Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: July 30, 2016

O. Sury
CZ.NIC
R. Edmonds
Farsight Security, Inc.

January 27, 2016

Ed25519ph for DNSSEC
draft-curdle-dnskey-ed25519-00

Abstract

This document describes how to specify Ed25519ph keys and signatures in DNS Security (DNSSEC). It uses the Ed25519 instance of the Edwards-curve Digital Signature Algorithm (EdDSA) with the SHA-512 prehash 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 July 30, 2016.

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. [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 Ed25519 instance of the Edwards-curve Digital Signature Algorithm with the SHA-512 as prehash algorithm. This variant of EdDSA with SHA-512 as prehash function is named Ed25519ph in [I-D.irtf-cfrg-eddsa]. A more thorough description of Ed25519ph can be found in [I-D.irtf-cfrg-eddsa].

Ed25519ph has a 128-bit security target, which is considered to be equivalent in strength to RSA with ~3000-bit keys. Ed25519ph public keys are 256 bits (32 bytes) long while signatures are 512 bits (64 bytes) long.

The usage of the Ed25519ph algorithm in DNSSEC has advantages and disadvantages relative to RSA. Ed25519ph keys are much shorter than RSA keys. At comparable strengths, Ed25519ph keys are 352 bytes smaller than RSA-3072 keys. Similarly, an Ed25519ph signature saves 320 bytes over an RSA-3072 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, Ed25519ph still provides substantially smaller keys and signatures.

Signing with Ed25519ph is significantly faster than signing with equivalently strong RSA, and it is also faster than signing with the existing ECDSA algorithms defined in [RFC6605]. However, the validation of RSA signatures is significantly faster than the validation of Ed25519ph 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 Ed25519ph

An Ed25519ph public key consists of a 32-byte 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 Chapter 5.1.5 in [I-D.irtf-cfrg-eddsa].

An Ed25519ph signature consists of a 64-byte value, which is encoded into the Signature field of an RRSIG resource record as a simple bit string. The Ed25519ph signature algorithm is described in Chapter 5.1.6 in [I-D.irtf-cfrg-eddsa].

The algorithm number associated with the use of Ed25519ph 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 Ed25519ph is assigned.

```
Private-key-format: v1.2
Algorithm: TBD (ED25519PH)
PrivateKey: ODIyNjAzODQ2MjgwODAxMjI2NDUxOTAyMDQxNDIyNjI=
# corresponding to 822603846280801226451902041422 62 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: TBD (ED25519PH)
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==)
```

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	Ed25519ph
Mnemonic	ED25519PH
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

The security level of Ed25519ph is is slightly under the standard 128-bit level ([RFC7748]). Security considerations listed in [RFC7748] also apply to the usage of Ed25519 in DNSSEC. 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.irtf-cfrg-eddsa] Josefsson, S. and I. Liusvaara, "Edwards-curve Digital Signature Algorithm (EdDSA)", draft-irtf-cfrg-eddsa-02 (work in progress), January 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>.

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

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

Phone: +1 650 489 7919
Email: edmonds@fsi.io