Internet Engineering Task Force (IETF)
Request for Comments: 6916
BCP: 182
Category: Best Current Practice
ISSN: 2070-1721

R. Gagliano
Cisco Systems
S. Kent
BBN Technologies
S. Turner
IECA, Inc.

April 2013

Процедура смены алгоритма для RPKI

Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)

Тезисы

В этом документе описан процесс, которому должны следовать удостоверяющие центры (CA[1]) и зависимые стороны (RP[2]), участвующие в инфраструктуре открытых ключей ресурсов (RPKI[3]), для перехода к новому (и возможно более криптостойкому) набору алгоритмов. Предполагается, что этот процесс займет несколько лет. Следовательно, какого-либо экстренного перехода не задается. Описанная здесь процедура поддерживает только миграцию «сверху вниз» (сначала переходят родители, а затем потомки).

Статус документа

Этот документ относится к категории «Обмен опытом» (Internet Best Current Practice).

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/rfc6916.

Оглавление

1. Введение....2
2. Уровни требований....2
3. Терминология....2
4. Этапы смены ключей при переходе на другой алгоритм....3
  4.1. Основные определения....3
  4.2. Обзор процесса....3
  4.3. Фаза 0....4
    4.3.1. Веха 1....4
  4.4. Фаза 1....5
  4.5. Фаза 2....5
  4.6. Фаза 3....6
  4.7. Фаза 4....6
  4.8. Возврат к фазе 0....7
5. Поддержка множества алгоритмов в протоколе обеспечения RPKI....7
6. Проверка пригодности множества подписанных экземпляров....7
7. Отзыв сертификатов....8
8. Смена ключа....8
9. Структура репозитория....8
10. Отказ от использования алгоритма....8
11. Вопросы безопасности....8
12. Благодарности....9
13. Нормативные документы....9

[1]Certification Authority.
[2]Relying Party — зависимая сторона.
[3]Resource Public Key Infrastructure.
[4]Internet Engineering Task Force.
[5]Internet Engineering Steering Group.

1. Введение

Инфраструктура открытых ключей ресурсов (RPKI[1]) должна приспосабливаться к переходам между открытыми ключами, используемыми удостоверяющими центрами (CA или УЦ). Переходы этого типа обычно называют «сменой ключей» (key rollover). Плановые замены ключей будут происходить регулярно в течение работы RPKI, поскольку каждый CA меняет свои открытые без координации с другими УЦ (это означает, что момент смены ключей в каждом УЦ определяется локальными условиями и не координируется в масштабе RPKI). Более того, поскольку смена ключей может быть вызвана предполагаемой компрометацией секретного ключа, предполагать координацию таких замен на всех УЦ в масштабе RPKI просто не реально. При вынужденной (аварийной) замене ключа старый сертификат отзывается и выпускается сертификат с новым ключом. Механизмы замены ключей в RPKI (плановой или аварийной) при использовании общего криптографического набора описаны в [RFC6489].

В этом документе описывается механизм смены ключей в RPKI по причине перехода к новому набору алгоритмов подписи. Документ определяет процесс, которому CA и RP, участвующие в RPKI, должны будут следовать для перехода на новый (возможно, более криптостойкий) набор алгоритмов. Предполагается, что процесс перехода может занимать месяцы и даже годы. Следовательно, экстренных мер перехода не задается. Определенная в документе процедура перехода только миграцию «сверху вниз» (сначала переходят родители, а затем потомки).

Набор алгоритмов подписи включает собственно алгоритм подписи (с заданным диапазоном размеров ключей) и необратимую хэш-функцию. Предполагается, что RPKI будет с течением времени требовать обновления размера ключей и/или замены набора алгоритмов. В этом документе рассматривается принятие нового алгоритма хэширования с сохранением текущего алгоритма подписи и необходимостью смены ключей в CA. Переход к новому набору алгоритмов может диктоваться требованиями поддержки необходимого уровня криптографической защиты и обеспечения целостности сертификатов, списков отзыва (CRL) и подписанных объектов в RPKI. Все структуры данных в RPKI явно указывают используемые алгоритмы подписи и хэширования. Однако опыт показывает, что возможность представить идентификаторы алгоритмов не достаточно для обеспечения возможности перехода к новому набору алгоритмов (algorithm agility — обновление алгоритма). Требуется обеспечить переход от одного набора алгоритмов к другому также на уровне протоколов, элементов инфраструктуры и рабочих процедур. Предполагается, что переход к другим алгоритмам будет происходить очень редко и будет требовать поддержки «текущего» и «будущего» набора алгоритмов в течение долгого срока (возможно, нескольких лет).

В этом документе определяется процедура запланированной в RPKI смены ключей CA при замене набора алгоритмов. Описание включает действия CA, операторов репозиториев и RP. Описаны требования к поведению CA и RP для обеспечения работы RPKI в процессе смены ключей, а также использование системы репозиториев RPKI для поддержки смены ключей.

Этот документ не задает какого-либо конкретного набора алгоритмов. Политика сертификации (CP[2]) RPKI [RFC6484] требует использования в CA и RP алгоритмов, определенных в [RFC6485]. При инициировании смены алгоритмов документ [RFC6485] **должен** быть обновлен (см. параграф 4.1 настоящего документа) для переопределения требуемых CP алгоритмов в совместимых со спецификацией RPKI CA и RP. Политика CP не меняется в результате смены алгоритмов и, таким образом, идентификатор OID для нее в сертификатах RPKI остается прежним.

Для каждой смены алгоритма **должен** публиковаться дополнительный документ (расписание перехода) в серии BCP для определения даты каждой вехи перехода. Такой документ будет определять фазы перехода в соответствии с приведенными в разделе 4 описаниями. Документ также будет описывать как сообщество RPKI будет оценивать готовность CA и RP к переходу в каждую фазу. В процессе перехода CA публикуют сертификаты, списки CRL и другие подписанные объекты с использованием нового набора алгоритмов. Это обеспечит видимость развертывания нового набора алгоритмов и позволит сообществу оценить процесс перехода. Процедура перехода позволяет CA удалять старые сертификаты, списки CRL и подписанные объекты после определенной («сумеречной» - twilight) даты, что позволит наблюдать и оценивать вывод из обращения старого набора алгоритмов. Таким образом, фазы, определенные в этом документе, позволят сообществу оценить процесс перехода. Документ с расписанием также будет определять изменение расписания при возникновении проблем, связанных с реализацией заключительных фаз перехода. Документы с расписанием **рекомендуется** разрабатывать представителям сообщества RPKI - например, IANA, регистраторам Internet, сетевым операторам.

2. Уровни требований

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

3. Терминология

В этом документе предполагается, что читатель знаком с терминологией и концепциями документов Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC5280], X.509 Extensions for IP Addresses and AS Identifiers [RFC3779] и A Profile for Resource Certificate Repository Structure [RFC6481]. Дополнительные термины и соглашения, используемые в примерах, приведены ниже.

Algorithm migration — смена алгоритмов
: Запланированный переход от одного алгоритма подписи и хэширования к другому.

Algorithm Suite A — набор алгоритмов A
: «Текущий» алгоритм хэширования и подписи (термин используется в примерах).

Algorithm Suite B — набор алгоритмов B
: «Следующий» алгоритм хэширования и подписи (термин используется в примерах).

CA X — УЦ X
: CA, выпустивший сертификат CA Y (т. е. «родитель» CA Y) (термин используется в примерах).

[1]Resource Public Key Infrastructure.
[2]Certificate Policy.

CA Y — УЦ Y
CA, не являющийся «листом» дерева (термин используется в примерах).

CA Z — УЦ Z
CA, являющийся «потомком» CA Y (термин используется в примерах).

Correspond - соответствие
Два сертификата, выпущенные с использованием разных наборов алгоритмов, соответствуют один другому, если они выпущены одним и тем же элементом одного CA и привязаны к идентичным ресурсам INR[1] для этого элемента. Два CRL соответствуют друг другу, если они выпущены одним CA и перечисляют соответствующие сертификаты. Два подписанных объекта (не манифесты) соответствуют друг другу, если они проверены с использованием соответствующих сертификатов EE[2] и содержат одинаковое инкапсулированное поле Context Info. Два манифеста соответствуют друг другу, если они охватывают соответствующие сертификаты, ROA[3], CRL и другие подписываемые объекты (по отношению к подписанным результатам (продукции) RPKI в качестве синонима используется термин «эквивалентны»).

Leaf CA — CA-лист (оконечный)
CA, выдающий только сертификаты EE.

Non-Leaf CA — CA, не являющийся «листом»
CA, выдающий сертификаты другим CA.

PoP (proof of possession) — подтверждение обладания
Исполнение протокола, показывающее эмитенту, что запрашивающий сертификат субъект обладает секретным ключом, соответствующим открытому ключу в запросе сертификата, поданном этим субъектом.

ROA
Полномочия «порождения» маршрута в соответствии с определением [RFC6482].

Signed product set (set или product set) — набор подписанных результатов (продукции)
Набор сертификатов, подписанных объектов, CRL и манифест, связанные проверяемостью с использованием одного и того же сертификата родительского CA.

4. Этапы смены ключей при переходе на другой алгоритм

«Текущий» набор алгоритмов RPKI (Suite A) определяется в документе RPKI CP со ссылкой на [RFC6485]. Когда возникает необходимость замены набора алгоритмов RPKI, первым шагом **должно** быть обновление [RFC6485] для задания нового набора алгоритмов. **Должен** также быть опубликован документ (в серии BCP) с расписанием (графиком) перехода для информирования сообщества о датах, выбранных вехами переходного процесса, как описано в параграфе 4.1.

4.1. Основные определения

CA Ready Algorithm B Date — дата готовности CA к алгоритму B
После этой даты все non-leaf CA **должны** быть готовы к обработке запросов от дочерних CA на выпуск сертификатов с использованием Algorithm Suite B. Все УЦ, публикующие [RFC6490] TAL[4] для Algorithm Suite A, **должны** также опубликовать соответствующие TAL для Algorithm Suite B.

CA Go Algorithm B Date — дата перехода CA на алгоритм B
После этой даты все CA **должны** заново выпустить все комплекты своей продукции с использованием Algorithm Suite B.

RP Ready Algorithm B Date — дата готовности RP к алгоритму B
После этой даты все RP **должны** быть готовы обрабатывать материалы, подписанные с помощью Algorithm Suite B.

Twilight Date — дата «сумерек»
После этой даты CA **могут** прекращать выпуск продукции, подписанной с использованием Algorithm Suite A, а RP **могут** отказаться от проверки пригодности материалов, подписанных с использованием Algorithm Suite A.

End-Of-Life (EOL) Date — дата завершения
После этой даты использование Algorithm Suite A **должно** быть прекращено в соответствии с процедурой, описанной в разделе 10, а все TAL набора алгоритмов A **должны** быть удалены из мест их публикации.

4.2. Обзор процесса

Процесс перехода, описанный в этом документе, включает последовательность этапов, которые **должны** быть пройдены (выполнены) CA и RP в хронологическом порядке. Единственной вехой, на которой CA и RP одновременно выполняют действия, является дата завершения (EOL Date). Децентрализованная природа RPKI предполагает протяженность процесса смены алгоритмов в несколько лет.

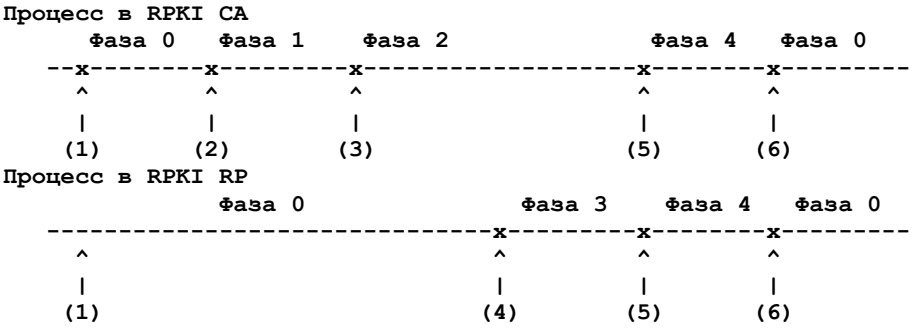
Для облегчения перехода CA будуи начинать выпуск сертификатов с использованием набора алгоритмов B в иерархическом порядке «сверху-вниз». В нашем примере CA Y будет выпускать сертификаты с использованием набора алгоритмов B только после того, как это начнет делать CA X (CA Y Ready Algorithm B Date > CA X Ready Algorithm B Date). Такой упорядоченный переход предотвращает выпуск «смеси» сертификатов CA — например, сертификат CA, подписанный с использованием алгоритмов A, который будет содержать ключ из набора B. В RPKI удостоверяющим центрам CA **недопустимо** подписывать сертификаты CA, содержащие ключ субъекта, который соответствует набору алгоритмов, отличающемуся от используемого для подписывания сертификата (X.509 приспосабливается к таким сертификатам со смешением алгоритмов, но этот процесс предотвращается за счет использования описанного подхода). Модель перехода, отличающаяся от «сверху-вниз», будет требовать применения таких смешанных сертификатов и приведет к экспоненциальному росту размера репозиториев RPKI. Кроме того, поскольку RPKI CP требует PoP для запросов сертификатов, для CA невозможно запросить сертификат для набора алгоритмов B, пока родительский CA не поддерживает этот набор (см. раздел 5).

Описанная здесь модель смены алгоритмов не запрещает CA выпуск сертификатов EE с использованием открытого ключа субъекта из другого набора алгоритмов, если этот сертификат не применяется для проверки пригодности

[1] Internet Number Resource — числовые ресурсы (номера) Internet.
[2] End-entity — конечный элемент.
[3] Route Origination Authorization — полномочия «порождения» маршрутов.
[4] Trust Anchor Locator — расположение доверенных привязок.

объектов в репозитории. Это исключение из правила запрета сертификатов со смешением алгоритмов сделано потому, что сертификаты EE не используются при проверке пригодности объектов репозитория и препятствуют RP загружать и проверять пригодность содержимого репозитория. Как отмечено выше, каждый CA в RPKI должен выполнять проверку PoP для открытого ключа субъекта при выпуске сертификата. В общем случае субъект не может предполагать, что CA может поддерживать разные алгоритмы. Однако у субъектов, тесно связанных с CA, есть основания предположить возможность выяснить способен ли CA поддержать запрос на выпуск сертификата EE, содержащего конкретный иной алгоритм открытого ключа. Данный документ не задает способа, с помощью которого субъект может узнать о способности CA выпускать смешанные сертификаты EE, поскольку возможность выдачи таких сертификатов предполагается лишь в контексте, где субъект и CA достаточно тесно связаны между собой (например, ISP, выпускающий сертификаты для управляемых им устройств).

На рисунке приведен обзор процесса смены набора алгоритмов.



(1) документ по алгоритму RPKI обновлен и выпущен документ с расписанием перехода к новому алгоритму;

(2) дата готовности CA к алгоритму B;

(3) дата перехода CA на алгоритм B;

(4) дата готовности RP к алгоритму B;

(5) дата «сумерек»;

(6) дата завершения (EOL).

Каждая из этих вех процесса рассмотрена в последующих параграфах при обсуждении фаз переходного процесса.

Были отмечены две ситуации, являющиеся мотивами для приостановки или отката назад процесса перехода. Первая ситуация возникает, если сообщество RPKI еще не готово к переходу. Например, множество УЦ может оказаться не подготовленным к выпуску сертификатов с набором B или многие RP окажутся не готовыми к обработке продукции набора B. В таких случаях расписание перехода **должно** выпускаться заново с переносом даты соответствующей фазы и сдвигом дат последующих фаз. Другая ситуация связана с обнаружением в процессе перехода серьезных проблем в безопасности алгоритмов набора B. Это будет служить мотивом остановки перехода и возврата к набору A. В таких случаях расписание перехода **должно** быть опубликовано заново, а документ по алгоритмам RPKI **должен** быть заменен. В описании фаз перехода при необходимости упоминаются обе эти ситуации.

4.3. Фаза 0

Фаза 0 является стационарной частью процесса, на которой Algorithm Suite A является единственным поддерживаемым в RPKI набором алгоритмов. Фаза 0 является устойчивым состоянием RPKI.

В фазе 0, удостоверяющие центры (CA) X, Y и Z должны генерировать подписанную продукцию, используя только Algorithm Suite A. RP также должны проверять пригодность подписанной продукции, используя только Algorithm Suite A.

На рисунке ниже приведен пример структуры подписанного объекта в репозитории, показывающий используемые наборы алгоритмов и отношения между CA (X, Y, Z), которые формируют цепочку сертификации. Размещение по вертикали показывает объекты, подписанные одним CA с использованием одного секретного ключа. Сдвиг по горизонтали представляет использование разных точек публикации для объектов, подписанных разными УЦ. Символы |-> использованы для визуализации связей при подписывании и изменения точек публикации. Например, объекты CA-Y-Certificate-Algorithm-Suite-A, CA-X-CRL-Algorithm-Suite-A и CA-X-Signed-Objects-Algorithm-Suite-A подписаны с использованием секретного ключа, соответствующего CA-X-Certificate-Algorithm-Suite-A, и опубликованы в точке CA X.

```
CA-X-Certificate-Algorithm-Suite-A (Cert-XA)
        |-> CA-Y-Certificate-Algorithm-Suite-A (Cert-YA)
                |-> CA-Z-Certificate-Algorithm-Suite-A (Cert-ZA)
                        |-> CA-Z-CRL-Algorithm-Suite-A (CRL-ZA)
                        |-> CA-Z-Signed-Objects-Algorithm-Suite-A
                |-> CA-Y-CRL-Algorithm-Suite-A (CRL-YA)
                |-> CA-Y-Signed-Objects-Algorithm-Suite-A
        |-> CA-X-CRL-Algorithm-Suite-A (CRL-XA)
        |-> CA-X-Signed-Objects-Algorithm-Suite-A
```

Примечание. Cert-XA представляет сертификат для CA X, подписанный с использованием Algorithm Suite A.

4.3.1. Веха 1

Первая веха инициирует процесс перехода. При этом обновляется [RFC6485] с приведенными ниже определениями для RPKI:

- Algorithm Suite A;
- Algorithm Suite B.

Кроме того, **должен** быть опубликован документ с расписанием перехода на новый алгоритм, содержащий следующую информацию:

- CA Ready Algorithm B Date (дата готовности CA к алгоритму B);
- CA Go Algorithm B Date (дата перехода CA на алгоритм B);
- RP Ready Algorithm B Date (дата готовности RP к алгоритму B);
- Twilight Date (дата «сумерек»);
- EOL Date (дата завершения);
- Параметры оценки готовности CA и RP для каждой фазы.

Для каждой из указанных здесь дат предполагается время 1 минута после полуночи для часового пояса UTC. Более точного задания времени не требуется и не поддерживается.

4.4. Фаза 1

Фаза 1 начинается с даты готовности CA к переходу на Algorithm B. В этой фазе все УЦ, не являющиеся «листьями» (non-leaf CA), **должны** быть готовы обрабатывать запросы дочерних CA на выдачу и отзыв сертификатов с использованием Algorithm Suite B. Если окажется, что достаточно много CA не готовы к переходу, **должен** быть выпущен новый документ с расписанием перехода, как отмечено в параграфе 4.2. Однако CA, способные выдавать сертификаты с использованием набора B, могут продолжать делать это при получении запросов от своих дочерних УЦ. Поскольку эта фаза не требует от RP обработки объектов, подписанных с помощью набора B, а продукцию набора B **следует** сохранять в независимых точках публикации, это не оказывает неблагоприятного воздействия на RP. Если алгоритм набора B будет признан непригодным, документы с расписанием смены алгоритма и спецификацией нового алгоритма **должны** быть заменены, а использование Algorithm Suite B **должно** быть отменено с использованием процедуры, описанной в разделе 10.

Поскольку переход будет происходить в иерархическом порядке «всверху-вниз», дочерние CA смогут выпускать сертификаты с использованием Algorithm Suite B только после того, как их родительские CA выпустят свои сертификаты. Протокол поддержки RPKI может определить способность родительского CA выпускать сертификаты с использованием Algorithm Suite B, а также может идентифицировать соответствующий набор алгоритмов в каждом запросе подписи сертификата CSR[1] (см. раздел 5). В течение большей части этой фазы дерево продукции набора B будет неполным, т. е. не все CA будут выпускать продукцию с использованием набора B. По этой причине для обеспечения работы RP **должны** получать и проверять только продукцию набора A. Продукцию набора B следует получать и обрабатывать только в целях тестирования.

На рисунке показано состояние элементов репозитория для трех примеров CA в течение этой фазы. Поддерживаются две различных цепочки сертификатов и CA Z еще не запрашивал каких-либо материалов, использующих набор B.

```
CA-X-Certificate-Algorithm-Suite-A (Cert-XA)
        |-> CA-Y-Certificate-Algorithm-Suite-A (Cert-YA)
                |-> CA-Z-Certificate-Algorithm-Suite-A (Cert-ZA)
                        |-> CA-Z-CRL-Algorithm-Suite-A (CRL-ZA)
                        |-> CA-Z-Signed-Objects-Algorithm-Suite-A
                |-> CA-Y-CRL-Algorithm-Suite-A (CRL-YA)
                |-> CA-Y-Signed-Objects-Algorithm-Suite-A
        |-> CA-X-CRL-Algorithm-Suite-A (CRL-XA)
        |-> CA-X-Signed-Objects-Algorithm-Suite-A

CA-X-Certificate-Algorithm-Suite-B (Cert-XB)
        |-> CA-Y-Certificate-Algorithm-Suite-B (Cert-YB)
                |-> CA-Y-CRL-Algorithm-Suite-B (CRL-YB)
                |-> CA-Y-Signed-Objects-Algorithm-Suite-B
        |-> CA-X-CRL-Algorithm-Suite-B (CRL-XB)
        |-> CA-X-Signed-Objects-Algorithm-Suite-B
```

4.5. Фаза 2

Фаза 2 начинается с даты перехода CA на алгоритм B. В начале этой фазы все подписанная продукция **должна** быть доступна с использованием обоих наборов алгоритмов A и B. Таким образом, до начала этой фазы каждый CA **должен** гарантировать наличие продукции набора B для всей продукции набора A, выпущенной данным CA. В течение этой фазы каждый CA **должен** поддерживать такое соответствие. В течение этой фазы RP **должны** быть готовы проверять пригодность продукции, выпущенной с использованием Algorithm Suite A и **могут** быть готовы для проверки пригодности с использованием Algorithm Suite B.

Если обнаруживается отсутствие готовности существенного числа CA, документ с расписанием перехода **должен** быть выпущен заново, как описано в параграфе 4.2 (поскольку для обработки в RP указан уровень требований «**может**», возникновение у RP проблем с продукцией Suite B, не требует отсрочки фазы 2, но может служить основанием для задержки начала фазы 3). УЦ, способные публиковать продукцию Suite B, **могут** продолжать это. Фаза 2, подобно фазе 1, не требует какой-либо обработки в RP объектов Suite B. Продукцию Suite B **следует** сохранять в независимых точках публикации, чтобы не оказывать негативного влияния на RP, которые не готовы обрабатывать продукцию Suite B (см. раздел 9). Если алгоритм B будет сочтен неприменимым, документы с расписанием перехода и спецификацией алгоритма **должны** быть заменены, а использование Algorithm Suite B **должно** быть отменено с использованием процесса, описанного в разделе 10.

RP, которые могут обрабатывать Algorithm Suite B, **рекомендуется** принимать и проверять продукцию Suite B. RP, которые не готовы обрабатывать продукцию Suite B, **должны** продолжать использование продукции Suite A. RP,

[1] Certificate Signing Request.

которые выбрали обработку продукции с использованием Algorithm Suite A и Algorithm Suite B, следует ожидать одинаковых результатов для этих вариантов. При наличии расхождения в результатов проверки успешного результата любой из проверок будет достаточно. Подробный анализ проверки множественных экземпляров подписанных объектов приведен в разделе 6.

На рисунке показано состояние элементов репозитория для трех примеров CA в течение этой фазы, когда все подписанные объекты доступны с использованием обоих наборов алгоритмов.

```
CA-X-Certificate-Algorithm-Suite-A (Cert-XA)
        |-> CA-Y-Certificate-Algorithm-Suite-A (Cert-YA)
                |-> CA-Z-Certificate-Algorithm-Suite-A (Cert-ZA)
                        |-> CA-Z-CRL-Algorithm-Suite-A (CRL-ZA)
                        |-> CA-Z-Signed-Objects-Algorithm-Suite-A
                |-> CA-Y-CRL-Algorithm-Suite-A (CRL-YA)
                |-> CA-Y-Signed-Objects-Algorithm-Suite-A
        |-> CA-X-CRL-Algorithm-Suite-A (CRL-XA)
        |-> CA-X-Signed-Objects-Algorithm-Suite-A

CA-X-Certificate-Algorithm-Suite-B (Cert-XB)
        |-> CA-Y-Certificate-Algorithm-Suite-B (Cert-YB)
                |-> CA-Z-Certificate-Algorithm-Suite-B (Cert-ZB)
                        |-> CA-Z-CRL-Algorithm-Suite-B (CRL-ZB)
                        |-> CA-Z-Signed-Objects-Algorithm-Suite-B
                |-> CA-Y-CRL-Algorithm-Suite-B (CRL-YB)
                |-> CA-Y-Signed-Objects-Algorithm-Suite-B
        |-> CA-X-CRL-Algorithm-Suite-B (CRL-XB)
        |-> CA-X-Signed-Objects-Algorithm-Suite-B
```

4.6. Фаза 3

Фаза 3 начинается с даты готовности RP к алгоритму B. В этой фазе все подписанные наборы продукции доступны с использованием обоих наборов алгоритмов и все RP **должны** быть способны проверить их пригодность (соответствие между продукцией Suite A и Suite B, требовалось в фазе 2 и будет поддерживаться на данной фазе с сохранением означенных выше требований). В процессе подготовки к фазе RP **рекомендуется** в первую очередь получать и обрабатывать продукцию Suite B и отдавать ей предпочтение при проверке пригодности в этой фазе. Таким образом, RP **следует** сначала предпринимать попытку проверки подписанной продукции из репозитория Algorithm Suite B.

Если значительное число RP не способны обрабатывать наборы продукции, подписанные с использованием Suite B, документ с расписанием перехода **должен** быть выпущен заново со сдвигом дат для этой и последующих вех, как описано в параграфе 4.2. Поскольку продукцию Suite B **следует** публиковать в независимых точках, предполагается, что RP, не способные обрабатывать продукцию Suite B вернуться к обработке продукции Suite A, которая сохраняется в этой фазе. Если алгоритм B будет сочтен неприменимым, документы с расписанием перехода и спецификацией алгоритма **должны** быть заменены, а использование Algorithm Suite B **должно** быть отменено с использованием процесса, описанного в разделе 10.

Поведение CA на этой фазе не меняется.

4.7. Фаза 4

Фаза 4 начинается с даты «сумерек» (Twilight Date), когда алгоритм A помечается, как «старый» (old), а алгоритм B становится «текущим» (current).

В течение этой фазы все подписанная продукция **должна** выпускаться с использованием Algorithm Suite B и **может** продолжаться использование Algorithm Suite A. Все подписанные каборы продукции, выпущенные с использованием набора B, **должны** публиковаться в соответствующих местах. Подписанная продукция Suite A может быть не доступна в соответствующих ей точках публикации. Каждый RP **должен** проверять подписанные наборы продукции с использованием Suite B. RP **могут** проверять подписанные наборы продукции Suite A. Однако RP **не следует** предполагать полноту наборов продукции Suite A. По этой причине RP **следует** использовать только наборы продукции Suite B (см. раздел 6).

Если значительное число RP не способны обрабатывать наборы продукции, подписанные с использованием Suite B, документ с расписанием перехода **должен** быть выпущен заново со сдвигом дат для этой и следующех вех. Документ **должен** от CA сохранение наборов продукции Suite A, если эта фаза задерживается. Если алгоритм B будет сочтен неприменимым, документы с расписанием перехода и спецификацией алгоритма **должны** быть заменены, а использование Algorithm Suite B **должно** быть отменено с использованием процесса, описанного в разделе 10, при этом для CA **недопустимо** удалять наборы продукции Suite A. На этой стадии RP сохраняют возможность обработки подписанной продукции Suite A и функционирование RPKI не нарушается.

Ниже приведены состояния репозиториев для используемых в наших примерах CA.

```
CA-X-Certificate-Algorithm-Suite-A (Cert-XA)
        |-> CA-Y-Certificate-Algorithm-Suite-A (Cert-YA)
                |-> CA-Y-CRL-Algorithm-Suite-A (CRL-YA)
                |-> CA-Y-Signed-Objects-Algorithm-Suite-A
        |-> CA-X-CRL-Algorithm-Suite-A (CRL-XA)
        |-> CA-X-Signed-Objects-Algorithm-Suite-A

CA-X-Certificate-Algorithm-Suite-B (Cert-XB)
        |-> CA-Y-Certificate-Algorithm-Suite-B (Cert-YB)
                |-> CA-Z-Certificate-Algorithm-Suite-B (Cert-ZB)
                        |-> CA-Z-CRL-Algorithm-Suite-A (CRL-ZB)
```

```
                        |-> CA-Z-Signed-Objects-Algorithm-Suite-B
                  |-> CA-Y-CRL-Algorithm-Suite-A (CRL-YB)
                  |-> CA-Y-Signed-Objects-Algorithm-Suite-B
            |-> CA-X-CRL-Algorithm-Suite-A (CRL-XB)
            |-> CA-X-Signed-Objects-Algorithm-Suite-B
```

4.8. Возврат к фазе 0

Дата завершения (EOL) инициирует возврат к фазе 0 (стабильное состояние). В этот момент старый набор алгоритмов - Algorithm Suite A **должен** быть выведен из обращения с помощью процесса, описанного в разделе 10.

Эта фаза завершает цикл, поскольку новый набор алгоритмов (Algorithm Suite B) становится единственным, требуемым в RPKI. В этого момента данный набор алгоритмов уже будет называться Algorithm Suite A.

Если выясняется, что многие RP не способны работать с новым набором алгоритмов, документ с расписанием перехода **должен** быть выпущен заново со сдвигом даты этой вехи.

5. Поддержка множества алгоритмов в протоколе обеспечения RPKI

Описанный в этом документе переход выполняется «сверху-вниз» и требует решения двух проблем синхронизации между дочерними и родительскими CA.

- Дочерним CA требуется определить, какой из наборов алгоритмов поддерживается родительским CA.
- Дочерним CA требуется проинформировать родительский CA, какой алгоритм ему следует применять для подписывания CSR.

Протокол обеспечения RPKI [RFC6492] поддерживает множество наборов алгоритмов путем реализации разных классов ресурсов для каждого набора. Несколько разных классов ресурсов могут использоваться для одного набора алгоритмов с разными наборами ресурсов.

Дочерний CA, желающий узнать поддерживаемый его родительским CA набор алгоритмов, **должен** выполнить перечисленные ниже операции.

1. Организовать сеанс протокола обеспечения со своим родительским CA.
2. Выполнить команду list в соответствии с параграфом 3.3.1 в [RFC6492].
3. Из поля Payload в классе ресурса list response извлечь issuer's certificate для каждого класса. Набор алгоритмов для каждого класса будет соответствовать набору алгоритмов, использованному для выпуска соответствующего issuer's certificate (указан в поле SubjectPublicKeyInfo этого сертификата).

Дочерний CA, желающий указать набор алгоритмов своему родительскому CA (например, в запросе сертификата), **должен** выполнить указанные ниже операции.

1. Выполнить описанную выше задачу по определению набора алгоритмов, поддерживаемого родительским CA, и класса ресурсов, соответствующего каждому набору.
2. Указать соответствующий класс ресурса в подходящей команде протокола обеспечения (например, issue или revoke).

При получении запроса сертификата от дочернего CA родительский CA будет проверять PoP секретного ключа. Если дочерний CA запрашивает выпущенный сертификат, использующий набор алгоритмов, который не соответствует классу ресурсов, проверка пригодности PoP завершится отказом и запрос не будет выполнен.

6. Проверка пригодности множества подписанных экземпляров

В фазах 1 - 4 в инфраструктуре RPKI будут пригодны для использования одновременно два набора алгоритмов. В этом разделе описано поведение RP при проверке пригодности подписанной продукции, для которой использованы разные наборы алгоритмов.

В фазе 1 для продукции **может** существовать два экземпляра, один из которых подписан с использованием Algorithm Suite A, другой - Algorithm Suite B. Как было отмечено в параграфе 4.4, на этой фазе отдается предпочтение продукции Suite A. Вся продукция доступна для Suite A и лишь часть продукции может быть доступна для Suite B. Для работы RP **может** получать и проверять пригодность только продукции Suite A. Продукцию Suite B **следует** получать и проверять на пригодность лишь с целью тестирования. Если набор продукции имеется для обоих алгоритмов, результаты для них должны быть эквивалентными (прямое сравнение продукции Suite A и Suite B невозможно, поскольку сертификаты, CRL и манифесты будут различаться синтаксически; однако результаты процесса, т. е. данные ROA — номера автономных систем и адресные префиксы **должны** (SHOULD) соответствовать)

На фазах 2 и 3 для RP **должны** быть доступны два соответствующих друг другу экземпляра всей подписанной продукции. Как отмечено в параграфе 4.5, при при поддержке RP нового алгоритма в фазе 2 **рекомендуется** получать и проверять пригодность продукции Suite B. Если RP сталкивается с проблемой при проверке пригодности продукции Suite B, ему **следует** вернуться к продукции Suite A. RP, поддерживающие Suite B, **могут** получать оба варианта продукции и сравнивать результаты (например, выход ROA) с целью тестирования.

В фазе 3 все RP **должны** поддерживать Suite B и **должны** получать наборы продукции Suite Bsets. Если RP сталкивается с проблемой при проверке пригодности продукции Suite B, ему можно вернуться к продукции Suite A. RP, столкнувшемуся с такой проблемой, **следует** связаться с держателями соответствующих репозиториев (например, с помощью механизма, определенного в [RFC6493]) для информирования о проблеме.

В фазе 4 для всех элементов RPKI требуется лишь наличие продукции Suite B, как отмечено в параграфе 4.7. Таким образом, RP **следует** получать и проверять на пригодность только эти наборы продукции. Получение продукции Suite A может приводить к неполноте набора подписанной продукции и по этой причине **не рекомендуется**.

7. Отзыв сертификатов

Процесс смены алгоритма требует поддержки двух параллельных и эквивалентных иерархий сертификации в фазах 2 и 3 этого процесса. На протяжении этих фаз CA **должны** отзывать и запрашивать отзыв сертификатов согласованно для обоих наборов алгоритмов. Когда не происходит смены ключа (key rollover), как описано в разделе 8, CA, запрашивающий отзыв своего сертификата во время этих двух фаз перехода, **должен** сделать запрос для обоих наборов алгоритмов (A и B). Не являющимся оконечными (non-leaf) CA **не следует** проверять соответствие дочерних CA этому требованию. Отметим, что CA **должен** запрашивать отзыв своего сертификата применительно к конкретному набору алгоритмов с использованием механизма, описанного в разделе 5.

В течение фазы 1 CA, отзывающему свой сертификат для Suite A, **следует** отозвать соответствующий сертификат для Suite B, если такой существует. В течение фазы 4 CA, отзывающему свой сертификат для Suite B, **следует** отзывать и соответствующий сертификат для Suite A, если такой существует.

В течение фазы 1 CA может отозвать сертификаты для Suite B, не отзывая сертификатов для Suite A, поскольку продукция Suite B предназначена лишь для тестирования. В течение фазы CA может отозвать сертификаты для Suite A, не отзывая сертификатов для Suite B, поскольку продукция Suite A выводится из обращения.

8. Смена ключа

Смена ключа (без замены алгоритмов) выполняется независимо для каждого набора алгоритмов и **должна** происходить в соответствии с [RFC6489].

9. Структура репозитория

Для двух параллельных иерархий в процессе перехода **следует** поддерживать две независимых точки публикации. Структура репозитория для каждого набора алгоритмов описана в [RFC6481].

10. Отказ от использования алгоритма

Для отказа от использования (запрета) набора алгоритмов на каждом CA в RPKI **должны** быть выполнены перечисленные ниже операции.

1. Все CA **должны** прекратить выпуск сертификатов с использованием этого набора. Это означает, что любой запрос сертификата CA от дочерних УЦ будет отвергаться (например, путем отправки сообщения error_response с кодом ошибки «request - no such resource class», как описано в [RFC6492]).
2. Все CA **должны** прекратить создание подписанной продукции для этого набора кроме CRL и манифестов.
3. Все CA **должны** отозвать сертификаты EE для всей продукции, подписанной с использованием данного набора. CA **следует** удалить эту продукцию из своих точек публикации для предотвращения загрузки и обработки этой продукции RP.
4. Все CA **должны** отозвать все сертификаты CA, выпущенные с использованием данного набора.
5. Всем CA **следует** удалить все сертификаты CA, выпущенные с использованием данного набора.
6. Все CA, публикующие TAL для данного данного набора, **должны** удалить их из пункта публикации TAL.
7. Всем CA **следует** поддерживать точку публикации для данного набора по крайней мере до наступления срока CRL nextUpdate. Эти точки публикации **должны** содержать только CRL и манифест для данной точки. Такое поведение обеспечивает временные рамки, в которых RP могут узнать состояние отзыва подписанной продукции, которая была удалена.
8. Все RP **должны** удалить любые TAL, опубликованные для данного набора алгоритмов.

CA в иерархии RPKI могут узнавать об отказе от использования набора алгоритмов в разное время и, следовательно, будут выполнять перечисленные выше процедуры асинхронно. Так, например, CA может запросить отзыв своего сертификата лишь для того, чтобы узнать, что он уже был отозван его эмитентом. Отзыв сертификата CA делает выпущенные им с использованием этого сертификата CRL и манифест непроверяемыми на пригодность. Асинхронное выполнение указанных выше процедур явно будет создавать временную «несогласованность» между точками публикации для отменяемого набора алгоритмов. Однако даже во время такой несогласованности следует давать «отказоустойчивые» результаты (. е. RP следует отвергать продукцию, подписанную с использованием отмененного набора алгоритмов).

11. Вопросы безопасности

Смены алгоритмов в RPKI должны быть очень редким явлением и для них нужно согласие широкого сообщества. Причины смены алгоритмов могут быть связаны с недостаточной их криптостойкостью (это нормально при долгом использовании алгоритмов). Описанная в документе процедура замены означает, что прежний алгоритм будет сохраняться действующим еще годы. В течение этого срока система RPKI будет уязвима для любых криптографических «слабостей, которые могут быть вызваны ею (например, атаки со снижением уровня защиты).

Этот документ не описывает «аварийных» механизмов для процесса смена алгоритмов. По причине распределенной природы RPKI, а также огромного числа CA и RP, авторы не считают возможной разработку такого механизма.

Если CA не завершает переход к новому набору алгоритмов, как описано в этом документе (после EOL продолжает использовать «старый» набор), подписанная им продукция становится не пригодной. Следовательно, в RPKI в конце фазы 4 может сократиться объем пригодной к использованию подписанной продукции по сравнению с началом перехода. RP, которые не выполняют описанные здесь процесс, теряют возможность проверять подписанную с использованием нового набора алгоритмов продукцию. В результате неполное представление маршрутной информации из RPKI (как результат неполного перехода CA или RP) может приводить к некоторому снижению эффективности маршрутизации в Internet.

12. Благодарности

Авторы хотели бы отметить работу сопредседателей рабочей группы SIDR (Sandra Murphy, Chris Morrow, Alexey Melnikov), а также вклад Geoff Huston, Arturo Servin, Brian Weis, Terry Manderson, Brian Dickson, David Black и Danny McPherson.

13. 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.

[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.

[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.

[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.

[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.

[RFC6492] Huston, G., Loomans, R., Ellacott, B., and R. Austein, "A Protocol for Provisioning Resource Certificates", RFC 6492, February 2012.

[RFC6493] Bush, R., "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record", RFC 6493, February 2012.

Адреса авторов

Roque Gagliano

Cisco Systems

Avenue des Uttins 5

Rolle 1180

Switzerland

EMail: rogaglia@cisco.com

Stephen Kent

BBN Technologies

10 Moulton St.

Cambridge, MA 02138

USA

EMail: kent@bbn.com

Sean Turner

IECA, Inc.

3057 Nutley Street, Suite 106

Fairfax, VA 22031

USA

EMail: turners@ieca.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com