Internet Engineering Task Force (IETF)
Request for Comments: 5933
Category: Standards Track
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Chuprina
I. Ustinov
Cryptocom Ltd.

July 2010

Использование алгоритмов электронной подписи ГОСТ в записях DNSKEY и RRSIG для DNSSEC

Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC

Аннотация

В этом документе описано создание цифровых подписей и хэш-значений с использованием алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 для записей DNSKEY, RRSIG и DS в защитных расширениях системы доменных имен (DNSSEC[1]).

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[2] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[3]. 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/rfc5933.

Оглавление

1. Введение

Система доменных имен (DNS[4]) представляет собой глобальную, иерархическую распределенную базу данных об именах Internet. Система DNS была расширена для использования криптографических ключей и цифровых подписей с целью проверки подлинности и целостности данных. RFC 4033 [RFC4033], RFC 4034 [RFC4034] и RFC 4035 [RFC4035] описывают эти защитные расширения DNS, называемые DNSSEC[5].

[1]Domain Name System Security Extensions.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[4]Domain Name System.
[5]DNS Security.

В RFC 4034 описано размещение записей DNSKEY и RRSIG, а также указан список криптографических алгоритмов для применения в DNSSEC. Этот документ расширяет указанный список, алгоритмами подписи и хэширования ГОСТ Р 34.10-2001 ([GOST3410], [RFC5832]) и ГОСТ Р 34.11-94 ([GOST3411], [RFC5831]), а также задаёт размещение записей DNSKEY и способ создания записей RRSIG с использованием этих алгоритмов.

Предполагается знакомство читателя с DNSSEC и алгоритмами хеширования и подписи GOST, упомянутыми в этом документе.

Термин ГОСТ не определён официально, но обычно применяется для обозначения российских криптографических алгоритмов ГОСТ Р 34.10-2001 [RFC5832], ГОСТ Р 34.11-94 [RFC5831] и ГОСТ 28147-89 [RFC5830]. Поскольку ГОСТ 28147-89 не используется в DNSSEC, в данном документе термин ГОСТ служит для обозначения только алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94.

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), возможно (MAY), необязательно (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

2. Записи DNSKEY

Формат DNSKEY RR определён в RFC 4034 [RFC4034].

Открытые ключи ГОСТ Р 34.10-2001 указываются с номером алгоритма 12.

Формат передачи открытых ключей совместим с RFC 4491 [RFC4491]:

Согласно [GOST3410] и [RFC5832], открытый ключ является точкой на эллиптической кривой Q = (x,y).

Представление открытого ключа при передаче **должно** содержать 64 октета, из которых первые 32 задают значение x в формате little-endian, а вторые 32 октета - значение y в таком же формате.

Соответствующие параметры открытых ключей идентифицируются значением id-GostR3410-2001-CryptoPro-A-ParamSet (1.2.643.2.2.35.1) [RFC4357], а параметры дайджеста (отпечатка) - id-GostR3411-94-CryptoProParamSet (1.2.643.2.2.30.1) [RFC4357].

2.1. Использование открытого ключа с имеющимися криптобиблиотеками

На момент подготовки этого документа существующие криптографические библиотеки с поддержкой ГОСТ были способные читать открытые ключи ГОСТ с помощью базового интерфейса X509 API, если ключ представлен в соответствии с параграфом 2.3.2 RFC 4491 [RFC4491].

Для использования этого представления из формата передачи открытого ключа ГОСТ с параметрами, применяемыми в этом документе, перед 64 октетами данных ключа добавляется приведённая ниже 37-байтовая последовательность.

```
0x30 0x63 0x30 0x1c 0x06 0x06 0x2a 0x85 0x03 0x02 0x02 0x13 0x30
0x12 0x06 0x07 0x2a 0x85 0x03 0x02 0x02 0x23 0x01 0x06 0x07 0x2a
0x85 0x03 0x02 0x02 0x1e 0x01 0x03 0x43 0x00 0x04 0x40
```

2.2. Пример DNSKEY RR

Если секретный ключ имеет значение (поле GostAsn1 разделено на 2 строки для удобства, в реальном ключе оно записывается одной строкой)

```
Private-key-format: v1.2
Algorithm: 12 (ECC-GOST)
GostAsn1: MEUCAQAwHAYGKoUDAgITMBIGByqFAwICIwEGByqFAwICHgEEIgQg/9M
          iXtXKg9FDXDN/R9CmVhJDyuzRAIgh4tPwCu4NHIs=
```

Запись DNSKEY RR с ключом зоны DNS для example.net будет иметь вид

```
example.net. 86400 IN DNSKEY 256 3 12 (
                            aRS/DcPWGQj2wVJydT8EcAVoC0kXn5pDVm2I
                            MvDDPXeD32dsSKcmq8KNVzigjL4OXZTV+t/6
                            w4X1gpNrZiC01g==
                            ) ; key id = 59732
```

3. Записи RRSIG

Значение поля подписи в RRSIG RR следует RFC 4490 [RFC4490] и рассчитывается, как показано ниже. Значения полей RDATA, предшествующих данным подписи, указаны в RFC 4034 [RFC4034].

```
hash = GOSTR3411(data)
```

где параметр data представляет собой формат передачи подписываемого набора записей, как указано в RFC 4034 [RFC4034].

Хэш-значение **должно** рассчитываться с параметрами ГОСТ Р 34.11-94, идентифицируемыми набором id-GostR3411-94-CryptoProParamSet [RFC4357].

Подпись рассчитывается из хэш-значения в соответствии со стандартом ГОСТ Р 34.10-2001, а формат её передачи соответствует RFC 4490 [RFC4490].

Цитата из RFC 4490:

> Алгоритм цифровой подписи ГОСТ Р 34.10-2001 создаёт подпись в виде двух 256-битовых чисел r и s. Её представление в форме строки октетов включает 64, из которых первые 32 содержат представление s в формате big-endian, а вторые 32 - представление r в том же формате.

3.1. Пример RRSIG RR

С помощью секретного ключа, указанного в параграфе 2.2, подписывается приведённый ниже набор RRSet, состоящий из записи A

```
www.example.net. 3600 IN A 192.0.2.1
```

При установке даты заполнения 2000-01-01 00:00:00 UTC и срока окончания 2030-01-01 00:00:00 UTC приведённая ниже запись RR будет корректной.

```
www.example.net. 3600 IN RRSIG A 12 3 3600 20300101000000 (
                                20000101000000 59732 example.net.
                                7vzzz6iLOmvtjs5FjVjSHT8XnRKFY15ki6Kp
                                kNPkUnS8iIns0Kv4APT+D9ibmHhGri6Sfbyy
                                zi67+wBbbW/jrA== )
```

Примечание. Алгоритм подписи ECC-GOST использует случайные данные, поэтому рассчитанное реально значение подписи будет отличаться от приведённого здесь.

4. Записи DS

Алгоритм цифровой подписи ГОСТ Р 34.11-94 обозначается в записях DS RR типом 3. Формат передачи значения подписи совместим с RFC 4490 [RFC4490], т. е., подпись использует представление little-endian.

Подпись всегда **должна** рассчитываться с параметрами ГОСТ Р 34.11-94, заданными набором id-GostR3411-94-CryptoProParamSet [RFC4357].

4.1. Пример DS RR

Для ключа подписывания ключей (KSK[1])

```
example.net. 86400   DNSKEY  257 3 12 (
                              LMgXRHzSbIJGn6i16K+sDjaDf/k1o9DbxScO
                              gEYqYS/rlh2Mf+BRAY3QHPbwoPh2fkDKBroF
                              SRGR7ZYcx+YIQw==
                              ) ; key id = 40692
```

Запись DS RR будет иметь вид

```
example.net. 3600 IN DS 40692 12 3 (
          22261A8B0E0D799183E35E24E2AD6BB58533CBA7E3B14D659E9CA09B
          2071398F )
```

5. Вопросы развёртывания

5.1. Размеры ключей

В соответствии с RFC 4357 [RFC4357] размер открытых ключей **должен** быть равен 512 битам.

5.2. Размеры подписей

В соответствии со спецификацией алгоритма цифровой подписи ГОСТ Р 34.10-2001 ([GOST3410], [RFC5832]) размер подписи составляет 512 битов.

5.3. Размеры дайджестов

В соответствии с ГОСТ Р 34.11-94 ([GOST3411], [RFC5831]) размер дайджеста (подписи) составляет 256 битов.

6. Вопросы реализации

6.1. Поддержка подписей ГОСТ

Осведомленные о DNSSEC реализации могут поддерживать записи RRSIG и DNSKEY, созданные с использованием алгоритмов ГОСТ, как описано в этом документе.

6.2. Поддержка NSEC3 Denial of Existence

Все реализации DNSSEC-GOST **должны** поддерживать NSEC [RFC4035] и NSEC3 [RFC5155].

7. Вопросы безопасности

В настоящее время криптостойкость алгоритма цифровой подписи ГОСТ Р 34.10-2001 оценивается в 2^{128} операций расчёта множества точек эллиптических кривых для модуля в виде простого числа порядка 2^{256}.

В настоящее время криптостойкость алгоритма ГОСТ Р 34.11-94 оценивается в 2^{128} операций расчёта хэш-функции (известен метод снижения этого значения примерно до 2^{105} операций, но он не пригоден для практического применения, поскольку требует создания конфликта с заполнением 1024 случайными блоками по 256 битов каждый).

8. Взаимодействие с IANA

Этот документ обновляет реестр IANA DNS Security Algorithm Numbers [RFC4034], добавляя в него приведённое в таблице значение.

Значение	*Алгоритм*	*Обозначение*	*Подпись зон*	*Защита транзакций*	*Документ*	*Статус*
12	GOST R 34.10-2001	ECC-GOST	+	*	RFC 5933	OPTIONAL

Этот документ обновляет реестр RFC 4034 Digest Types ([RFC4034], параграф A.2), добавляя в него значение и статус для алгоритма ГОСТ Р 34.11-94.

[1]Key Signing Key.

Значение	Алгоритм	Статус
3	GOST R 34.11-94	OPTIONAL

9. Благодарности

Этот документ является незначительным дополнением к RFC 4034 [RFC4034]. Для согласованности авторы пытались следовать RFC 3110 [RFC3110], RFC 4509 [RFC4509] и RFC 4357 [RFC4357]. Авторам и участникам этих работ выражается признательность за хорошо выполненную работу.

Помощь в работе над документом оказали также комментарии и предложения Dmitry Burkov, Jaap Akkerhuis, Olafur Gundmundsson, Jelte Jansen и Wouter Wijngaards.

10. Литература

10.1. Нормативные документы

[GOST3410] «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.», ГОСТ Р 34.10-2001, Государственный стандарт Российской Федерации, Госстандарт России, 2001.

[GOST3411] «Информационная технология. Криптографическая защита информации. Функция хеширования.», ГОСТ Р 34.11-94, Государственный стандарт Российской Федерации, Госстандарт России, 1994.

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

[RFC3110] Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4357] Popov, V., Kurepkin, I., and S. Leontiev, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms", RFC 4357, January 2006.

[RFC4490] Leontiev, S., Ed. and G. Chudov, Ed., "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)", RFC 4490, May 2006.

[RFC4491] Leontiev, S., Ed. and D. Shefanovski, Ed., "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 4491, May 2006.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

10.2. Дополнительная литература

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

[RFC5830] Dolmatov, V., Ed., "GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms", RFC 5830, March 2010.

[RFC5831] Dolmatov, V., Ed., "GOST R 34.11-94: Hash Function Algorithm", RFC 5831, March 2010.

[RFC5832] Dolmatov, V., Ed., "GOST R 34.10-2001: Digital Signature Algorithm", RFC 5832, March 2010.

Адреса авторов

Vasily Dolmatov (редактор)
Cryptocom Ltd.
14/2, Kedrova St.
Moscow, 117218
Russian Federation
Phone: +7 499 124 6226
EMail: dol@cryptocom.ru

Artem Chuprina
Cryptocom Ltd.
14/2, Kedrova St.
Moscow, 117218
Russian Federation
Phone: +7 499 124 6226
EMail: ran@cryptocom.ru

Igor Ustinov
Cryptocom Ltd.
14/2, Kedrova St.
Moscow, 117218
Russian Federation
Phone: +7 499 124 6226
EMail: igus@cryptocom.ru

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru