Internet Engineering Task Force (IETF)
Request for Comments: 7935
Obsoletes: 6485
Category: Standards Track
ISSN: 2070-1721

G. Huston
G. Michaelson, Ed.
APNIC

August 2016

Профиль алгоритмов и размеров ключей для использования в RPKI

The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure

Аннотация

Этот документ задаёт алгоритмы, их параметры, форматы асимметричных ключей, размеры асимметричных ключей и формат подписи для абонентов инфраструктуры открытых ключей ресурсов (RPKI1), создающих цифровые подписи для сертификатов, списков отзыва сертификатов (CRL2), подписанных объектов CMS3 и запросов сертификатов, а также для зависимых от инфраструктуры сторон (RP4), которые проверяют эти подписи.

Статус документа

Этот документ является проектом стандарта Internet (Internet Standards Track).

Документ является результатом работы IETF[1] и представляет согласованное мнение сообщества IETF. Документ был представлен на общее обозрение и одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 документа RFC 7841.

Информация о текущем статусе данного документа, обнаруженных ошибках и способах обратной связи приведена на странице http://www.rfc-editor.org/info/rfc7935.

Оглавление

1. Введение

Этот документ задаёт:

- алгоритмы и параметры цифровых подписей;
- алгоритмы и параметры хэширования;
- форматы открытых и секретных ключей;
- формат подписи,

применяемые абонентами инфраструктуры RPKI [RFC6480], которые используют цифровые подписи для сертификатов, CRL [RFC5280], подписанных объектов CMS [RFC5652] (например ROA[3]) [RFC6482] и манифестов [RFC6486]), а также запросов сертификатов [RFC2986] [RFC4211]. Зависимые от инфраструктуры стороны (RP) также используют заданные здесь алгоритмы для проверки цифровых подписей абонентов RPKI [RFC6480].

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[3]Route Origin Authorization - полномочия на создание маршрутов.

Профили и спецификации RPKI, где содержатся ссылки на RFC 6485, теперь указывают на этот документ. К таким документам относятся [RFC6484] (политика сертификации (CP[1]) в RPKI), [RFC6487] (профиль сертификатов RPKI), [RFC6480] (архитектура RPKI) и [RFC6488] (шаблон подписанных объектов для RPKI). Предполагается знакомство читателя с этими документами.

1.1. 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].

2. Алгоритмы

В RPKI используется два криптографических алгоритма.

- Алгоритмом цифровой подписи в сертификатах, CRL, подписанных объектах CMS и запросах сертификатов является RSA Public-Key Cryptography Standards (PKCS) #1 версии 1.5 (иногда его называют RSASSA-PKCS1-v1_5) из параграфа 8.2 [RFC3447].

- Алгоритмом хэширования для сертификатов, CRL, подписанных объектов CMS и запросов сертификатов является SHA-256 [SHS] (см. примечание ниже).

  Примечание. Исключением является применение алгоритма SHA-1 [SHS] при генерации в CA идентификаторов организации (generate) и ключа субъекта [RFC6487].

В сертификатах, CRL и запросах сертификатов алгоритмы хэширования и цифровой подписи указываются совместно (например, RSA PKCS #1 v1.5 with SHA-256 или проще RSA with SHA-256). Для них **должен** использоваться OID[2] sha256WithRSAEncryption из [RFC4055].

OID размещается в перечисленных ниже местах:

для сертификатов OID указывается в полях signature и signatureAlgorithm [RFC4055];

для CRL идентификатор OID указывается в поле signatureAlgorithm [RFC4055];

в запросах сертификатов OID указывается в поле signatureAlgorithm PKCS #10 [RFC2986] или в поле CRMF[3] POPOSigningKey algorithmIdentifier [RFC4211].

В CMS SignedData алгоритмы хэширования (дайджест сообщения) и цифровой подписи указываются раздельно. В полях SignedData digestAlgorithms и SignerInfo digestAlgorithm **должны** указываться алгоритм и параметры SHA-256 (как определено в [RFC5754]). При генерации объектов CMS SignedData в поле SignerInfo signatureAlgorithm **должны** указываться идентификатор объекта и параметры rsaEncryption [RFC3370]. Реализации RPKI **должны** воспринимать значения rsaEncryption или sha256WithRSAEncryption для поля SignerInfo signatureAlgorithm при проверке объектов CMS SignedData (для совместимости с объектами, созданными реализациями, которые соответствуют [RFC6485]).

3. Форматы пар асимметричных ключей

Ключевые пары RSA, используемые для расчёта подписей, **должны** иметь 2048-битовый модуль (modulus) и показатель (public exponent - e) 65537.

3.1. Формат открытых ключей

Открытый ключ субъекта помещается в структуру subjectPublicKeyInfo [RFC5280], имеющую два поля - algorithm и subjectPublicKey. Назначение этих полей и их структура описаны ниже.

algorithm (имеет тип AlgorithmIdentifier)
: В поле algorithm **должен** использоваться идентификатор для RSA PKCS #1 v1.5 с SHA-256 как указано в разделе 5 [RFC4055]. Значение для связанных параметров **должно** использоваться для поля parameters.

subjectPublicKey
: Для кодирования поля subjectPublicKey в сертификате **должна** использоваться структура RSAPublicKey как указано в [RFC4055].

3.2. Формат секретных ключей

Формат секретного ключа определяется локальной политикой.

4. Формат подписи

Структура поля signature для сертификата описана в параграфе 1.2 [RFC4055]. Структура поля signature в SignerInfos объектов CMS SignedData описана в [RFC5652].

5. Дополнительные требования

Предполагается, что RPKI потребует принятия обновлённых размеров ключей и другого набора ключей и алгоритмов хэширования по истечении времени с целью обеспечения приемлемого уровня криптографической защиты для обеспечения целостности подписанной продукции в RPKI. В этом случае данный профиль следует заменить новыми документами, соответствующими новым требованиям безопасности.

Процедуры перехода к новым размерам ключей и алгоритмам описаны в [RFC6916].

---

[1] Certificate Policy.
[2] Object Identifier - идентификатор объекта.
[3] Certificate Request Message Format - формат сообщений с запросом сертификата.

6. Вопросы безопасности

Одноимённые разделы [RFC4055], [RFC5280] и [RFC6487] применимы к сертификатам и CRL. Такие же разделы [RFC2986], [RFC4211] и [RFC6487] применимы к запросам сертификатов. Аналогичный раздел [RFC5754] применим для подписанных объектов CMS. Данная спецификация не вносит новых проблем безопасности.

7. Отличия от RFC 6485

Это обновление включает незначительные технические обновления [RFC6485], которые не считаются связанными ошибками. В процессе обновления также были учтены замеченные ошибки и внесены разные поправки.

В разделе 2 [RFC6485] значение sha256WithRSAEncryption указано в качестве OID для использования в поле SignerInfo signatureAlgorithm подписанных объектов CMS (SignedObjects). Однако имеющиеся реализации используют для этого поля rsaEncryption OID (поддержка rsaEncryption в сторонних криптографических библиотеках лучше, нежели для sha256WithRSAEncryption возможно в результате того, что в [RFC3370] поддержка rsaEncryption указана обязательной, а поддержка OID для RSA и алгоритма подписи совместно - опциональной).

Вместо того, чтобы требовать от имеющихся реализаций перехода на sha256WithRSAEncryption, данный документ изменён с учётом сложившейся практики. Это не меняет криптографический алгоритм, а меняет лишь идентификатор (в отличие от сертификатов, CRL и запросов сертификатов, подписанные объекты CMS имеют отдельное поле для идентификатора алгоритма хэширования и это поле должно содержать id-sha256 OID в соответствии с разделом 2).

Для предотвращения проблем совместимости от RP по прежнему требуется воспринимать идентификаторы sha256WithRSAEncryption, если они встречаются.

Другие изменения перечислены ниже.

- Исправлены опечатки и внесены незначительные редакторские правки.
- Исправлены ссылки ([RFC5652] взамен [RFC3370], [RFC3447] взамен [RFC4055]).
- Добавлены ссылки во Введение.
- Внесена корректировка для поля CRMF POPOSigningKey в разделе 2 (algorithmIdentifier вместо signature).
- Добавлены запросы сертификатов в упоминания сертификатов, CRL и подписанных объектов CMS.
- Заменён текст в разделе 5 с указанием процедуры, определённой в [RFC6916] (смена алгоритма).
- Слова «подписанный объект» заменены повсюду словами «подписанный объект CMS».

8. Литература

8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <http://www.rfc-editor.org/info/rfc2986>.

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, DOI 10.17487/RFC3370, August 2002, <http://www.rfc-editor.org/info/rfc3370>.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, DOI 10.17487/RFC3447, February 2003, <http://www.rfc-editor.org/info/rfc3447>.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, DOI 10.17487/RFC4055, June 2005, <http://www.rfc-editor.org/info/rfc4055>.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, DOI 10.17487/RFC4211, September 2005, <http://www.rfc-editor.org/info/rfc4211>.

[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, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <http://www.rfc-editor.org/info/rfc5652>.

[RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", RFC 5754, DOI 10.17487/RFC5754, January 2010, <http://www.rfc-editor.org/info/rfc5754>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <http://www.rfc-editor.org/info/rfc6480>.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, DOI 10.17487/RFC6484, February 2012, <http://www.rfc-editor.org/info/rfc6484>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <http://www.rfc-editor.org/info/rfc6487>.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, DOI 10.17487/RFC6488, February 2012, <http://www.rfc-editor.org/info/rfc6488>.

[SHS] National Institute of Standards and Technology (NIST), "FIPS Publication 180-3: Secure Hash Standard", FIPS Publication 180-3, October 2008.

8.2. Дополнительная литература

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <http://www.rfc-editor.org/info/rfc6482>.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, DOI 10.17487/RFC6485, February 2012, <http://www.rfc-editor.org/info/rfc6485>.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012, <http://www.rfc-editor.org/info/rfc6486>.

[RFC6916] Gagliano, R., Kent, S., and S. Turner, "Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)", BCP 182, RFC 6916, DOI 10.17487/RFC6916, April 2013, <http://www.rfc-editor.org/info/rfc6916>.

Благодарности

Авторы подтверждают использование в этом документе материалов, содержащихся в черновых вариантах документов RPKI Certificate Policy [RFC6484] и профиля сертификатов ресурсов [RFC6487]. Спасибо соавторам этих двух документов, а именно, - Stephen Kent, Derrick Kong, Karen Seo, Ronald Watro, George Michaelson и Robert Loomans. Указанные в этом документе ограничения для размеров ключей взяты из комментариев Stephen Kent и рецензии David Cooper. Дополнительную рецензию для этого документа предоставил Sean Turner.

Andrew Chi и David Mandelberg обнаружили проблему, рассмотренную в этой замене документа [RFC6485]. Изменения включают также результаты дискуссии между Rob Austein и Matt Lepinski в списке рассылки рабочей группы SIDR. Richard Hansen внес множество предложений, включенных в этот документ.

Адреса авторов

Geoff Huston

APNIC

Email: gih@apnic.net

George Michaelson (редактор)

APNIC

Email: ggm@apnic.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru