Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: February 26, 2016

O. Sury
CZ.NIC

August 25, 2015

Ed25519 and Ed448 for DNSSEC
draft-sury-dnskey-ed25519-02

Abstract

This document describes how to specify Ed25519 and Ed448 keys and signatures in DNS Security (DNSSEC). It uses the Ed25519 and Ed448 curve and the SHA-512 for signatures.

Status of This Memo

This Internet-Draft will expire on February 26, 2016.

Copyright Notice

Table of Contents

1. Introduction

DNSSEC, which is broadly defined in RFCs 4033 [RFC4033], 4034 [RFC4034], and 4035 [RFC4035], uses cryptographic keys and digital signatures to provide authentication of DNS data. Currently, the most popular signature algorithm is RSA. RFC 6605 [RFC6605] defines usage of Elliptic Curve Digital Signature Algorithm (ECDSA) for DNSSEC with curve P-256 and SHA-256, and ECDSA with curve P-384 and SHA-384.

This document defines the DNSKEY and RRSIG resource records (RRs) of two new signing algorithm:

Curve Ed25519 and SHA-512.

Curve Ed448 and SHA-512.

A description of both curves can be found in Elliptic Curves for Security [I-D.irtf-cfrg-curves]. A more thorough description of Ed25519 can be found in EdDSA and Ed25519 [I-D.josefsson-eddsa-ed25519].)

Ed25519 is targeted to provide attack resistance comparable to quality 128-bit symmetric ciphers that is equivalent strength of RSA with 3072-bit keys. Public keys are 256 bits (32 bytes) in length and signatures are 512 bits (64 bytes).

Ed448 is targeted to provide attack resistance comparable to quality 224-bit symmetric ciphers that is equivalent strength of RSA with

~12448-bit keys. However only RSA with 4096-bit keys is defined for use in DNSSEC, so we are going to use RSA-4096 in comparisons below. Ed448 public keys are 448 bits (56 bytes) in length and signatures are 896 bits (112-bytes). The curve is meant as a more conservative alternative to Ed25519.

Using the Ed25519 and Ed448 curve in DNSSEC has some advantages and disadvantage relative to using RSA. The Ed25519 and Ed448 keys are much shorter than RSA keys; at the comparable size, the difference is 256 versus 3072 bits for the Ed25519 and 448 versus 4096 bits for the Ed448. The Ed25519 and Ed448 signatures are also much shorter than RSA keys; at the comparable size, the difference is 512 versus 3072 bits for the Ed25519 and 896 versus 4096 bits for the Ed448. This is relevant because DNSSEC stores and transmits both keys and signatures.

Signing with Ed25519 and Ed448 is significantly faster than with equivalently strong RSA, it is also faster than existing ECDSA curves in DNSSEC defined in RFC 6605 [RFC6605]. However, validating RSA signatures is significantly faster than validating Ed25519 and Ed448 signatures.

1.1. 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 RFC 2119 [RFC2119].

2. DNSKEY and RRSIG Resource Records for Ed25519 and Ed448

2.1. Public Keys

The Ed25519 public keys consist of a 32-byte value that represents encoding of the curve point. The generation of public key is defined Chapter 5.5 in I-D.josefsson-eddsa-ed25519 [I-D.josefsson-eddsa-ed25519].

The Ed448 public key consist of a 56-byte value that represents encoding of the curve point.

In DNSSEC keys, the Ed25519 and Ed448 public key is a simple bit string that represents uncompressed form of a curve point.

2.2. Signatures

The Ed25519 signature consists of a 64-byte value. The Ed25519 signature algorithm is described Chapter 5.6 in I-D.josefsson-eddsa-ed25519 [I-D.josefsson-eddsa-ed25519].

The Ed448 signature consists of a 112-byte value. In DNSSEC keys, the Ed448 signatures is a simple bit string that represents the Ed448 signature.

In DNSSEC keys, the Ed25519 and Ed448 signatures is a simple bit string that represents the signature.

2.3. Algorithm Numbers

The algorithm number associated with the DNSKEY and RRSIG resource records is fully defined in the IANA Considerations section. DNSKEY and RRSIG RRs signifying:

Ed25519 and SHA-512 use the algorithm number TBD1.

Ed448 and SHA-512 use the algorithm number TBD2.

3. Examples

3.1. Ed25519 Example

This section need an update after the algorithm for Ed25519 with SHA-512 is assigned.

```
Private-key-format: v1.2
Algorithm: TBD1 (ED25519SHA512)
PrivateKey: ODIyNjAzODQ2MjgwODAxMjI2NDUxOTAyMDQxNDIyNjI=
# coresponding to 82260384628080122645190204142262 INT

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

example.com. 3600 IN DS 3613 TBD 2 (
        3aa5ab37efce57f737fc1627013fee07bdf241bd10f3
        b1964ab55c78e79a304b )

www.example.com. 3600 IN A 192.0.2.1
www.example.com. 3600 IN RRSIG A TBD 3 3600 (
        20150820000000 20150730000000 3613 example.com.
        cvTRVrU7dwnemQuBq9/E4tlIiRpvWcEmYdzqs6SCQxw6
        qmczBBQGldssMx1TCJnwsEs9ZuA2phPzuJNoon9BCA== )
```

```
Private-key-format: v1.2
Algorithm: TBD1 (ED25519SHA512)
PrivateKey: DSSF3o0s0f+ElWzj9E/Osxw8hLpk55chkmx0LYN5WiY=

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

example.com. 3600 IN DS 55648 TBD 2 (
        96401675bc7ecdd541ec0f70d69238c7b95d3bd4de1e
        231a068ceb214d02a4ed )

www.example.com. 3600 IN A 192.0.2.1
www.example.com. 3600 IN RRSIG A TBD 3 3600 (
        20150820000000 20150730000000 35452 example.com.
        yuGb9rCNIuhDaRJbuhYHj89Y/3Pi8KWUm7lOt00ivVRGvgulmVX8DgpE
        AFyMP2MKXJrqYJr+ViiCIDwcOIbPAQ==)
```

3.2. Ed448 Example

[[TODO]]

4. Acknowledgements

Some of the material in this document is copied liberally from RFC 6605 [RFC6605].

The author of this document wants to thanks Pieter Lexis and Kees Monshouwer for a review of this document.

5. IANA Considerations

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

Number	TBD1
Description	Ed25519 with SHA-512
Mnemonic	Ed25519SHA512
Zone Signing	Y
Trans. Sec.	*
Reference	This document

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

Number	TBD2
Description	Ed448 with SHA-512
Mnemonic	Ed448SHA512
Zone Signing	Y
Trans. Sec.	*
Reference	This document

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

6. Security Considerations

Ed25519 is targeted to provide attack resistance comparable to quality 128-bit symmetric ciphers, and Ed448 is targeted to provide attack resistance comparable to quality 224-bit symmetric ciphers. Such an assessment could, of course, change in the future if new attacks that work better than the ones known today are found.

7. References

7.1. Normative References

[I-D.irtf-cfrg-curves]
Langley, A. and M. Hamburg, "Elliptic Curves for Security", draft-irtf-cfrg-curves-05 (work in progress), August 2015.

[I-D.josefsson-eddsa-ed25519]
Josefsson, S. and N. Moller, "EdDSA and Ed25519", draft-josefsson-eddsa-ed25519-03 (work in progress), May 2015.

[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>.

7.2. Informative References

[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>.

Author's Address

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

Phone: +420 222 745 111
Email: ondrej.sury@nic.cz