Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: June 20, 2017

O. Sury
CZ.NIC
R. Edmonds
Fastly

December 17, 2016

EdDSA for DNSSEC
draft-ietf-curdle-dnskey-eddsa-03

Abstract

This document describes how to specify EdDSA keys and signatures in DNS Security (DNSSEC). It uses the Edwards-curve Digital Security Algorithm (EdDSA) with the choice of two curves, Ed25519 and Ed448.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

DNSSEC, which is broadly defined in [RFC4033], [RFC4034], and [RFC4035], uses cryptographic keys and digital signatures to provide authentication of DNS data. Currently, the most popular signature algorithm in use is RSA. GOST ([RFC5933]) and NIST-specified elliptic curve cryptography ([RFC6605]) are also standardized.

[I-D.irtf-cfrg-eddsa] describes the elliptic curve signature system EdDSA and recommends two curves, Ed25519 and Ed448.

This document defines the use of DNSSEC's DS, DNSKEY, and RRSIG resource records (RRs) with a new signing algorithm, Edwards-curve Digital Signature Algorithm (EdDSA) using a choice of two instances: Ed25519 and Ed448.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. DNSKEY Resource Records

An Ed25519 public key consists of a 32-octet value, which is encoded into the Public Key field of a DNSKEY resource record as a simple bit string. The generation of a public key is defined in Section 5.1.5 in [I-D.irtf-cfrg-eddsa].

An Ed448 public key consists of a 57-octet value, which is encoded into the Public Key field of a DNSKEY resource record as a simple bit string. The generation of a public key is defined in Section 5.2.5 in [I-D.irtf-cfrg-eddsa].

4. RRSIG Resource Records

An Ed25519 signature consists of a 64-octet value, which is encoded into the Signature field of an RRSIG resource record as a simple bit string. The Ed25519 signature algorithm is described in Section 5.1.6 and verification of the Ed25519 signature is described in Section 5.1.7 in [I-D.irtf-cfrg-eddsa].

An Ed448 signature consists of a 114-octet value, which is encoded into the Signature field of an RRSIG resource record as a simple bit string. The Ed448 signature algorithm is described in Section 5.2.6 and verification of the Ed448 signature is described in Section 5.2.7 in [I-D.irtf-cfrg-eddsa].

5. Algorithm Number for DS, DNSKEY and RRSIG Resource Records

The algorithm number associated with the use of Ed25519 in DS, DNSKEY and RRSIG resource records is TBD1. The algorithm number associated with the use of Ed448 in DS, DNSKEY and RRSIG resource records is TBD2. This registration is fully defined in the IANA Considerations section.

6. Examples

6.1. Ed25519 Examples

This section needs an update after the algorithm number for Ed25519 is assigned.

```
Private-key-format: v1.2
Algorithm: TBD1 (ED25519)
PrivateKey: ODIyNjAzODQ2MjgwODAxMjI2NDUxOTAyMDQxNDIyNjI=

example.com. 3600 IN DNSKEY 257 3 TBD1 (
             l02Woi0iS8Aa25FQkUd9RMzZHJpBoRQwAQEX1SxZJA4= )

example.com. 3600 IN DS 3613 TBD1 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== )
```

This section needs an update after the algorithm number for Ed25519 is assigned.

```
Private-key-format: v1.2
Algorithm: TBD1 (ED25519)
PrivateKey: DSSF3o0s0f+ElWzj9E/Osxw8hLpk55chkmx0LYN5WiY=

example.com. 3600 IN DNSKEY 257 3 TBD1 (
             zPnZ/QwEe7S8C5SPz2OfS5RR40ATk2/rYnE9xHIEijs= )

example.com. 3600 IN DS 35217 TBD1 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. Ed448 Examples

This section needs an update after the algorithm number for Ed448 is assigned.

```
Private-key-format: v1.2
Algorithm: TBD2 (ED448)
PrivateKey: xZ+5Cgm463xugtkY5B0Jx6erFTXp13rYegst0qRtNsOYnaVpMx0Z/c5EiA9x
            8wWbDDct/U3FhYWA

example.com. 3600 IN DNSKEY 257 3 TBD2 (
             3kgROaDjrh0H2iuixWBrc8g2EpBBLCdGzHmn+G2MpTPhpj/OiBVHHSfPodx
             1FYYUcJKm1MDpJtIA )

example.com. 3600 IN DS 9713 TBD2 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 )
```

This section needs an update after the algorithm number for Ed448 is assigned.

```
Private-key-format: v1.2
Algorithm: TBD2 (ED448)
PrivateKey: WEykD3ht3MHkU8iH4uVOLz8JLwtRBSqiBoM6fF72+Mrp/u5gjxuB1DV6NnPO
            2BlZdz4hdSTkOdOA

example.com. 3600 IN DNSKEY 257 3 TBD2 (
             kkreGWoccSDmUBGAe7+zsbG6ZAFQp+syPmYUurBRQc3tDjeMCJcVMRDmgcN
             Lp5HlHAMy12VoISsA )

example.com. 3600 IN DS 38353 TBD2 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. Acknowledgements

Some of the material in this document is copied liberally from [RFC6605].

The authors of this document wish to thank Jan Vcelak, Pieter Lexis, Kees Monshouwer, Simon Josefsson, Paul Hoffman and others for a review of this document.

8. IANA Considerations

This document updates the IANA registry "Domain Name System Security (DNSSEC) Algorithm Numbers". The following entries have been added to the registry:

Number	TBD1	TBD2
Description	Ed25519	Ed448
Mnemonic	ED25519	ED448
Zone Signing	Y	Y
Trans. Sec.	*	*
Reference	This document	This document

* There has been no determination of standardization of the use of this algorithm with Transaction Security.

9. Security Considerations

The security considerations of [I-D.irtf-cfrg-eddsa] and [RFC7748]are inherited in the usage of Ed25519 and Ed448 in DNSSEC.

Ed25519 is intended to operate at around the 128-bit security level, and Ed448 at around the 224-bit security level. A sufficiently large quantum computer would be able to break both. Reasonable projections of the abilities of classical computers conclude that Ed25519 is perfectly safe. Ed448 is provided for those applications with relaxed performance requirements and where there is a desire to hedge against analytical attacks on elliptic curves.

These assessments could, of course, change in the future if new attacks that work better than the ones known today are found.

A private key used for a DNSSEC zone MUST NOT be used for any other purpose than for that zone. Otherwise cross-protocol or cross-application attacks are possible.

10. References

10.1. Normative References

[I-D.irtf-cfrg-eddsa]
Josefsson, S. and I. Liusvaara, "Edwards-curve Digital Signature Algorithm (EdDSA)", draft-irtf-cfrg-eddsa-08 (work in progress), August 2016.

[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>.

10.2. Informative References

[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>.

Authors' Addresses

Ondrej Sury
CZ.NIC
Milesovska 1136/5
Praha 130 00
CZ

Email: ondrej.sury@nic.cz

Robert Edmonds
Fastly
Atlanta, Georgia
US

Email: edmonds@mycre.ws