Internet Engineering Task Force (IETF)
Request for Comments: 6487
Category: Standards Track
ISSN: 2070-1721

G. Huston
G. Michaelson
R. Loomans
APNIC

February 2012

Профиль для сертификатов ресурсов X.509 PKIX

A Profile for X.509 PKIX Resource Certificates

Аннотация

Этот документ определяет стандартный профиль сертификатов X.509, используемых для проверки заявлений о «праве использования» (right-of-use) ресурсов INR[1]. Сертификаты, выпускаемые с этим профилем, служат для передачи от эмитента подтверждения владения полномочиями на использование INR, описанных в сертификате. Этот документ содержит нормативную спецификацию синтаксиса сертификатов и списков отзыва (CRL[2]) в инфраструктуре открытых ключей ресурсов (RPKI[3]). Документ также задаёт профили для формата запросов сертификатов и процедуру проверки сертификатов пути Relying Party RPKI.

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[4] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[5]. 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/rfc6487.

Оглавление

[1]Internet Number Resource - числовой ресурс (номер) Internet.
[2]Certificate Revocation List.
[3]Resource Public Key Infrastructure.
[4]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[5]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Этот документ определяет стандартный профиль сертификатов X.509, используемых для проверки заявлений о «праве использования» (right-of-use) ресурсов INR, т. е. адресов IP и номеров автономных систем (AS[1]). Такие сертификаты называют «сертификатами ресурсов» (resource certificate). Сертификатами ресурсов являются сертификаты, соответствующие профилю PKIX [RFC5280], а также ограничениям, заданным в этом профиле. Сертификат ресурса свидетельствует о том, эмитент предоставил субъекту «право использования» перечисленного множества адресов IP и/или номеров AS.

Этот документ ссылается на раздел 7 документа «Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)» [RFC6484]. Это неотъемлемая часть политики и нормативная спецификация для синтаксиса сертификатов и списков отзыва (CRL), используемых в RPKI. Документ также задаёт профили для формата запросов сертификатов и процедуры проверки пригодности пути сертификации зависимыми сторонами (RP[2]) RPKI.

Сертификаты ресурсов будут применяться в соответствии с политикой сертификации RPKI (CP[3]) [RFC6484]. Они выпускаются организациями, которые назначают и/или выделяют значения INR, и, таким образом RPKI согласуется в функцией распределения INR общего пользования. При выделении или присваивании INR регистратором некому объекту это выделение может быть описано связанным с ним сертификатом ресурса. Этот сертификат выпускается регистратором и ключ сертификата субъекта привязывается к INR, указанным в сертификате. Одно или два нормативных расширения (IP Address Delegation или AS Identifier Delegation Extensions [RFC3779]) перечисляют значения INR, выделенные или назначенные этому субъекту эмитентом.

Проверка пригодности сертификата ресурса в RP выполняется в соответствии с описанием в параграфе 7.1. Эта процедура отличается от описанной в разделе 6 [RFC5280]:

- требуется дополнительная обработка связанная с расширениями INR;
- требуется подтверждение соответствия открытого ключа между эмитентами CRL и сертификата ресурса;
- требуется соответствие сертификата ресурса данному профилю.

Этот профиль определяет поля сертификата ресурса, которые **должны** присутствовать, чтобы сертификат считался пригодным. Любые расширения, не указанные явно, **должны** отсутствовать. Такие же правила применяются для CRL, используемых в RPKI, которые тоже «профилируются» данным документом. Удостоверяющие центры (CA[4]), выполняющие правила RPKI CP, **должны** выпускать сертификаты и CRL, соответствующие данному профилю.

1.1. Терминология

Предполагается знакомство читателя с концепциями и терминами, 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].

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. Описание ресурсов в сертификатах

Схема для описания связи между субъектом сертификата и INR, контролируемым в настоящее время этим субъектом, приведена в [RFC3779]. Данный профиль вносит дополнительные требования:

- каждый сертификат ресурса **должен** содержать расширение IP Address Delegation или Autonomous System Identifier Delegation (возможно, оба);
- эти расширения **должны** быть помечены как критические;

[1]Autonomous System.
[2]Relying party.
[3]Certificate Policy.
[4]Certification Authority - агентство по выдаче сертификатов.

- для поля расширения **должен** использоваться канонический формат описания INR с сортировкой, максимально охватываемым диапазоном и максимальной маской префикса в соответствии с определением [RFC3779] (за исключением случаев использования конструкции inherit).

При проверке пригодности сертификата ресурса RP **должны** убедиться в том, что INR, описанные в сертификате эмитента сертификата ресурса, охватывают INR с проверяемом сертификате ресурса. В этом контексте термин «охватывает» включает и случай совпадения INR в проверяемом сертификате и сертификате эмитента.

3. Сертификаты конечных элементов и функции подписи в RPKI

Как отмечено в [RFC6480], основным назначением сертификатов конечных элементов (EE[1]) в RPKI является проверка пригодности подписанных объектов, относящихся к использованию INR, описанных в сертификате (например, ROA[2] и манифестов).

Секретный ключ, связанный с EE, используется для подписывания одного объекта RPKI (т. е. сертификат EE используется для проверки пригодности единственного объекта). Сертификат EE встраивается в объект как часть структуры CMS signed-data [RFC6488]. Поскольку имеется взаимно однозначное соответствие между сертификатом EE и подписанным объектом, отзыв сертификаты фактически отзывает подписанный объект.

Сертификат EE может использоваться для проверки пригодности последовательности подписанных объектов, где каждый подписанный объект переписывает предыдущий экземпляр подписанного объекта в репозитории точки публикации так, что публикуется только один экземпляр подписанного объекта в любой момент времени (например, сертификат EE **может** быть использован для подписывания последовательности манифестов [RFC6486]). Такие сертификаты EE называют сертификатами «последовательного использования» (sequential use).

Сертификаты EE, используемые для проверки пригодности единственного экземпляра подписанного объекта и не применяемые в дальнейшем или в другом контексте, называют одноразовыми сертификатами (one-time-use).

4. Сертификаты ресурсов

Сертификат ресурса является пригодным к применению сертификатом открытого ключа X.509, совместимым с профилем PKIX [RFC5280] и содержащим поля, перечисленные в этом разделе. Отличия от [RFC5280] отмечены ниже.

Если конкретное поле явно не указано в качестве **необязательного** (OPTIONAL), все перечисленные здесь поля **должны** присутствовать в сертификате, а наличие каких-либо иных полей в соответствующих спецификации сертификатах **недопустимо**. Если здесь задано значение поля, это значение **должно** использоваться в соответствующих спецификации сертификатах.

4.1. Версия

Поскольку сертификаты ресурсов являются сертификатами X.509 версии 3, поле version **должно** указывать версию 3 (т. е. поле **должно** иметь значение 2).

RP должны отказываться от обработки сертификатов версий 1 или 2 (в отличие от [RFC5280]).

4.2. Порядковый номер

Порядковый номер сертификата задаётся положительным целым числом, которое является уникальным в рамках данного CA.

4.3. Алгоритм подписи

Алгоритм, используемый в этом профиле, задан в [RFC6485].

4.4. Эмитент

В этом поле указывается пригодное к использованию отличительное имя X.501.

Имя эмитента **должно** содержать один экземпляр атрибута CommonName и **может** также включать один экземпляр атрибута serialNumber. При наличии обоих атрибутов **рекомендуется** представлять их в форме множества (set). Атрибут CommonName **должен** кодироваться с использованием типа ASN.1 PrintableString [X.680]. Имя эмитента не предназначено описывать отождествление эмитента.

В RPKI не предполагается уникальность имён эмитентов в глобальном масштабе (по соображениям безопасности). Однако **рекомендуется** выбирать имена эмитентов так, чтобы минимизировать вероятность конфликтов (совпадений). В разделе 8 рассмотрены (ненормативные) механизмы генерации имён в соответствии с приведённой выше рекомендацией.

4.5. Субъект

Значением этого поля является пригодное для использования отличительное имя X.501 [RFC4514], для которого действуют ограничения, указанные для имени эмитента.

В RPKI имя субъекта определяется эмитентом, а не предлагается субъектом [RFC6481]. Каждый различающийся подчинённый CA и EE, сертифицируемые данным эмитентом, **должны** идентифицироваться с использованием имени субъекта, которое уникально в рамках эмитента. В этом контексте «различающийся» определяется, как элемент и данный открытый ключ. Эмитентам **следует** использовать другое имя субъекта, если ключевая пара для него меняется (т. е. когда CA выпускает сертификат в процессе замены ключа субъекта). Имя субъекта не предназначено описывать отождествление этого субъекта.

[1] End-entity.
[2] Route Origin Authorization - полномочия на порождение маршрута.

4.6. Срок действия

Срок действия субъекта представляется последовательностью (SEQUENCE) двух дат - начала (notBefore) и завершения (notAfter) срока действия сертификата.

Хотя CA обычно предостерегают от выпуска сертификатов со сроком действия, превышающим срок действия сертификата CA, который будет применяться для проверки пригодности выпущенного сертификата, у CA **могут** быть достаточные основания выпускать сертификаты подчинённых объектов со сроком действия, превышающим срок действия сертификата самого CA.

4.6.1. notBefore

В качестве значения notBefore **следует** указывать время не раньше момента создания сертификата.

В RPKI допускается указывать в этом поле значение, предшествующее значению одноимённого поля в любом «вышестоящем» сертификате. RP **не следует** предполагать, что этот сертификат действовал в прошлом или будет пригоден в будущем, поскольку область действия проверки пригодности в RP относится лишь к пригодности сертификата в момент проверки.

4.6.2. notAfter

Поле notAfter задаёт предполагаемый срок действия текущего выделения ресурса или соглашения о назначении между эмитентом и субъектом.

Сертификат может содержать в этом поле значение после времени, указанного одноимённым полей в каком-либо вышестоящем сертификате. Для RP действуют такие же, как отмечено выше, предостережения относительно пригодности сертификата в прошлом или будущем.

4.7. Информация об открытом ключе субъекта

Используемый в этом профиле алгоритм указан в [RFC6485].

4.8. Расширения сертификатов ресурса

Описанные ниже расширения X.509 v3 **должны** присутствовать в соответствующих этой спецификации сертификатах ресурсов, если явно не указано иное. Использующая сертификаты система **должна** отвергать сертификаты с неопознанным критическим расширением, не опознанные некритические расширения **можно** игнорировать [RFC5280].

4.8.1. Базовые ограничения

Поле расширения Basic Constraints является критическим в данном профиле и **должно** присутствовать в сертификатах, где субъектом является CA. В сертификатах других субъектов это расширение **недопустимо**.

Установка логического значения cA определяется эмитентом сертификата.

Поле Path Length Constraint не задано для сертификатов RPKI и его присутствие **недопустимо**.

4.8.2. Идентификатор ключа субъекта

Это расширение **должно** присутствовать во всех сертификатах ресурсов. Расширение не является критическим.

Key Identifier в сертификатах ресурсов представляет собой 160-битовых хэш SHA-1 для DER-представления ASN.1 битовой строки Subject Public Key, как описано в параграфе 4.2.1.2 [RFC5280].

4.8.3. Идентификатор ключа УЦ

Это расширение **должно** присутствовать во всех сертификатах ресурсов, за исключением CA, выпускающих «самоподписанные» (self-signed) сертификаты. При подписывании своих (self-signed) сертификатов CA **может** включить это расширение и установить для него значение, эквивалентное Subject Key Identifier. Включение полей authorityCertIssuer и authorityCertSerialNumber **недопустимо**. Расширение не является критическим.

Key Identifier в сертификатах ресурсов представляет собой 160-битовых хэш SHA-1 для DER-представления ASN.1 битовой строки открытого ключа эмитента, как описано в параграфе 4.2.1.1 [RFC5280].

4.8.4. Применение ключа

Это расширение является критическим и **должно** присутствовать.

В сертификатах, выпускаемых только для УЦ, биты keyCertSign и CRLSign устанавливаются (TRUE), а прочие биты **должны** отличаться от TRUE.

В сертификатах EE бит digitalSignature **должен** быть установлен (TRUE) и это **должен** быть единственный бит со значением TRUE.

4.8.5. Расширенное применение ключа

Расширение EKU[1] **недопустимо** включать в сертификаты CA в RPKI. Это расширение **недопустимо** также включать в сертификаты EE, используемые для проверки пригодности объектов RPKI (например, ROA или манифестов). Расширение **недопустимо** указывать критическим.

Расширение EKU **может** присутствовать в сертификатах EE, выпущенных для маршрутизаторов и других устройств. Разрешённые значения идентификаторов EKU OID будут заданы в документах Standards Track RFC, выпускаемых другими рабочими группами IETF, которые принимают профиль RPKI и указывают требования конкретных приложений, связанные с использованием таких EKU.

[1] Extended Key Usage - расширенное использование ключа.

4.8.6. Точки распространения CRL

Это расширение **должно** присутствовать (за исключением самоподписанных сертификатов) и является некритическим. В самоподписанных сертификатах это расширение **должно** опускаться.

В этом профиле область действия CRL включает все сертификаты, выпущенные данным CA.

Расширение CRLDP[1] указывает места размещения CRL, связанных с выпущенными эмитентом сертификатами. RPKI использует для идентификации объекта форму URI [RFC3986]. Предпочтительным механизмом доступа к URI является одиночный идентификатор rsync URI ("rsync://") [RFC5781], который указывает единый (включительный) CRL для каждого эмитента.

В этом профиле издатель сертификатов является также эмитентом CRL, поэтому поле CRLIssuer **должно** опускаться, а поле distributionPoint **должно** присутствовать. Поле Reasons **должно** опускаться.

В distributionPoint **должно** включаться поле fullName, а включение поля nameRelativeToCRLIssuer **недопустимо**. Поле generalName **должно** иметь тип URI.

Последовательность значений distributionPoint **должна** включать единственное поле DistributionPoint, которое **может** содержать более одного значения URI. Идентификатор rsync URI [RFC5781] **должен** присутствовать в DistributionPoint и **должен** указывать самый «свежий» экземпляр CRL данного эмитента. Другие формы URI **могут** использоваться в дополнение к rsync URI, представляя дополнительные механизмы доступа к этому CRL.

4.8.7. Доступ к информации об УЦ

В контексте RPKI это расширение указывает точку публикации сертификата эмитента, выпустившего сертификат, в котором присутствует это расширение. Для этого профиля в сертификатах **должна** указываться единственная точка публикации непосредственного «вышестоящего» сертификата. Исключением являются самоподписанные сертификаты, в которых это расширение **должно** опускаться. Расширение является некритическим.

Данный профиль использует для идентификации объектов форму URI. Предпочтительным механизмом доступа к URI является rsync и идентификатор rsync URI [RFC5781] **должен** задаваться с accessMethod = id-ad-caIssuers. Значение URI **должно** указывать точку публикации сертификата, в котором эмитент (Issuer) является субъектом (непосредственный «вышестоящий» сертификат для эмитента). Другие accessMethod URI, указывающие на этот же объект, могут включаться в последовательность значений данного расширения.

CA **должен** использовать постоянную схему URL для выпускаемых им сертификатов CA [RFC6481]. Это предполагает замену вновь выпущенным сертификатом ранее имевшейся версии сертификата (для того же объекта) в репозитории. Таким образом, сертификаты, «подчинённые» выпущенному заново сертификату (CA), могут поддерживать постоянный указатель на расширение AIA[2] и, следовательно, их не требуется выпускать заново при смене сертификата.

4.8.8. Доступ к информации о субъекте

В контексте RPKI расширение SIA[3] указывает точку публикации продукции, подписанной субъектом сертификата.

4.8.8.1. SIA для сертификатов CA

Это расширение **должно** присутствовать и **должно** помечаться как некритическое.

Это расширение **должно** использовать accessMethod = id-ad-caRepository с accessLocation в форме URI, который **должен** указывать rsync URI [RFC5781]. Этот идентификатор URI указывает на каталог, содержащий все опубликованные материалы, выпущенные данным CA, т. е. все пригодные сертификаты CA, опубликованные сертификаты EE, текущий список CRL, манифест и подписанные объекты, пригодность которых была проверена с использованием сертификатов EE, выпущенных данным CA [RFC6481]. **Могут** присутствовать другие элементы accessDescription с accessMethod = id-ad-caRepository. В таких случаях значения accessLocation описывают поддерживаемые URI дополнительных механизмов доступа к тому же каталогу. Порядок URI в этой последовательности accessDescription отражает относительные предпочтения CA в части методов доступа, которые могут использоваться RP (первый элемент является наиболее предпочтительным для CA).

Это расширение **должно** иметь экземпляр AccessDescription с accessMethod = id-ad-rpkiManifest,

```
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }
id-ad-rpkiManifest OBJECT IDENTIFIER ::= { id-ad 10 }
```

и формой rsync URI [RFC5781] для accessLocation. Идентификатор URI указывает на манифест CA для опубликованных объектов [RFC6486] как URL объекта. **Могут** существовать другие элементы accessDescription для id-ad-rpkiManifest accessMethod, где значение accessLocation указывает дополнительные механизмы доступа к тому же манифесту.

4.8.8.2. SIA для сертификатов EE

Это расширение **должно** присутствовать и **должно** помечаться как некритическое.

Это расширение **должно** иметь экземпляр accessMethod = id-ad-signedObject,

```
id-ad-signedObject OBJECT IDENTIFIER ::= { id-ad 11 }
```

с accessLocation в форме URI, который **должен** включать rsync URI [RFC5781]. Этот идентификатор URI указывает на подписанный объект, пригодность которого проверена с использованием сертификата EE [RFC6481]. Могут существовать другие элементы accessDescription для id-ad-signedObject accessMethod, где значение accessLocation указывает URI дополнительного механизма доступа к тому же объекту с упорядочением по относительным предпочтениям EE в части выбора механизмов доступа.

Другие accessMethod **недопустимо** использовать для SIA сертификатов EE.

---

[1] CRL Distribution Points - точки распространения списков отзыва.
[2] Authority Information Access - доступ к информации об УЦ.
[3] Subject Information Access - доступ к информации о субъекте.

4.8.9. Политика сертификации

Это расширение **должно** присутствовать и **должно** помечаться как критическое. Расширение **должно** включать в точности одно правило, как указано в RPKI CP [RFC6484]

4.8.10. Ресурсы IP

Одно или оба расширения IP Resources и AS Resources **должны** присутствовать во всех сертификатах RPKI. Включённое расширение **должно** быть помечено как критическое.

Это расширение содержит список адресных ресурсов IP [RFC3779]. Значение может указывать наследуемый (inherit) элемент для конкретного значения AFI[1]. В контексте сертификатов ресурсов, описывающих числовые ресурсы для использования в публичной сети Internet, **недопустимо** использование значение SAFI[2].

Это расширение **должно** задавать непустое множество адресных записей IP или использовать значение inherit для индикации того, что набор адресов IP для этого сертификата наследуется от эмитента сертификата.

4.8.11. Ресурсы AS

Одно или оба расширения IP Resources и AS Resources **должны** присутствовать во всех сертификатах RPKI. Включённое расширение **должно** быть помечено как критическое.

Это расширение содержит список номеров AS [RFC3779] или может задавать наследуемый элемент. Идентификаторы RDI3 не поддерживаются этим профилем и использование их недопустимо.

Это расширение **должно** задавать непустое множество номеров AS или использовать значение inherit для индикации того, что набор номеров AS для этого сертификата наследуется от эмитента сертификата.

5. Списки отозванных сертификатов ресурсов

Каждый CA **должен** выпускать CRL версии 2, соответствующие [RFC5280]. От RP **не** требуется обрабатывать CRL версии 1 (в отличие от [RFC5280]). Эмитентом CRL является CA. В CRL, соответствующие данному профилю, **недопустимо** включать непрямые ((Indirect) или инкрементные (Delta) CRL. Областью действия каждого CRL **должны** быть все сертификаты, выпущенные данным CA.

Имя эмитента указывается в соответствии с параграфом 4.4.

При наличии более одного CRL, выпущенного одним CA, список CRL с наибольшим значением CRL Number заменяет собой все прочие CRL, выпущенные этим CA.

Алгоритм, используемый в CRL, выпускаемых в соответствии с данным профилем, описан в [RFC6485].

Содержимое CRL представляет собой список сертификатов с незавершённым сроком действия, которые были отозваны CA.

RPKI CA **должны** включать два расширения - Authority Key Identifier и CRL Number - в каждый выпускаемый список CRL. RP **должны** быть готовы обрабатывать CRL с этими расширениями. Другие расширения CRL не разрешаются. Каждое из упомянутых выше расширений **недопустимо** включать более одного раза[3].

Для каждого отозванного сертификата ресурсов **должны** присутствовать только поле Serial Number и Revocation Date, использование других полей **недопустимо**. В этом профиле не поддерживаются расширения CRL и включение таких расширений **недопустимо**.

6. Запросы сертификата ресурса

Для запроса сертификата **может** использоваться формат PKCS#10 или CRMF[4]. CA **должны** поддерживать выпуск сертификатов по запросам PKCS#10 и **могут** поддерживать запросы CRMF.

Отметим, что для этого профиля не определяется отклик на запрос сертификата. Для запросов сертификатов CA удостоверяющий центр (CA) помещает сертификат ресурса в репозиторий, как указано в [RFC6484]. Для запроса сертификатов EE отклик не определён.

6.1. Профиль PCKS#10

Этот профиль уточняет спецификацию [RFC2986] в части сертификатов ресурсов. Объект Certificate Request Message, отформатированный в соответствии с PKCS#10, передаётся CA в качестве первого шага по выпуску сертификата.

CA при выпуске сертификата может изменить любое поле запроса за исключением SubjectPublicKeyinfo и запроса расширения SIA.

6.1.1. Поля шаблона запроса сертификата ресурса PKCS#10

Этот профиль задаёт дополнительные требования к полям, которые **могут** присутствовать в CertificationRequestInfo.

Version

Это поле является обязательным и **должно** иметь значение 0.

Subject

Это поле **может** быть опущено. При наличии этого поля его **следует** оставить пустым (т. е. NULL) и в этом случае CA **должен** самостоятельно создать имя субъекта, уникальное в контексте сертификатов, выпущенных данным CA. Поле может быть непустым только в запросах на смену ключей или переиздание сертификата и лишь в том

[1] Address Family Identifier - идентификатор семейства адресов.
[2] Subsequent AFI.
[3] В оригинале это предложение отсутствует, см. https://www.rfc-editor.org/errata/eid3205. *Прим. перев.*
[4] Certificate Request Message Format - формат сообщения с запросом сертификата.

случае, когда CA поддерживает политику (в своём заявлении CPS1), которая позволяет в таких обстоятельствах повторно использовать имена.

SubjectPublicKeyInfo

Это поле задаёт открытый ключ субъекта и алгоритм, который используется с этим ключом. Используемый данным профилем алгоритм задан в [RFC6485].

Attributes

[RFC2986] определяет поле атрибутов, как пары «ключ-значение», где ключом служит идентификатор объекта (OID), а структура значения определяется этим ключом.

Единственным атрибутом в этом профиле является атрибут extensionRequest, определённый в [RFC2985]. Этот атрибут содержит расширения сертификата. Профиль для расширения в запросах сертификатов указан в параграфе 6.3.

Этот профиль задаёт дополнительное ограничение на поля, которые **могут** присутствовать в объекте CertificationRequest:

signatureAlgorithm

Значение signatureAlgorithm задано в [RFC6485].

6.2. Профиль CRMF

Этот профиль уточняет спецификацию CRMF [RFC4211] в части сертификатов ресурсов. Объект Certificate Request Message в формате CRMF передаётся CA в качестве первого шага по выпуску сертификата.

CA при выпуске сертификата может изменить любое поле запроса за исключением SubjectPublicKeyinfo и запроса расширения SIA.

6.2.1. Поля шаблона запроса сертификата CRMF

Этот профиль определяет приведённые ниже дополнительные ограничения на поля, которые могут включаться в Certificate Request Template.

version

Это поле **следует** опускать. При наличии этого поля оно **должно** указывать запрос сертификата версии 3.

serialNumber

Это поле **должно** быть опущено.

signingAlgorithm

Это поле **должно** быть опущено.

issuer

Это поле **должно** быть опущено в данном профиле.

Validity

Это поле **может** быть опущено и в таком случае CA будет выпускать сертификат со сроком действия, определяемым по своему усмотрению. При заданном в запросе сроке действия CA **может** заменить запрошенные значения по своему усмотрению.

Subject

Это поле **следует** оставлять пустым (т. е. NULL) и в этом случае CA **должен** самостоятельно создать имя субъекта, уникальное в контексте сертификатов, выпущенных данным CA. Поле может быть непустым только в запросах на смену ключей или переиздание сертификата и лишь в том случае, когда CA поддерживает политику (в своём заявлении CPS), которая позволяет в таких обстоятельствах повторно использовать имена.[1]

PublicKey

Это поле **должно** присутствовать.

extensions

Профиль для расширений в запросах сертификатов описан в параграфе 6.3.

6.2.2. Управляющие поля запросов сертификата ресурса

Данный профиль поддерживает дополнительное управляющее поле, приведённое ниже.

Authenticator Control

Предполагаемая модель аутентификации субъекта является «долгосрочной» (long term) и рекомендации [RFC4211] предлагают использовать поле Authenticator Control.

6.3. Атрибуты расширения сертификата в запросах сертификатов

Ниже перечислены расширения, которые **могут** присутствовать в запросах сертификатов PKCS#10 или CRMF. Появление каких-либо иных расширений в Certificate Request **недопустимо**. Этот профиль накладывает на расширения некоторые дополнительные ограничения, перечисленные ниже.

BasicConstraints

При отсутствии этого расширения CA будет выпускать сертификат EE (и тоже без расширения BasicConstraints).

Поле pathLengthConstraint не поддерживается данным профилем и **должно** быть опущено.

CA **может** следовать установленному биту cA = TRUE (CA Certificate Request). Установленный бит показывает, что субъект запрашивает сертификат CA.

CA **должен** следовать сброшенному биту cA = FALSE (EE Certificate Request) и в этом случае соответствующий сертификат EE не будет включать расширения Basic Constraints.

KeyUsage

CA **может** следовать расширениям KeyUsage со значениями keyCertSign и cRLSign, если они указаны и согласуются с полем BasicConstraints SubjectType, когда оно задано.

ExtendedKeyUsage

CA **может** следовать расширениям ExtendedKeyUsage в запросах сертификатов EE, выпускаемых для маршрутизаторов и других устройств, которые согласуются со значениями, заданными в документах Standards

[1] В оригинале текст этого абзаца содержал ошибку, см. https://www.rfc-editor.org/errata/eid4080. *Прим. перев.*

Track RFC, принимающих этот профиль и указывающих специфические для приложения требования, служащие мотивом использования таких EKU.[1]

SubjectInformationAccess

Это поле **должно** присутствовать и CA **следует** соблюдать его значение, если оно соответствует требованиям, указанным в параграфе 4.8.8. Если CA не может соблюсти значение этого поля, он **должен** отбросить запрос сертификата.

7. Проверка пригодности сертификата ресурса

В этом разделе описана процедура проверки пригодности сертификата ресурсов, уточняющая базовую процедуру, которая описана в разделе 6 [RFC5280].

7.1. Проверка пригодности расширения

Расширения IP Resources и AS Resources [RFC3779] являются критическими для INR. Они используют представление ASN.1 для адресных диапазонов IPv4 и IPv6 а также номеров AS.

Пригодные для использования сертификаты ресурсов **должны** иметь расширение с корректными адресами IP и/или номерами AS. Для проверки пригодности сертификата ресурса пригодность расширения также **должна** проверяться. Процедура проверки основана на приведённых ниже правилах сравнения наборов ресурсов.

more specific - более специфический (узкий)

Если даны два непрерывных диапазона адресов IP или номеров AS, обозначенные A и B, множество A является более узким по сравнению с B, если B включает все адреса IP или номера AS, входящие в A, и диапазон B больше диапазона A.

equal - равный

Два заданных непрерывных диапазона адресов IP или номеров AS, обозначенные A и B, считаются равными (equal), если диапазон A включает в точности такой же набор адресов IP или номеров AS, что и диапазон B. Определение наследования (inheritance) в [RFC3779] эквивалентно данному определению равенства.

encompass - включающий

Для двух данных наборов адресов IP или номеров AS, обозначенных X и Y, X «включает» в себя (encompasses) Y, если каждый непрерывный диапазон адресов IP или номеров AS в наборе Y, является более узким или равным непрерывному диапазону в наборе X.[2]

Проверка пригодности расширения сертификата ресурса в контексте пути сертификации (см. параграф 7.2) означает, что для каждой пары сертификатов в пути сертификации (сертификаты x и x + 1) числовые ресурсы, описанные в сертификате x, включают числовые ресурсы, описанные в сертификате x + 1, а ресурсы, описанные в информации о доверенной точке привязки включают ресурсы, описанные в первом сертификате пути сертификации.

7.2. Проверка пригодности пути сертификации ресурса

Проверка пригодности подписанных данных ресурса с использованием сертификата этого ресурса состоит в проверке пригодности цифровой подписи данных с использованием открытого ключа сертификата этого ресурса, а также проверке пригодности самого сертификата в контексте RPKI с использованием процесса проверки пригодности пути сертификации. Это процесс, среди прочего, проверяет, что ожидаемый путь сертификации (последовательность из n сертификатов) удовлетворяет всем приведённым ниже условиям:

1. для всех x в {1, ..., n-1} субъект сертификата x является эмитентом сертификата x+1;
2. сертификат 1 выпущен доверенной привязкой (trust anchor);
3. сертификат n является проверяемым на пригодность сертификатом;
4. для всех x в {1, ..., n} сертификат x является пригодным для применения (корректным).

Проверка пригодности сертификата включает проверку выполнения всех перечисленных ниже условий в дополнение к критериям проверки пригодности пути сертификации из раздела 6 [RFC5280].

1. Сертификат может быть проверен с использованием открытого ключа эмитента и алгоритма подписи.
2. Текущее время попадает в интервал действия сертификата.
3. Сертификат включает все поля, которые **должны** присутствовать в соответствии с данной спецификацией, и значения полей разрешены этой спецификацией.
4. Нет полей или значений, которые в соответствии с данной спецификацией **недопустимы** в сертификате.
5. Эмитент не отозвал сертификат. Отозванные сертификаты идентифицируются порядковыми номерами в текущем CRL эмитента, как определено в CRLDP сертификата. Сам CRL пригоден для использования и открытый ключ, используемый для проверки подписи в CRL, совпадает с открытым ключом, используемым для проверки самого сертификата.
6. Данные расширения ресурса входят (encompassed) в данные расширения ресурса, содержащиеся в пригодном сертификате, где эмитент является субъектом (предыдущий сертификат в контексте упорядоченной последовательности, определяемой путём сертификации).
7. Путь сертификации начинается с сертификата, выпущенного доверенной привязкой (trust anchor) и имеется цепочка подписей по пути сертификации, где субъект сертификата x на этом пути соответствует эмитенту сертификата x+1 этого же пути, а открытый ключ в сертификате x позволяет проверить значение подписи в сертификате x+1.

Алгоритм проверки пригодности сертификата **может** выполнять приведённые выше тесты в любом порядке.

Сертификаты и CRL, используемые в этом процессе, **могут** быть найдены в поддерживаемом локально кэше, который регулярно синхронизируется со структурой распределенных репозиториев публикации [RFC6481].

[1] В оригинале это предложение ошибочно было копией предыдущего, см. https://www.rfc-editor.org/errata/eid3228. *Прим. перев.*

[2] В оригинале это предложение содержало ошибку, см. https://www.rfc-editor.org/errata/eid5187. *Прим. перев.*

Возможны случаи когда пути сертификации имеют произвольную длину и даже попытки создания таких путей с петлями, как способы организации возможных DOS-атак[1] на RP. Выполняющие эту процедуру RP **могут** применять дополнительную эвристику в процессе проверки пути сертификации с прерыванием обработки для предотвращения проблем, связанный с попытками проверки пригодности таких искажённых структур пути сертификации. Реализации проверки пригодности сертификатов ресурсов **могут** прерывать процесс отказом, если размер пути сертификации превышает значение локально заданного конфигурационного параметра.

8. Замечания по устройству

Приведённые ниже замечания содержат некоторые дополнительные комментарии по вопросам, касающимся выбора некоторых вариантов, сделанного при разработке профиля сертификатов. Эти замечания не являются нормативными, т. е. данный раздел не является формальной частью спецификации профиля и интерпретация ключевых слов в соответствии с RFC 2119 не применима к этому разделу документа.

Расширения в сертификатах

Данный профиль не позволяет применять какие-либо другие[2] критические или некритические расширения. Причиной этого служит то, что профиль предназначен для определённого здесь конкретного применения. В этом контексте наличие сертификатов с дополнительными некритическими расширениями, которые RP могут считать пригодными, даже не понимая таких расширений, было бы неуместным, поскольку в случае понимания RP этих расширений так или иначе могло бы изменяться изначальное суждение о пригодности сертификата. Было решено отказаться от расширяемости в пользу минимализма. Конкретной целью RPKI является точно соответствие между структурой распределения INR и соответствующей структурой сертификатов, которая описывает распределение и его контекст внутри иерархии распределения INR. Профиль определяет сертификаты ресурсов, которые структурированы в соответствии с этими требованиями.

Удостоверяющие центры (CA) и значения ключей

Данный профиль использует определение экземпляра CA, как комбинацию именованного объекта (сущности) и пары ключей. В рамках этого определения экземпляр CA не может сменить свою ключевую пару. Однако объект может создать новый экземпляр CA с новой парой ключей и перенести всю подписанную подчинённую продукцию в этот новый CA [RFC6489].

Это оказывает влияние на поддержку имён субъектов, область действия CRL и управление точками публикации репозиториев.

Область действия CRL и значения ключей

Для области действия списка отзыва (CRL Scope) данный профиль указывает, что CA выпускает один список CRL (в каждый момент) и область действия этого CRL включает все сертификаты, выпущенные данным CA. Поскольку экземпляр CA привязан к одной паре ключей, это ведёт к тому, что в качестве открытого ключа CA, ключа, применяемого для проверки пригодности CRL этого CA, и ключа, применяемого для проверки пригодности сертификатов, отозванных в данном CRL, служит один и тот же ключ.

Точки публикации репозиториев

Определение CA оказывает влияние на устройство системы публикации репозиториев. Для минимизации работы по вынужденной повторной сертификации при смене ключей режим публикации репозитория использует одну и ту же точку публикации для всех экземпляров CA, относящихся к одному объекту, что позволяет сузить область повторного создания сертификатов до напрямую подчинённых сертификатов. Это описано подробно в [RFC6489].

Имена субъектов

Этот профиль задаёт уникальность имён субъектов в рамках каждого эмитента и не требует уникальности имён в глобальном масштабе (в части гарантии уникальности). Это обусловлено самой природой RPKI, которая представляет собой распределенную систему PKI, предполагающую отсутствие у удостоверяющих центров возможностей координации простого пространства имён с уникальностью в масштабе всей RPKI без применения каких-либо внешних зависимостей, оказывающих критическое влияние на работу системы в целом. УЦ предлагается использовать процедуры генерации имён субъектов, минимизирующие вероятность совпадения имён.

Одним из способов решения этой задачи является использование CA практики именования субъектов с включением компоненты CommonName отличительного имени (DistinguishedName) в качестве постоянного значения для данного элемента, который является субъектом выпускаемых CA сертификатом, и установки для компоненты serialNumber отличительного имения значения, получаемого из хэшированного значения открытого ключа данного субъекта.

Если CA выбирает отказ от использования компоненты serialNumber в DistinguishedName, ему следует рассмотреть вариант создания имён CommonName, содержащих в себе случайную компоненту со значительным (более 40 битов) объёмом энтропии. Ниже приведены некоторые не нормативные рекомендации.

1) Хэш открытого ключа субъекта (представленного в формате ASCII HEX).
   Пример: cn="999d99d564de366a29cd8468c45ede1848e2cc14"
2) Универсальный уникальный идентификатор (UUID[3]) [RFC4122].
   Пример: cn="6437d442-6fb5-49ba-bbdb-19c260652098"
3) Случайная строка в формате ASCII HEX размером не менее 20 символов.
   Пример: cn="0f8fcc28e3be4869bc5f8fa114db05e1"
   (строка из 20 символов ASCII HEX будет содержать 80 битов энтропии).
4) Ключ внутренней базы данных или идентификатор абонента в комбинации с одним из перечисленных выше вариантов.
   Пример: cn="<DBkey1> (6437d442-6fb5-49ba-bbdb-19c2606520980)"
   CA может захотеть обеспечить себе возможность извлекать ключ базы данных или идентификатор абонента из commonName. Поскольку возможность разбора commonName нужна только эмитенту, ключ базы данных и источник энтропии (например, UUID) могут быть разделены тем или иным способом без нарушения требований для PrintableString. Разделителем может служить пробел, скобки, дефис, дробная черта, кавычки и т. п.

[1] Denial-of-service - атака, нацеленная на отказ в обслуживании.
[2] Кроме явно указанных в этой спецификации. *Прим. перев.*
[3] Universally Unique Identifier.

9. Вопросы, связанные со сменой профиля

Этот профиль требует от RP отвергать сертификаты и CRL, которые не соответствуют данному профилю (в оставшейся части этого раздела термин сертификат будет использоваться для обозначения как самих сертификатов, так и списков CRL). В число отвергаемых входят сертификаты с недозволенными расширениями, который в остальном пригодны для использования [RFC5280]. Это означает, что любое изменение профиля (например, расширения, дозволенные атрибуты или необязательные поля, представление полей) для сертификатов, используемых в RPKI не будет совместимо с прежними версиями. В обычном контексте PKI такое ограничение будет вызывать серьёзные проблемы. В RPKI существует несколько факторов, которые минимизируют сложности этого типа.

Отметим, что инфраструктура RPKI уникальна в том, что каждому RP требуется доступ к каждому сертификату, выпущенному CA, входящими в систему. Важные обновления используемых в RPKI сертификатов должны поддерживаться всеми CA и RP в системе, чтобы представления данных RPKI не различались для разных RP. Таким образом, постепенные (incremental) изменения требуют тщательной координации. Постепенное добавление нового расширения или разрешение применять имеющееся стандартное расширение с относящимися к защите целями будет неприемлемо.

Можно предположить, что флаг критичности (critical flag) в расширениях сертификатов X.509 может использоваться для смягчения этой проблемы. Однако такое решение не будет полным и не избавит от проблем при добавлении новых критичных расширений, связанных с безопасностью (это обусловлено тем, что расширения должны поддерживаться повсеместно, всеми CA и RP). Кроме того, хотя некоторые стандартные расширения можно помечать как критические или некритические по усмотрению эмитента, такое свойство присуще не всем расширениям и некоторые стандартные расширения никогда не бывают критическими. Таким образом, флаг критичности не обеспечивает решения проблемы.

В типичных системах PKI имеется несколько CA и много RP. Однако в RPKI каждый CA является одновременно и RP. Таким образом, набор объектов, которые потребуется изменить для выпуска сертификатов в новом формате, совпадает с набором объектов, которые потребуется изменить для восприятия этих новых сертификатов. Это говорит о том, что при внесении изменений требуется тесная координация CA/RP. На практике для этого наблюдения имеется важное исключение. Предполагается, что небольшие ISP[1] и владельцы провайдеро-независимых адресов используют услуги CA, предлагаемые региональными регистраторами (RIR[2]) и возможно крупными ISP. Это снижает число разных реализаций CA и упрощает внесение изменений в систему выдачи сертификатов. Представляется очевидным, что на этих объектах будут также использоваться программы RP, предоставляемые их поставщиком услуг CA, и это снижает число разных реализаций RP. Отметим также, что многие мелкие ISP (и владельцы провайдеро-независимых адресов) используют принятый по умолчанию маршрут и им не требуется выполнять проверку RP для данных RPKI (т. е. эти объекты не являются RP).

Широкодоступные программы PKI RP не кэшируют большое число сертификатов, что важно для стратегии RPKI. Они не обрабатывают манифесты и структуры данных ROA, являющиеся важными элементами системы репозиториев RPKI. Опыт показывает, что такие программы плохо работают с данными о статусе отзыва. По этой причине имеющиеся программы RP не подходят для RPKI, хотя некоторые открытые программные средства (например, OpenSSL и cryptlib) можно использовать в качестве компонент реализации RPKI RP. Таким образом, предполагается, что RP будут использовать программы, разработанные специально для среды RPKI и доступные из небольшого числа открытых источников. Такие программы уже предлагают несколько RIR и две компании. Таким образом, вполне возможна координация действий небольшого числа разработчиков программ.

Если профиль сертификата ресурсов будет измене (например, путём добавления новых расширений, изменения разрешённого набора атрибутов имён или представления этих атрибутов), для изменения развёрнутой системы RPKI будет применяться описанная ниже процедура. Эта модель аналогична описанной в [RPKI-ALG], но проще её.

Новый документ будет выпускаться как обновление данного RFC. Политика CP для RPKI [RFC6484] будет обновлена в соответствии с новым профилем сертификата. Новая CP будет определять новый идентификатор политики (OID) для сертификатов, выпущенных с использованием нового профиля. Обновлённая CP также будет определять расписание перехода на новых формат сертификатов и CRL. Этот расписание будет определять 3 фазы и связанные с ними даты.

1. В конце фазы 1 все RPKI CA **должны** быть способны выпускать сертификаты в соответствии с новым профилем по запросам субъектов. Все сертификаты, выпущенные с новым форматом, должны включать новое значение OID для политики.

2. В течение фазы 2 CA **должны** выпускать сертификаты с новым профилем и эти сертификаты **должны** сосуществовать с сертификатами старого формата (CA будут пока продолжать выпуск сертификатом со старым форматом и OID). Старые и новые сертификаты **должны** быть идентичными, за исключением OID политики, а также новых расширений, представлений и т. п. Новые сертификаты и связанные с ними подписанные объекты будут сосуществовать со старыми в системе репозиториев RPKI на этой фазе аналогично тому, как это описано для смены алгоритма RPKI в [RPKI-ALG]. RP **могут** применять старые или новые сертификаты при обработке подписанных объектов, получаемых из репозиториев RPKI. В этой фазе RP, решившие обрабатывать оба формата, будут получать одинаковые значения для всех полей сертификатов, которые присутствуют в старом и новом формате. Таким образом, если любой из форматов сертификата может быть проверен, RP будет воспринимать данные из этого сертификата. Это позволяет CA начать выпуск сертификатов нового формата до того, как все RP будут готовы его обрабатывать.

3. В начале фазы 3 все RP **должны** обеспечивать возможность обработки сертификатов нового формата. В этой фазе CA будут выпускать новые сертификаты с использованием **только** нового формата. Сертификаты, выпущенные со старым OID будут заменены сертификатами с OID новой политики. От системы репозиториев больше не требуется обеспечивать соответствие старых и новых сертификатов.

В конце фазы 3 все сертификаты со старыми OID будут заменены. RFC с профилем сертификата ресурсов будет заменён для прекращения поддержки старого формата сертификатов, а политика CP будет заменена для удаления ссылки на OID старой политики и RFC со старым профилем сертификатов. Система перейдёт в новое стабильное состояние.

[1] Internet Service Provider - поставщик услуг Internet, провайдер.
[2] Regional Internet Registry региональный регистратор Internet.

10. Вопросы безопасности

Разделы «Вопросы безопасности» в [RFC5280] и [RFC3779] применимы к сертификатам ресурсов. Разделы «Вопросы безопасности» в [RFC2986] и [RFC4211] применимы к запросам сертификатов ресурсов.

PKI сертификатов ресурсов не может сама по себе разрешать какие-либо неоднозначности, связанные с уникальностью заявлений о правах использования в случаях, когда два или более сертификата охватывают один и тот же ресурс. Если выдача сертификатов ресурсов согласована со статусом распределения и присвоения ресурсов, информация в сертификате является ничем не лучше информации в базах данных о распределении и присвоении значений.

Этот профиль требует совпадения ключа, использованного для подписи при выпуске сертификата, с ключом, используемым для подписи CRL с отзывами сертификатов. Это предполагает, что путь сертификации, используемый для проверки пригодности подписи сертификата совпадает с путём, используемым для проверки пригодности подписи CRL, который может отозвать сертификат. Отмечено, что это ограничение жёстче требуемого в X.509 PKI и может возникать риск появления реализации проверки пути, которая сможет использовать разные пути для проверки сертификата и соответствующего CRL. Если в RPKI возникает конфликт имён субъектов в результате отступления CA от приведённых здесь рекомендаций по обеспечению достаточной энтропии в именах субъектов и это происходит в ситуации, когда RP использует реализацию, в которой создание пути проверки также не соответствует данному профилю RPKI, конфликт имён субъектов может привести RP в ложному заключению об отзыве сертификата.

11. Благодарности

Авторы хотели бы отметить особо ценный вклад Stephen Kent в рецензирование этого документа и подготовку множества включённых в документ фрагментов текста. Авторы также благодарят Sandy Murphy, Robert Kisteleki, Randy Bush, Russ Housley, Ricardo Patara и Rob Austein за подготовку и последующее рецензирование документа. В документе также отражены комментарии, полученные от Roque Gagliano, Sean Turner и David Cooper.

12. Литература

12.1. Нормативные документы

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

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, November 2000.

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

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, September 2005.

[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.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, February 2012.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, February 2012.

[X.509] ITU-T, "Recommendation X.509: The Directory - Authentication Framework", 2000.

[X.680] ITU-T, "Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", 2002.

12.2. Дополнительная литература

[RFC2985] Nystrom, M. and B. Kaliski, "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, November 2000.

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

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, July 2005.

[RFC4514] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, June 2006.

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

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

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

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

[RPKI-ALG] Gagliano, R., Kent, S., and S. Turner, "Algorithm Agility Procedure for RPKI", Work in Progress[1], November 2011.

Приложение A. Пример сертификата ресурса

Ниже приведён пример сертификата ресурса.

```
Certificate Name: 9JfgAEcq7Q-47IwMC5CJIJr6EJs.cer
Data:
  Version: 3 (0x2)
  Serial: 1500 (0x5dc)
  Signature Algorithm: SHA256WithRSAEncryption
  Issuer: CN=APNIC Production-CVPQSgUkLy7pOXdNeVWGvnFX_0s
  Validity
   Not Before: Oct 25 12:50:00 2008 GMT
    Not After : Jan 31 00:00:00 2010 GMT
  Subject: CN=A91872ED
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
    Modulus (2048 bit):
      00:bb:fb:4a:af:a4:b9:dc:d0:fa:6f:67:cc:27:39:
      34:d1:80:40:37:de:88:d1:64:a2:f1:b3:fa:c6:7f:
      bb:51:df:e1:c7:13:92:c3:c8:a2:aa:8c:d1:11:b3:
      aa:99:c0:ac:54:d3:65:83:c6:13:bf:0d:9f:33:2d:
      39:9f:ab:5f:cd:a3:e9:a1:fb:80:7d:1d:d0:2b:48:
      a5:55:e6:24:1f:06:41:35:1d:00:da:1f:99:85:13:
      26:39:24:c5:9a:81:15:98:fb:5f:f9:84:38:e5:d6:
      70:ce:5a:02:ca:dd:61:85:b3:43:2d:0b:35:d5:91:
      98:9d:da:1e:0f:c2:f6:97:b7:97:3e:e6:fc:c1:c4:
      3f:30:c4:81:03:25:99:09:4c:e2:4a:85:e7:46:4b:
      60:63:02:43:46:51:4d:ed:fd:a1:06:84:f1:4e:98:
      32:da:27:ee:80:82:d4:6b:cf:31:ea:21:af:6f:bd:
      70:34:e9:3f:d7:e4:24:cd:b8:e0:0f:8e:80:eb:11:
      1f:bc:c5:7e:05:8e:5c:7b:96:26:f8:2c:17:30:7d:
      08:9e:a4:72:66:f5:ca:23:2b:f2:ce:54:ec:4d:d9:
      d9:81:72:80:19:95:57:da:91:00:d9:b1:e8:8c:33:
      4a:9d:3c:4a:94:bf:74:4c:30:72:9b:1e:f5:8b:00:
      4d:e3
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      F4:97:E0:00:47:2A:ED:0F:B8:EC:8C:0C:0B:90:89:
      20:9A:FA:10:9B
    X509v3 Authority Key Identifier:
      keyid:09:53:D0:4A:05:24:2F:2E:E9:39:77:4D:79:
      55:86:BE:71:57:FF:4B
    X509v3 Key Usage: critical
      Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical
      CA:TRUE
    X509v3 CRL Distribution Points:
      URI:rsync://rpki.apnic.net/repository/A3C38A24
          D60311DCAB08F31979BDBE39/CVPQSgUkLy7pOXdNe
          VWGvnFX_0s.crl
    Authority Information Access:
       CA Issuers - URI:rsync://rpki.apnic.net/repos
          itory/8BDFC7DED5FD11DCB14CF4B1A703F9B7/CVP
          QSgUkLy7pOXdNeVWGvnFX_0s.cer
    X509v3 Certificate Policies: critical
       Policy: 1.3.6.1.5.5.7.14.2
    Subject Information Access:
       CA Repository - URI:rsync://rpki.apnic.net/mem
           ber_repository/A91872ED/06A83982887911DD81
           3F432B2086D636/
       Manifest - URI:rsync://rpki.apnic.net/member_r
           epository/A91872ED/06A83982887911DD813F432
           B2086D636/9JfgAEcq7Q-47IwMC5CJIJr6EJs.mft
     sbgp-autonomousSysNum: critical
      Autonomous System Numbers:
        24021
        38610
        131072
        131074
     sbgp-ipAddrBlock: critical
      IPv4:
        203.133.248.0/22
        203.147.108.0/23
Signature Algorithm: sha256WithRSAEncryption
    51:4c:77:e4:21:64:80:e9:35:30:20:9f:d8:4b:88:60:b8:1f:
    73:24:9d:b5:17:60:65:6a:28:cc:43:4b:68:97:ca:76:07:eb:
    dc:bd:a2:08:3c:8c:56:38:c6:0a:1e:a8:af:f5:b9:42:02:6b:
    77:e0:b1:1c:4a:88:e6:6f:b6:17:d3:59:41:d7:a0:62:86:59:
    29:79:26:76:34:d1:16:2d:75:05:cb:b2:99:bf:ca:c6:68:1b:
```

[1]Работа опубликована в RFC 6916. *Прим. перев.*

```
      b6:a9:b0:f4:43:2e:df:e3:7f:3c:b3:72:1a:99:fa:5d:94:a1:
      eb:57:9c:9a:2c:87:d6:40:32:c9:ff:a6:54:b8:91:87:fd:90:
      55:ef:12:3e:1e:2e:cf:c5:ea:c3:4c:09:62:4f:88:00:a0:7f:
      cd:67:83:bc:27:e1:74:2c:18:4e:3f:12:1d:ef:29:0f:e3:27:
      00:ce:14:eb:f0:01:f0:36:25:a2:33:a8:c6:2f:31:18:22:30:
      cf:ca:97:43:ed:84:75:53:ab:b7:6c:75:f7:2f:55:5c:2e:82:
      0a:be:91:59:bf:c9:06:ef:bb:b4:a2:71:9e:03:b1:25:8e:29:
      7a:30:88:66:b4:f2:16:6e:df:ad:78:ff:d3:b2:9c:29:48:e3:
      be:87:5c:fc:20:2b:df:da:ca:30:58:c3:04:c9:63:72:48:8c:
      0a:5f:97:71
```

Приложение B. Пример списка отозванных сертификатов

Ниже приведён пример списка отозванных сертификатов (CRL).

```
CRL Name: q66IrWSGuBE7jqx8PAUHAlHCqRw.crl
Data:
  Version: 2
  Signature Algorithm:
    Hash: SHA256, Encryption: RSA
  Issuer: CN=Demo Production APNIC CA - Not for real use,
    E=ca@apnic.net
  This Update: Thu Jul 27 06:30:34 2006 GMT
  Next Update: Fri Jul 28 06:30:34 2006 GMT
  Authority Key Identifier: Key Identifier:
    ab:ae:88:ad:64:86:b8:11:3b:8e:ac:7c:3c:05:
    07:02:51:c2:a9:1c
  CRLNumber: 4
  Revoked Certificates: 1
    Serial Number: 1
    Revocation Date: Mon Jul 17 05:10:19 2006 GMT
    Serial Number: 2
    Revocation Date: Mon Jul 17 05:12:25 2006 GMT
    Serial Number: 4
    Revocation Date: Mon Jul 17 05:40:39 2006 GMT
  Signature:
    b2:5a:e8:7c:bd:a8:00:0f:03:1a:17:fd:40:2c:46:
    0e:d5:64:87:e7:e7:bc:10:7d:b6:3e:39:21:a9:12:
    f4:5a:d8:b8:d4:bd:57:1a:7d:2f:7c:0d:c6:4f:27:
    17:c8:0e:ae:8c:89:ff:00:f7:81:97:c3:a1:6a:0a:
    f7:d2:46:06:9a:d1:d5:4d:78:e1:b7:b0:58:4d:09:
    d6:7c:1e:a0:40:af:86:5d:8c:c9:48:f6:e6:20:2e:
    b9:b6:81:03:0b:51:ac:23:db:9f:c1:8e:d6:94:54:
    66:a5:68:52:ee:dd:0f:10:5d:21:b8:b8:19:ff:29:
    6f:51:2e:c8:74:5c:2a:d2:c5:fa:99:eb:c5:c2:a2:
    d0:96:fc:54:b3:ba:80:4b:92:7f:85:54:76:c9:12:
    cb:32:ea:1d:12:7b:f8:f9:a2:5c:a1:b1:06:8e:d8:
    c5:42:61:00:8c:f6:33:11:29:df:6e:b2:cc:c3:7c:
    d3:f3:0c:8d:5c:49:a5:fb:49:fd:e7:c4:73:68:0a:
    09:0e:6d:68:a9:06:52:3a:36:4f:19:47:83:59:da:
    02:5b:2a:d0:8a:7a:33:0a:d5:ce:be:b5:a2:7d:8d:
    59:a1:9d:ee:60:ce:77:3d:e1:86:9a:84:93:90:9f:
    34:a7:02:40:59:3a:a5:d1:18:fb:6f:fc:af:d4:02:
    d9
```

Адреса авторов

Geoff Huston
APNIC
EMail: gih@apnic.net
URI: http://www.apnic.net

George Michaelson
APNIC
EMail: ggm@apnic.net
URI: http://www.apnic.net

Robert Loomans
APNIC
EMail: robertl@apnic.net
URI: http://www.apnic.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru