Internet Engineering Task Force (IETF)
Request for Comments: 6481
Category: Standards Track
ISSN: 2070-1721

G. Huston
R. Loomans
G. Michaelson
APNIC

February 2012

Профиль структуры репозитория сертификатов ресурсов

A Profile for Resource Certificate Repository Structure

Аннотация

Этот документ определяет профиль для структуры распределенного репозитория ресурсов инфраструктуры открытых ключей ресурсов (RPKI[1]). Каждая отдельная точка публикации репозитория является каталогом, содержащим файлы, которые соответствуют сертификатам ресурсов X.509/PKIX, спискам отзыва (CRL[2]) и подписанным объектам. Профиль определяет схему именования объектов (файлов), содержимое точек публикации репозитория (каталогов) и предлагаемую внутреннюю структуру локального кэша репозитория для облегчения процедур синхронизации распределенного множества точек публикации и процедур построения путей сертификации.

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/rfc6481.

Оглавление

1. Введение

Для проверки аттестаций, сделанных в контексте RPKI [RFC6480] зависимым сторонам (RP[5]) нужен доступ ко всем сертификатам ресурсов X.509/PKIX, спискам отзыва (CRL) и подписанным объектам, совместно определяющим RPKI.

Каждый эмитент сертификата, CRL или подписанного объекта делает его доступным для загрузки в RP путём публикации объектов в репозитории RPKI.

[1]Resource Public Key Infrastructure.
[2]Certificate Revocation List - список отзыва сертификатов.
[3]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[5]Relying party.

Система репозиториев (хранилищ) представляет собой коллекцию всех подписанных объектов, которая **должна** быть доступна глобально для всех RP. При создании сертификатов, CRL и подписанных объектов они выгружаются (upload) в точку публикации репозитория, откуда они могут быть загружены для использования в RP.

Этот профиль определяет рекомендуемую схему именования объектов (файлов), рекомендуемое содержимое точек публикации репозиториев (каталогов) и предлагаемую внутреннюю структуру локального кэша репозитория, который предназначен для облегчения синхронизации распределенного набора точек публикации репозиториев и создания пути сертификации.

Сертификат ресурса служит свидетельством привязки открытого ключа элемента к набору блоков адресов IP и номеров AS. Субъект сертификата ресурса может показать, что он является владельцем ресурса, указанного в сертификате, используя свой секретный ключ для создания цифровой подписи (которая может быть проверена с помощью открытого ключа из сертификата).

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].

Ниже приведены определения терминов, используемых в этом документе.

Repository Object (или Object) - объект репозитория
: Конечный объект в точке публикации репозитория. Эти объекты обычно реализуются в виде файлов каталога с публичным доступом, где файлы не является каталогами, хотя иная форма объекта, которая выглядит аналогично файлу, также описывается этим термином.

Repository Publication Point - точка публикации репозитория
: Обозначает набор объектов (Repository Object), опубликованных в общей точке публикации. Обычно это каталог файловой системы с публичным доступом, который указывается идентификатором URI [RFC3986], хотя иная форма локального хранилища, которая выглядит подобно простому каталогу файлов, также описывается этим термином.

Repository Instance - экземпляр репозитория
: Обозначает набор из одной или множества точек публикации репозитория (Repository Publication Point), представляющих единый экземпляр публикации. Обычно это реализуется в форме набора файловых каталогов систем, которые используют общий префикс URI, а каждый каталог идентифицируется своим уникальным URI.

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].

2. Содержимое и структура точки публикации репозитория RPKI

RPKI не требует включения в один экземпляр хранилища всех опубликованных объектов RPKI. Вместо этого система репозиториев RPKI образуется множеством экземпляров хранилищ. Каждый отдельный экземпляр репозитория имеет одну или множество точек публикации. Каждая точка публикации используется одним или множеством элементов, указанных в сертификатах RPKI, как определено в расширении SIA[1].

В этом разделе описана коллекция объектов (сертификаты RPKI, списки CRL, манифесты и подписанные объекты), поддерживаемая в точке публикации репозитория.

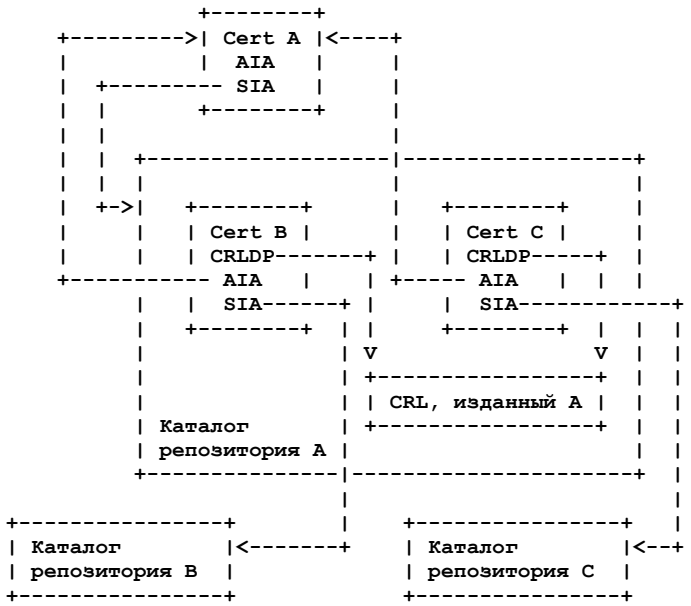

Рисунок 1. Использование расширений AIA и SIA в RPKI.

Для каждого сертификата удостоверяющего центра (УЦ или CA[2]) в RPKI имеется соответствующая точка публикации репозитория, которая является уполномоченной для всех текущих сертификатов и CRL, выпущенных этим CA. Расширение SIA в сертификате содержит идентификатор URI [RFC3986], указывающий точку публикации репозитория

[1]Subject Information Access - доступ к информации субъекта.
[2]Certification Authority - агентство по сертификации.

и механизмы доступа к нему. В дополнение к этому расширение AIA[1] содержит идентификатор URI, указывающий полномочное местоположение сертификата CA, которым был выпущен данный сертификат.

Например, если субъект сертификата A выпустил сертификаты B и C, то расширение AIA сертификатов B и C будет указывать на точку публикации сертификата объекта A, а расширение SIA в сертификате A будет указывать точку публикации (каталог), содержащий сертификаты B и C (см. рисунок 1).

На рисунке 1 сертификаты B и C изданы CA A. Следовательно, расширения AIA в сертификатах B и C будут указывать на (сертификат) A, а расширение SIA в сертификате A - на точку публикации репозитория для продукции CA A, который включает сертификаты B и C, а также CRL выпущенный A. Расширение CRLDP[2] в сертификатах B и C будет указывать на CRL, выпущенные A.

В такой структуре распределенного хранилища точка публикации репозитория CA содержит все опубликованные этим CA сертификаты, а также выпущенные им списки отзыва (CRL). Этот репозиторий включает также все опубликованные объекты с цифровыми подписями, которые проверяются по сертификатам конечных элементов (EE[3]), выпущенных этим CA.

2.1. Манифесты

Каждая точка публикации репозитория **должна** включать манифест [RFC6486], содержащий список имён всех объектов, а также хэш-значение содержимого каждого объекта, опубликованного в настоящий момент CA или EE.

УЦ **может** выполнять множество операций с объектами при публикации репозитория в части изменения его содержимого перед тем, как выпустить единый манифест, который учитывает все операции в области действия этих изменений. Оператору репозитория **следует** реализовать ту или иную форму режима управления доступом к каталогам хранилища, позволяющую не показывать зависимым от него сторонам (RP), которые выполняют информации по извлечению данных из хранилища, промежуточные состояния, которые возникают между изменением репозитория и выпуском соответствующего манифеста[4].

2.2. Точки публикации репозиториев CA

Сертификат CA имеет два элемента accessMethod, заданных в поле SIA. Элемент id-ad-caRepository accessMethod связан с элементом accessLocation, который указывает точку публикации репозитория с сертификатами, выпущенными этим CA, как указано в [RFC6487]. Элемент id-ad-rpkiManifest accessMethod связан с элементом accessLocation, указывающим с помощью URI объекта (а не URI каталога) на объект манифеста, связанного с этим CA.

Репозиторий публикации CA содержит текущие (не просроченные и не отозванные) сертификаты, выпущенные этим CA, наиболее свежий список CRL, выпущенный этим CA, текущий манифест и все прочие подписанные объекты, которые могут быть проверены с использованием сертификата EE [RFC6487] выпущенного этим CA.

Манифест CA содержит имена (файлов) данного набора объектов, а также хэш-значение содержимого каждого объекта за исключением самого манифеста.

Устройство RPKI требует уникальной привязки CA к одной паре ключей. Таким образом, административный орган, являющийся CA, выполняет смену ключей путём генерации нового сертификата CA с новым именем сегмента и новой парой ключей [RFC6489] (смена имени обусловлена тем, что в контексте RPKI имена субъектов во всех выпускаемых CA сертификатах должны быть уникальными, а также тем, что в процедуре смены ключей RPKI создаётся новый экземпляр CA с новым ключом). В таких случаях объекту **следует** продолжать использование прежней точки публикации репозитория для обоих экземпляров CA в процессе смены ключей, обеспечивая в процессе смены ключей сохранение пригодности ссылок на выпущенные этим CA сертификаты, которые указаны в расширении AIA непрямых подчинённых объектов, а также ограничение перевыпуска подчинённых сертификатов только прямыми «подчинёнными» данного CA [RFC6489]. В таких случаях точка публикации репозитория будет содержать CRL, манифест и подчинённые сертификаты для обоих экземпляров CA (для объекта можно использовать разные точки публикации для старого и нового CA, но в таких случаях требуется очень аккуратная координация с подчинёнными CA и EE, чтобы указатели AIA на уровнях иерархии RPKI, не подчинённых данному CA непосредственно, корректно согласовывались с подчинённой продукцией нового CA.)

Ниже приведены рекомендации по именованию объектов в точке публикации репозитория CA.

CRL

Когда CA выпускает новый список CRL, он заменяет им прежний CRL (выпущенный с той же парой ключей CA) в точке публикации репозитория. CA недопустимо сохранять прежние CRL в точке публикации. Таким образом, они **должны** заменять (переписывать) прежние CRL, подписанный тем же (экземпляром) CA. Ненормативные рекомендации по именованию таких объектов предлагают выбирать имена файлов для CRL в репозитории на основе открытого ключа CA. Один из таких методов создания имени CRL описан в параграфе 2.1 [RFC4387] - 160 битов хэш-значения открытого ключа CA преобразуются в строку из 27 символов с использованием модифицированного кодирования Base64, как описано в разделе 5 (таблица 2) [RFC4648]. Для файла **должно** использоваться расширение имени .crl, обозначающее CRL. Каждый файл .crl содержит один CRL в формате DER.

Манифест

При публикации нового экземпляра манифеста он **должен** заменять собой предыдущий экземпляр во избежание путаницы. CA **недопустимо** сохранять прежние манифесты в точке публикации репозитория. Ненормативные рекомендации по именованию таких объектов предлагают выбирать имена файлов для манифестов в репозитории на основе открытого ключа CA, аналогично описанному выше алгоритму для CRL. Файлы **должны** иметь расширение .mft, указывающее, что объект является манифестом.

---

[1] Authority Information Access - доступ к информации УЦ (агентства).
[2] CRL Distribution Points - тоски распространения CRL.
[3] End-entity.
[4] Отмечено, что при отсутствии такого режима доступа RP **могут** быть показаны промежуточные состояния, в которых содержимое репозитория не отражено точно в манифесте. Конкретные случая такого рассогласования и действия в таких ситуациях рассмотрены в [RFC6486].

Сертификаты

В RPKI орган сертификации CA **может** выпускать серии сертификатов для одного имени субъекта с одним открытым ключом и одним и тем же набором ресурсов. Однако зависимым от инфраструктуры сторонам нужен доступ лишь к последнему сертификату такой серии. Поэтому для сертификатов таких серий **следует** применять одно имя файла. Это приводит к тому, что каждый новый сертификат в серии будет записываться вместо его предшественника. Можно использовать разные имена, но это осложнит проверку для пользователей. Ненормативные рекомендации по именованию сертификатов предлагают реализовать (локальное) правило, требующее от субъекта использовать уникальную пару ключей для каждой уникальной серии сертификатов, выпущенных для него. Это позволяет CA использовать схему именования на основе открытого ключа субъекта, как это описано выше для имён файлов CRL. Опубликованные сертификаты **должны** использовать расширение .cer, показывающее, что объект является сертификатом. Каждый файл .cer содержит один сертификат в формате DER.

Подписанные объекты

Подписанные объекты RPKI [RFC6488] публикуются в точке публикации репозитория, указываемой SIA в сертификате CA, который выпустил сертификат EE, используемый для проверки подписи этого объекта (напрямую указана SIA в сертификате EE). Ненормативные рекомендации по именованию подписанных объектов предлагают создавать имена на основе открытого ключа соответствующего сертификата EE, применяя описанный выше алгоритм. Для опубликованных подписанных объектов RPKI **недопустимо** использовать расширения имён файлов .crl, .mft, .cer.

На момент публикации этого документа была определена одна форма подписанного объекта ROA[1] [RFC6482]. Опубликованные ROA **должны** иметь расширение имени файлов .roa, указывающие, что объект является ROA.

3. Вопросы публикации сертификатов ресурсов

Каждый эмитент **может** публиковать выпущенные им сертификаты и CRL в любом репозитории. Однако существует множество ограничений, которые диктуют выбор подходящей структуры репозитория.

- Репозиторий **следует** размещать на доступном сервисе с высокопроизводительной платформой.

- Репозиторий **должен** быть доступен с помощью rsync [RFC5781] [RSYNC]. Поддержка других механизмов возможна по выбору оператора. Поддерживаемые механизмы **должны** быть согласованы с элементом accessMethod, указанным в SIA соответствующих сертификатов CA и EE.

- В каждой точке публикации репозитория CA **следует** размещать продукцию этого CA, включая те объекты, которые могут быть проверены по сертификатам EE, выпущенным этим CA. Подписанная продукция связанных CA той же организации (объекта) **может** размещаться в той же точке публикации репозитория CA. Непосредственно в точке публикации репозитория **не следует** размещать объектов, отличных от каталогов.

  Каждому из таких каталогов **следует** быть точкой публикации сертификата CA или EE, содержащегося в каталоге CA. Эти соображения применимы также к каталогам следующего уровня внутри этих каталогов. Наличие содержимого, не являющегося продукцией CA, может создать путаницу для RP, которым в таких случаях следует соблюдать осторожность, чтобы не счесть годную продукцию CA неприемлемой для использования.

- Подписанные объекты размещаются в месте, указанном полем SIA в сертификате EE, используемом для проверки подписи каждого объекта. Подписанные объекты размещаются в точке публикации репозитория сертификата CA, выпустившего сертификат EE. Расширение SIA в сертификате EE указывает сам объект, а не каталог в точке публикации репозитория [RFC6487].

- В параграфе 2.1 сказано, что операторам репозитория **следует** реализовать ту или иную форму управления каталогами в репозитории, чтобы гарантировать, что RP, выполняющие операции поиска в репозитории, не получали промежуточных состояний при внесении изменений в репозиторий и связанные с ним манифесты. Несмотря на следующий комментарий, RP **не следует** полагаться на соответствие манифеста содержимому репозитория и **следует** подобающим образом организовать свои операции поиска (см. раздел 5).

  Способ организации оператором режима обновления каталога, снижающий риск несоответствия между манифестом и содержимым обновляемого каталога, зависит от рабочих параметров файловой системы репозитория, поэтому приведённые ниже рекомендации не могут служить нормативным руководством.

  Наиболее часто используемым способом предотвращения несоответствия при обновлении больших каталогов является «пакетная» обработка, когда готовится пакет изменений содержимого каталога, создаётся рабочая копия содержимого каталога и к ней применяется пакет изменений. После завершения операции изменяется символьная ссылка в файловой системе. Содержимое старого каталога может быть удалено по истечении некоторого времени. Однако следует отметить, что результат применения этого метода в плане обеспечения целостности клиентских операций синхронизации зависит от взаимодействия поддерживаемого механизма доступа с локальной файловой системой репозитория. Существует вероятность того, что RP увидит некоторое несоответствие между манифестом и содержимым каталога. Поскольку хранилище может находиться в состоянии частичного обновления, невозможно дать гарантию наличия постоянной согласованности.

4. Повторный выпуск сертификатов и репозитории

Если сертификат CA выпускается заново (например, в результате изменения набора ресурсов, содержащегося во множестве расширений), не требуется заново издавать все сертификаты, выпущенные с использованием заменяемого сертификата. Поскольку эти сертификаты включают расширения AIA, которые указывают на точку публикации для сертификата CA, сертифицирующему органу (CA) **следует** использовать для своей точки публикации имя, которое сохраняется после смены сертификата. Т. е. в новых сертификатах CA **следует** использовать ту же точку публикации, что и в прежних сертификатах CA с тем же именем субъекта и открытым ключом субъекта, а новый сертификат при повторном выпуске **следует** просто записывать взамен старого в той же точке публикации.

В параграфе 2.2 отмечено, что при смена ключей CA **следует** использовать для точки публикации имя, которое сохраняется после этой замены. В таких случаях точка публикации репозитория будет содержать CRL и манифесты

[1] Route Origination Authorization - полномочия по созданию маршрута.

обоих экземпляров CA в течение процедуры смены ключей. Процедура смены ключей в RPKI [RFC6489] требует, чтобы подчинённая продукция старого CA переписывалась в общей точке публикации репозитория подчинённой продукцией нового CA.

5. Синхронизация репозитория с локальным кэшем

Можно выполнить связанную с проверкой пригодности задачу создания пути сертификации путём получения отдельных сертификатов и списков отзыва на основе поиска отдельных сертификатов, наборов возможных сертификатов и списков отзыва по значениям полей AIA, SIA и CRLDP в сертификатах. Такой вариант **не** рекомендуется в тех случаях, значимость скорости и эффективности близки.

Для эффективной проверки пригодности сертификатов, CRL и подписанных объектов RPKI каждой зависимой от инфраструктуры стороне рекомендуется поддерживать локальной хранилище с синхронизированными копиями действующих сертификатов, списков отзыва и всех связанных с ними подписанных объектов.

Общей моделью синхронизации репозитория является проход «сверху-вниз» по распределенной структуре. Процесс начинается с локального набора доверенных привязок, соответствующего локальному выбору привязок TA, которые могут использоваться для загрузки начального набора самоподписанных сертификатов ресурсов, формирующего «затравку» процесса [RFC6490]. Далее локальный кэш заполняется всеми действительными сертификатами, которые были выпущены найденными эмитентами. Эта процедура может рекурсивно повторяться для каждого из этих подчинённых сертификатов. Для такого процесса прохождения через репозиторий **следует** задавать локальное ограничение максимальной длины цепочки от начальных доверенных привязок. Если этого не сделать, может образоваться петля указателей SIA или возникнуть иные вырожденные формы логической иерархии RPKI, что будет приводить к невозможности RP выполнить синхронизацию репозитория с локальным кэшем RPKI.

При локальной синхронизации RP **следует** применять полученные манифесты [RFC6486], чтобы обеспечить синхронизацию с текущим, согласованным состоянием точки публикации репозитория. В разделе 3 отмечено, что при обновлении точки публикации оператор репозитория не может гарантировать RP, что манифест постоянно согласовано с содержимым репозитория. RP **следует** применять алгоритмы извлечения данных из репозитория, принимающие во внимание возможность несоответствия. Возможные для RP алгоритмы включают двухкратную синхронизацию или извлечение манифеста перед синхронизацией и после неё с повтором синхронизации при обнаружении различий в манифестах.

6. Вопросы безопасности

Целостность хранилищ баз данных не предполагается защищённой и операции извлечения данных из репозитория могут быть уязвимы для разных форм MITM-атак[1]. Повреждение извлекаемых объектов обнаруживается зависимыми сторонами путём проверки подписей, связанных с каждым объектом. Подмена новых экземпляров объектов более старыми обнаруживается с помощью манифестов. Добавление отозванных, удалённых сертификатов обнаруживается путём получения и обработки CRL в периодическом режиме. Однако даже при использовании манифестов и CRL зависимая сторона может не обнаружить некоторые варианты атак с подменой на основе старых (но с неистекшим сроком действия) объектов .

Конфиденциальность репозиториев и опубликованных в них объектов не обеспечивается. Данные с ограниченным доступом не следует включать в подписанные объекты, если не применяется тех или иных механизмов защиты конфиденциальности данных для этих объектов.

7. Взаимодействие с IANA

7.1. Типы сред

Агентство IANA зарегистрировало два новых типа (media type):

```
application/rpki-manifest
application/rpki-roa
```

Данный документ также использует расширения имён файлов .cer и .crl file для типов application/pkix-cert и application/pkix-crl, определённых в [RFC2585].

7.1.1. application/rpki-manifest

```
MIME media type name:  application
MIME subtype name:  rpki-manifest
Required parameters:  None
Optional parameters:  None
Encoding considerations:  binary
Security considerations:  Carries an RPKI Manifest [RFC6486]
Interoperability considerations:  None
Published specification:  This document
Applications that use this media type:  Any MIME-complaint transport
Additional information:
   Magic number(s):  None
   File extension(s):  .mft
   Macintosh File Type Code(s):
Person & email address to contact for further information:
   Geoff Huston <gih@apnic.net>
Intended usage:  COMMON
Author/Change controller:  Geoff Huston <gih@apnic.net>
```

7.1.2. application/rpki-roa

```
MIME media type name:  application
MIME subtype name:  rpki-roa
```

[1]Man-in-the-middle - атака по пути передачи с участием человека.

```
   Required parameters:  None
   Optional parameters:  None
   Encoding considerations:  binary
   Security considerations:  Carries an RPKI ROA [RFC6482]
   Interoperability considerations:  None
   Published specification:  This document
   Applications that use this media type:  Any MIME-complaint transport
   Additional information:
      Magic number(s):  None
      File extension(s):  .roa
      Macintosh File Type Code(s):
   Person & email address to contact for further information:
      Geoff Huston <gih@apnic.net>
   Intended usage:  COMMON
   Author/Change controller:  Geoff Huston <gih@apnic.net>
```

7.2. Реестр RPKI Repository Name Scheme

Агентство IANA создало реестр RPKI Repository Name Scheme, содержащий трёхсимвольные расширения имён файлов для объектов репозитория RPKI. Содержимое реестра поддерживается на основе процедуры IETF Review [RFC5226]. Начальное состояние реестра отражено в таблице.

Расширение имени	*Объект RPKI*	*Документ*
`.cer`	Сертификат	[RFC6481]
`.crl`	Список отзыва сертификатов	[RFC6481]
`.mft`	Манифест	[RFC6481]
`.roa`	Полномочия по созданию маршрутов	[RFC6481]

8. Благодарности

Этот документ много выиграл от полезных комментариев и предложений Stephen Kent, Matt Lepenski, Michael Elkins, Russ Housley и Sean Turner.

9. Литература

9.1. Нормативные документы

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

[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 (RPKI)", 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 (RPKI)", RFC 6488, February 2012.

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

9.2. Дополнительная литература

[RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

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

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4387] Gutmann, P., Ed., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP", RFC 4387, February 2006.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[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.

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

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

Адреса авторов

Geoff Huston

APNIC

EMail: gih@apnic.net

URI: http://www.apnic.net

Robert Loomans

APNIC

EMail: robertl@apnic.net

URI: http://www.apnic.net

George Michaelson

APNIC

EMail: ggm@apnic.net

URI: http://www.apnic.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru