Internet Engineering Task Force (IETF)
Request for Comments: 8080
Category: Standards Track
ISSN: 2070-1721

O. Sury
CZ.NIC
R. Edmonds
Fastly

February 2017

Алгоритм EdDSA для DNSSEC

Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC

Аннотация

В этом документе описано, как задать ключи и подписи EdDSA[1] для защиты DNS (DNSSEC[2]). Алгоритм EdDSA может применяться с кривыми Ed25519 и Ed448.

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[3] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[4]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 7841.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc8080.

Оглавление

1. Введение

Механизмы DNSSEC, описанные в [RFC4033], [RFC4034] и [RFC4035], используют криптографические ключи и цифровые подписи для проверки подлинности данных DNS. В настоящее время наиболее популярным алгоритмом защиты является RSA. Стандартизована также заданная GOST [RFC5933] и NIST криптография на основе эллиптических кривых [RFC6605].

В [RFC8032] описана система подписи на основе эллиптических кривых (EdDSA) и рекомендованы две кривые - Ed25519 и Ed448.

В этом документе определяется использование в DNSSEC записей о ресурсах (RR[5]) DS, DNSKEY и RRSIG с новым алгоритмом подписи EdDSA и предложены на выбор две кривые - Ed25519 и Ed448.

[1]Edwards-curve Digital Security Algorithm.
[2]DNS Security.
[3]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[5]Resource record.

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

3. Записи DNSKEY

Открытый ключ Ed25519 представляет собой 32-октетное значение, помещаемое в поле Public Key записей DNSKEY в форме простой битовой строки. Генерация открытого ключа описана в параграфе 5.1.5 [RFC8032].

Открытый ключ Ed448 представляет собой 57-октетное значение, помещаемое в поле Public Key записей DNSKEY в форме простой битовой строки. Генерация открытого ключа описана в параграфе 5.1.5 [RFC8032].

4. Записи RRSIG

Подпись Ed25519 представляет собой 64-октетное значение, помещаемое в поле Signature записей RRSIG в форме простой битовой строки. Алгоритм и проверка подписи Ed25519 описаны в параграфах 5.1.6 и 5.1.7 [RFC8032], соответственно.

Подпись Ed448 представляет собой 114-октетное значение, помещаемое в поле Signature записей RRSIG в форме простой битовой строки. Алгоритм и проверка подписи Ed448 писаны в параграфах 5.1.6 и 5.1.7 [RFC8032], соответственно.

5. Номер алгоритма для записей DS, DNSKEY и RRSIG

Для алгоритма Ed25519 в записях DS, DNSKEY и RRSIG выделен номер 15. Для алгоритма Ed448 в записях DS, DNSKEY и RRSIG выделен номер 16. Эта регистрация полностью определена в разделе «Согласование с IANA».

6. Примеры

6.1. Примеры Ed25519

```
Private-key-format: v1.2
Algorithm: 15 (ED25519)
PrivateKey: ODIyNjAzODQ2MjgwODAxMjI2NDUxOTAyMDQxNDIyNjI=

example.com. 3600 IN DNSKEY 257 3 15 (
             l02Woi0iS8Aa25FQkUd9RMzZHJpBoRQwAQEX1SxZJA4= )

example.com. 3600 IN DS 3613 15 2 (
             3aa5ab37efce57f737fc1627013fee07bdf241bd10f3b1964ab55c78e79
             a304b )

example.com. 3600 IN MX 10 mail.example.com.

example.com. 3600 IN RRSIG MX 3 3600 (
             1440021600 1438207200 3613 example.com. (
             Edk+IB9KNNWg0HAjm7FazXyrd5m3Rk8zNZbvNpAcM+eysqcUOMIjWoevFkj
             H5GaMWeG96GUVZu6ECKOQmemHDg== )

Private-key-format: v1.2
Algorithm: 15 (ED25519)
PrivateKey: DSSF3o0s0f+ElWzj9E/Osxw8hLpk55chkmx0LYN5WiY=

example.com. 3600 IN DNSKEY 257 3 15 (
             zPnZ/QwEe7S8C5SPz2OfS5RR40ATk2/rYnE9xHIEijs= )

example.com. 3600 IN DS 35217 15 2 (
             401781b934e392de492ec77ae2e15d70f6575a1c0bc59c5275c04ebe80c
             6614c )

example.com. 3600 IN MX 10 mail.example.com.

example.com. 3600 IN RRSIG MX 3 3600 (
             1440021600 1438207200 35217 example.com. (
             5LL2obmzdqjWI+Xto5eP5adXt/T5tMhasWvwcyW4L3SzfcRawOle9bodhC+
             oip9ayUGjY9T/rL4rN3bOuESGDA== )
```

6.2. Примеры Ed448

```
Private-key-format: v1.2
Algorithm: 16 (ED448)
PrivateKey: xZ+5Cgm463xugtkY5B0Jx6erFTXp13rYegst0qRtNsOYnaVpMx0Z/c5EiA9x
            8wWbDDct/U3FhYWA

example.com. 3600 IN DNSKEY 257 3 16 (
             3kgROaDjrh0H2iuixWBrc8g2EpBBLCdGzHmn+G2MpTPhpj/OiBVHHSfPodx
             1FYYUcJKm1MDpJtIA )

example.com. 3600 IN DS 9713 16 2 (
             6ccf18d5bc5d7fc2fceb1d59d17321402f2aa8d368048db93dd811f5cb2
             b19c7 )

example.com. 3600 IN MX 10 mail.example.com.
```

```
example.com. 3600 IN RRSIG MX 3 3600 (
             1440021600 1438207200 9713 example.com. (
             Nmc0rgGKpr3GKYXcB1JmqqS4NYwhmechvJTqVzt3jR+Qy/lSLFoIk1L+9e3
             9GPL+5tVzDPN3f9kAwiu8KCuPPjtl227ayaCZtRKZuJax7n9NuYlZJIusX0
             SOIOKBGzG+yWYtz1/jjbzl5GGkWvREUCUA )

Private-key-format: v1.2
Algorithm: 16 (ED448)
PrivateKey: WEykD3ht3MHkU8iH4uVOLz8JLwtRBSqiBoM6fF72+Mrp/u5gjxuB1DV6NnPO
            2BlZdz4hdSTkOdOA

example.com. 3600 IN DNSKEY 257 3 16 (
             kkreGWoccSDmUBGAe7+zsbG6ZAFQp+syPmYUurBRQc3tDjeMCJcVMRDmgcN
             Lp5HlHAMy12VoISsA )

example.com. 3600 IN DS 38353 16 2 (
             645ff078b3568f5852b70cb60e8e696cc77b75bfaaffc118cf79cbda1ba
             28af4 )

example.com. 3600 IN MX 10 mail.example.com.

example.com. 3600 IN RRSIG MX 3 3600 (
             1440021600 1438207200 38353 example.com. (
             +JjANio/LIzp7osmMYE5XD3H/YES8kXs5Vb9H8MjPS8OAGZMD37+LsCIcjg
             5ivt0d4Om/UaqETEAsJjaYe56CEQP5lhRWuD2ivBqE0zfwJTyp4WqvpULbp
             vaukswvv/WNEFxzEYQEIm9+xDlXj4pMAMA )
```

7. Согласование с IANA

Этот документ обновляет реестр IANA Domain Name System Security (DNSSEC) Algorithm Numbers. В реестр добавляются две записи, показанные в таблице.

Номер	15	16
Описание	Ed25519	Ed448
Обозначение	ED25519	ED448
Подпись зоны	+	+
Защита транзакций	*	*
Документ	RFC 8080	RFC 8080

** Стандартизация использования этого алгоритма для защиты транзакций не определена*

8. Вопросы безопасности

Вопросы безопасности, рассмотренные в [RFC8032] и [RFC7748], сохраняются для использования алгоритмов Ed25519 и Ed448 в DNSSEC.

Алгоритм Ed25519 предназначен для работы с уровнем защиты 128 битов, Ed448 — с уровнем защиты 224 бита. Взломать такую защиту способны достаточно большие квантовые компьютеры. Разумные оценки возможностей традиционных компьютеров говорят о полной безопасности Ed25519. Алгоритм Ed448 предназначен для приложений, где требования к производительности менее высоки и имеется желание обеспечить защиту от аналитических атак на эллиптические кривые.

Эти оценки, естественно, могут измениться в будущем, если новые атаки станут более совершенными по сравнению с известными сегодня.

Секретный ключ, используемый для зоны DNSSEC, **недопустимо** применять для каких-либо других целей. Иначе станут возможными кросс-протокольные и кросс-программные атаки.

9. Литература

9.1. 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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <http://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <http://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <http://www.rfc-editor.org/info/rfc8032>.

9.2. Дополнительная литература

[RFC5933] Dolmatov, V., Ed., Chuprina, A., and I. Ustinov, "Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5933, DOI 10.17487/RFC5933, July 2010, <http://www.rfc-editor.org/info/rfc5933>.

[RFC6605] Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <http://www.rfc-editor.org/info/rfc6605>.

Благодарности

Часть материалов этого документа заимствована из [RFC6605].

Авторы документа выражают благодарность Jan Vcelak, Pieter Lexis, Kees Monshouwer, Simon Josefsson, Paul Hoffman и другим за рецензирование этого документа.

Адреса авторов

Ondrej Sury

CZ.NIC

Milesovska 1136/5

Praha 130 00

Czech Republic

Email: ondrej.sury@nic.cz

Robert Edmonds

Fastly

Atlanta, Georgia

United States of America

Email: edmonds@mycre.ws

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru