Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: January 31, 2016

O. Sury
CZ.NIC

July 30, 2015

Ed25519 for DNSSEC
draft-sury-dnskey-ed25519-00

Abstract

This document describes how to specify Ed25519 keys and signatures in DNS Security (DNSSEC). It uses a Ed25519 curve and uses the SHA-256 for public key and SHA-512 hash for signatures.

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 January 31, 2016.

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
2. DNSKEY and RRSIG Resource Records for Ed25519 3
3. Support for NSEC3 Denial of Existence 3
4. Examples 4
4.1. Ed25519 Example 4
5. Acknowledgements 4
6. IANA Considerations 4
7. Security Considerations 5
8. References 5
8.1. Normative References 5
8.2. Informative References 5
Author's Address 6

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 one new signing algorithm: curve Ed25519 and SHA-256. (A description of Ed25519 can be found in EdDSA and Ed25519 [I-D.josefsson-eddsa-ed25519].) The DS RR for SHA-256 is already defined in RFC 4509 [RFC4509].

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). Using Ed25519 curve in DNSSEC has some advantages and disadvantage relative to using RSA with SHA-256 and with 3072-bit keys. Ed25519 keys are much shorter than RSA keys; at this size, the difference is 256 versus 3072 bits. Similarly, Ed25519 signatures are much shorter than RSA signatures; at this size, the difference is 512 versus vs 3072 bits. This is relevant because DNSSEC stores and transmits both keys and signatures.

In the signing algorithm defined in this document, the size of the key for the elliptic curve is matched with the size of the output of the hash algorithm (SHA-256). The size of the signatures are also matched with size of the hashing algorithm (SHA-256).

Signing with Ed25519 is significantly faster than with RSA (The reference implementation signs 109000 messages per second on a quad-core 2.4GHz Westmere CPU). However, validating RSA signatures is significantly faster than validating Ed25519 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

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

The Ed25519 signature constist 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]. In DNSSEC keys, the Ed25519 signatures is a simple bit string that represents Ed25519 signature.

The algorithm number associated with the DNSKEY and RRSIG resource records are fully defined in the IANA Considerations section. They are:

- DNSKEY and RRSIG RRs signifying Ed25519 and SHA-512 use the algorithm number TBD.

3. Support for NSEC3 Denial of Existence

RFC 5155 [RFC5155] defines new algorithm identifiers for existing signing algorithms to indicate that zones signed with these algorithm identifiers can use NSEC3 as well as NSEC records to provide denial of existence. That mechanism was chosen to protect implementations predating RFC 5155 from encountering resource records they could not know about. This document does not define such algorithm aliases.

A DNSSEC validator that implements the signing algorithms defined in this document MUST be able to validate negative answers in the form of both NSEC and NSEC3 with hash algorithm 1, as defined in RFC 5155. An authoritative server that does not implement NSEC3 MAY still serve zones that use the signing algorithms defined in this document with NSEC denial of existence.

4. Examples

4.1. Ed25519 Example

This needs a real example - this copied example of P-256

```
   Private-key-format: v1.2
   Algorithm: TBD (Ed25519)
   PrivateKey: ODIyNjAzODQ2MjgwODAxMjI2NDUxOTAyMDQxNDIyNjI= # coresponding to
82260384628080122645190204142262 INT

   example.net. 3600 IN DNSKEY 257 3 13 (
           XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
           XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX== )

   example.net. 3600 IN DS 55648 13 2 (
           b4c8c1fe2e7477127b27115656ad6256f424625bf5c1
           e2770ce6d6e37df61d17 )

   www.example.net. 3600 IN A 192.0.2.1
   www.example.net. 3600 IN RRSIG A 13 3 3600 (
           20150909100439 20150812100439 55648 example.net.
           XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
           XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX== )
```

5. Acknowledgements

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

6. 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	TBD
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.

7. Security Considerations

Ed25519 is targeted to provide attack resistance comparable to quality 128-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.

The security considerations listed in RFC 4509 apply here as well.

8. References

8.1. 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>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <http://www.rfc-editor.org/info/rfc5155>.

8.2. Informative References

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, DOI 10.17487/RFC4509, May 2006, <http://www.rfc-editor.org/info/rfc4509>.

[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