеть абонента. Поскольку для префиксов таких абонентов отдельные маршруты не анонсируются, выпуск ROA также не нужен - ISP абонента будет выпускать нужные ROA для более общих префиксов с сертификатами своих ресурсов. Таким образом «однодомный» абонент с адресами IP из блока своего провайдера просто не входит в RPKI, не получая сертификата CA и не выпуская сертификатов EE или разрешений ROA.

7.3.2. Абоненты с множеством подключений

Рассмотрим абонента с адресами PA от основного ISP (т. е., IP-адреса этого абонента являются частью адресного пространства этого ISP) и дополнительным «восходящим» соединением с одним или несколькими резервными ISP. Для таких «многодомных» абонентов предпочтительным решением является получение номера AS и использование протокола BGP для каждого из своих провайдеров. Для такой ситуации **рекомендуется** два способа поддержки ROA. В первом основной ISP выпускает сертификат CA для абонента и этот абонент выпускает ROA со своим номером AS и адресным префиксом IP. Во втором варианте ISP не выпускает сертификата CA для абонента, а просто от его имени выпускает ROA с номером AS и префиксом IP этого абонента.

Если абонент не может или не хочет получить номер AS и использовать BGP, он может запросить у своего основного ISP создание ROA для каждого дополнительного ISP, дающие этим ISP полномочия на создание маршрутов к блоку адресов абонента. Основной ISP также создает ROA со своим номером AS и адресным префиксом абонента. Очевидно, что в таких случаях основной ISP будет анонсировать точный префикс абонента, а не включающий его блок адресов. Отметим, что такой подход ведет к несогласованности номеров AS происхождения маршрута и адресных префиксов абонентов, что является нежелательным для публичной сети Internet и по этой причине **не рекомендуется**.

7.3.3. Провайдеро-независимые адреса

Провайдеро-независимыми (переносимыми) называются блоки адресов, получаемые абонентами непосредственно от RIR или NIR. Поскольку такие блоки адресов не входят в пространство какого-либо ISP, ни один из провайдеров не будет анонсировать более общий префикс. Держатель переносимого блока адресов IP **должен** предоставить одной или множеству AS полномочия на создание маршрутов к своим префиксам. Поэтому держатель ресурса **должен** создать один или множество сертификатов EE и соответствующих ROA, чтобы позволить этим AS создавать маршруты к его префиксам. Выпуск ROA требуется по причине того, что ROA провайдеров не дают полномочий на создание маршрутов в переносимый блок адресов.

8. Вопросы безопасности

Этот документ сфокусирован на защите и вопросы безопасности органически входят в эту спецификацию.

Механизмы защиты, обеспечиваемые этой архитектурой, основаны на целостности и доступности описываемой инфраструктуры. Целостность объектов в инфраструктуре обеспечивается средствами контроля доступа к репозиториям, описанными в параграфе 4.4. В силу своей распределенной структуры система репозитория устойчива к атакам на отказ в обслуживании (denial-of-service), однако нужны и дополнительные меры предосторожности на базе репликации и создания резервных копий, а также физической защиты серверов с базами данных.

9. Взаимодействие с IANA

Инструкции для IANA в части RPKI приведены в [RFC6491].

10. Благодарности

Описанная здесь архитектура основана на идеях и работе большой группы людей. Работа была бы невозможна без интеллектуального вклада George Michaelson, Robert Loomans, Sanjaya и Geoff Huston из APNIC, Robert Kisteleki и Henk Uijterwaal из RIPE NCC, Tim Christensen и Cathy Murphy из ARIN, Rob Austein из ISC и Randy Bush из IIJ.

Авторы в долгу перед всеми, кто внес вклад в эту архитектуру, но особо хочется отметить Rob Austein за концепцию манифеста и Geoff Huston за концепцию проверки пригодности объектов на базе однократного применения ключевых пар сертификатов EE, а также Richard Barnes за помощь в подготовке предварительной версии этого документа.

[1]Provider Aggregatable — агрегируемые провайдером.

11. Литература

11.1. Нормативные документы

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

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

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[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.

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

[RFC5781] Weiler, S., Ward, D., and R. Housley, "The rsync URI Scheme", RFC 5781, February 2010.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, February 2012.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

[RFC6486] Austein, R., Huston., G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure", RFC 6486, February 2012.

[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", RFC 6488, February 2012.

[RFC6491] Manderson, T., Vegoda, L., and S. Kent, "Resource Public Key Infrastructure (RPKI) Objects Issued by IANA", RFC 6491, February 2012.

11.2. Дополнительная литература

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, February 2012.

[RFC6489] Huston, G., Michaelson, G., and S. Kent, "Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)", BCP 174, RFC 6489, February 2012.

[RFC6490] Huston, G., Weiler, S., Michaelson, G., and S. Kent, "Resource Public Key Infrastructure (RPKI) Trust Anchor Locator", RFC 6490, February 2012.

[RSYNC] rsync web pages, <http://rsync.samba.org/>.

[S-BGP] Kent, S., Lynn, C., and Seo, K., "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, April 2000.

[soBGP] White, R., "soBGP", May 2005, <ftp://ftp-eng.cisco.com/sobgp/index.html>

Адреса авторов

Matt Lepinski

BBN Technologies

10 Moulton St.

Cambridge, MA 02138

EMail: mlepinski@bbn.com

Stephen Kent

BBN Technologies

10 Moulton St.

Cambridge, MA 02138

EMail: kent@bbn.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com