

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: March 11, 2016

O. Sury  
CZ.NIC  
R. Edmonds  
Farsight Security, Inc.  
September 8, 2015

**Ed448 for DNSSEC**  
**draft-sury-dnskey-ed448-00**

Abstract

This document describes how to specify Ed448 keys and signatures in DNS Security (DNSSEC). It uses the Ed448 instance of the Edwards-curve Digital Signature Algorithm (EdDSA) with the SHA-512 hash algorithm.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 11, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Requirements Language . . . . .	<a href="#">3</a>
<a href="#">3.</a>	DNSKEY and RRSIG Resource Records for Ed448 . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Examples . . . . .	<a href="#">3</a>
<a href="#">5.</a>	Acknowledgements . . . . .	<a href="#">4</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">7.</a>	Implementation Status . . . . .	<a href="#">5</a>
<a href="#">8.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">9.</a>	References . . . . .	<a href="#">6</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">6</a>
	Authors' Addresses . . . . .	<a href="#">7</a>

## [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. [[RFC5933](#)] and [[RFC6605](#)] later defined the use of GOST and NIST specified elliptic curve cryptography in DNSSEC.

This document defines the use of DNSSEC's DS, DNSKEY, and RRSIG resource records (RRs) with a new signing algorithm: the Ed448 instance of the Edwards-curve Digital Signature Algorithm (EdDSA) used with the SHA-512 hash algorithm. A more thorough description of Ed448 can be found in (TODO: Simon is going to add Ed448 to his draft) [[I-D.josefsson-eddsa-ed25519](#)].

Ed448 has a 224-bit security target, which is considered to be equivalent in strength to RSA with ~12000-bit keys. Ed448 public keys are 448 bits (56 bytes) long while signatures are 896 bits (112 bytes) long. The curve is meant as a more conservative alternative to Ed25519.

The usage of the Ed448 algorithm in DNSSEC has advantages and disadvantages relative to RSA. Ed448 keys are much shorter than RSA keys. At RSA-4096 strength that is the maximum defined for DNSSEC, Ed448 keys are 456 bytes smaller than RSA-4096 keys. Similarly, an Ed448 signature saves 400 bytes over an RSA-4096 signature.

However, DNSSEC with RSA is not commonly deployed on the Internet with signatures as large as 3072 bits. [[RFC6781](#)] contemplates the routine use of RSA-1024 and RSA-2048 in DNSSEC. Even when compared to the use of RSA at reduced strengths, Ed448 still provides smaller keys and signatures.



TODO - this is boilerplate :), we need to see the numbers. Signing with Ed448 is significantly faster than signing with equivalently strong RSA. However, the validation of RSA signatures is significantly faster than the validation of Ed448 signatures.

## **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 and RRSIG Resource Records for Ed448**

An Ed448 public key consists of a 56-byte value that represents the compressed encoding of the curve point, 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 Chapter 5.5 in [[I-D.josefsson-eddsa-ed25519](#)]. (TODO)

An Ed448 signature consists of a 112-byte 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 Chapter 5.6 in [[I-D.josefsson-eddsa-ed25519](#)]. (TODO)

The algorithm number associated with the use of Ed448 with SHA-512 in DS, DNSKEY and RRSIG resource records is TBD. This registration is fully defined in the IANA Considerations section.

## **4. Examples**



This section needs an update after the algorithm for Ed448 is assigned. NOTE: Also the examples are copied from Ed25519 draft and they need to be replaced with real examples.

```
Private-key-format: v1.2
Algorithm: TBD (ED448SHA512)
PrivateKey: ODIyNjAzODQ2MjgwODAxMjI2NDUxOTAyMDQxNDIyNjI=
# corresponding 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.
    cvTRVrU7downemQuBq9/E4t1IiRpvWcEmYdzqs6SCQxw6
    qmczBBQGLdssMx1TCJnwsEs9ZuA2phPzuJNoon9BCA== )
```

```
Private-key-format: v1.2
Algorithm: TBD (ED448SHA512)
PrivateKey: DSSF3o0s0f+ElWzj9E/0sXw8hLpk55chkmx0LYN5WiY=
```

```
example.com. 3600 IN DNSKEY 257 3 TBD (
    zPnZ/QwEe7S8C5SPz20fS5RR40Atk2/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/3Pi8KWUm7l0t00ivVRGvgulmVX8DgpE
    AFyMP2MKXJrqYJr+ViiCIDwc0IbPAQ==)
```

## 5. 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 and Kees Monshouwer for a review of this document.



## 6. IANA Considerations

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

+-----+-----+		
Number	TBD	
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.

## 7. Implementation Status

(Note to the RFC Editor: please remove this entire section as well as the reference to [RFC 6982](#) before publication.)

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [[RFC6982](#)]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [[RFC6982](#)], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

TODO: Fill out this section.





## 8. Security Considerations

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.

## 9. References

### 9.1. Normative References

- [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>>.

### 9.2. 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>>.



[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", [RFC 6781](#), DOI 10.17487/RFC6781, December 2012, <<http://www.rfc-editor.org/info/rfc6781>>.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", [RFC 6982](#), DOI 10.17487/RFC6982, July 2013, <<http://www.rfc-editor.org/info/rfc6982>>.

#### Authors' Addresses

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

Phone: +420 222 745 111  
Email: [ondrej.sury@nic.cz](mailto:ondrej.sury@nic.cz)

Robert Edmonds  
Farsight Security, Inc.  
155 Bovet Rd #476  
San Mateo, California 94402  
US

Phone: +1 650 489 7919  
Email: [edmonds@fsi.io](mailto:edmonds@fsi.io)

