Network Working Group
Internet-Draft
Updates: 6376 (if approved)
Intended status: Standards Track
Expires: December 17, 2018

J. Levine
Taughannock Networks

June 15, 2018

A new cryptographic signature method for DKIM
draft-ietf-dcrup-dkim-crypto-13

Abstract

This document adds a new signing algorithm to DKIM, ed25519-sha256. DKIM verifiers are required to implement this 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 https://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 December 17, 2018.

Table of Contents

1. Introduction

Discussion Venue: Discussion about this draft is directed to the dcrup@ietf.org [1] mailing list.

DKIM [RFC6376] signs e-mail messages, by creating hashes of the message headers and body and signing the header hash with a digital signature. Message recipients fetch the signature verification key from the DNS. The defining documents specify a single signing algorithm, RSA [RFC3447].

This document adds a new stronger signing algorithm, Edwards-Curve Digital Signature Algorithm using the Curve25519 curve (ed25519), which has much shorter keys than RSA for similar levels of security.

2. Conventions Used in This Document

The capitalized 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 [RFC8174].

Syntax descriptions use Augmented BNF (ABNF) [RFC5234]. The ABNF tokens sig-a-tag-k and key-k-tag-type are imported from [RFC6376].

3. Ed25519-SHA256 Signing Algorithm

The ed25519-sha256 signing algorithm computes a message hash as defined in section 3 of [RFC6376] using SHA-256 [FIPS-180-4-2015] as the hash-alg, and signs it with the PureEdDSA variant Ed25519, as defined in in RFC 8032 section 5.1 [RFC8032]. Example keys and signatures in Appendix A below are based on the test vectors in RFC 8032 section 7.1 [RFC8032].

The DNS record for the verification public key has a "k=ed25519" tag to indicate that the key is an Ed25519 rather than RSA key.

This is an additional DKIM signature algorithm added to Section 3.3 of [RFC6376] as envisioned in Section 3.3.4 of [RFC6376].

Note: since Ed25519 public keys are 256 bits long, the base64 encoded key is only 44 octets, so DNS key record data will generally fit in a single 255 byte TXT string, and will work even with DNS provisioning software that doesn't handle multi-string TXT records.

4. Signature and key syntax

The syntax of DKIM signatures and DKIM keys are updated as follows.

4.1. Signature syntax

The syntax of DKIM algorithm tags in section 3.5 of [RFC6376] is updated by adding this rule to the existing rule for sig-a-tag-k:

ABNF:

```
sig-a-tag-k =/ "ed25519"
```

4.2. Key syntax

The syntax of DKIM key tags in section 3.6.1 of [RFC6376] is updated by adding this rule to the existing rule for key-k-tag-type:

ABNF:

```
key-k-tag-type  =/ "ed25519"
```

The p= value in the key record is the ed25519 public key encoded in base64. Since the key is 256 bits long, the base64 text is 44 octets long. See Appendix A.2 for a sample key record using the public key in [RFC8032] Section 7.1, Test 1.

5. Key and algorithm choice and strength

Section 3.3 of [RFC6376] describes DKIM's hash and signature algorithms. It is updated as follows:

Signers SHOULD implement and verifiers MUST implement the ed25519-sha256 algorithm.

6. Transition Considerations

For backward compatibility, signers can add multiple signatures that use old and new signing algorithms. Since there can only be a single key record in the DNS for each selector, the signatures have to use different selectors, although they can use the same d= and i= identifiers.

7. Security Considerations

Ed25519 is a widely used cryptographic technique, All of the security advice in [RFC6376] continues to apply except that the security advice about ED25519 in Section 8 of [RFC8032] supplants the advice about RSA threats.

8. IANA Considerations

IANA is requested to update registries as follows.

8.1. DKIM Key Type registry

The following value is added to the DKIM Key Type Registry

TYPE	REFERENCE	STATUS
ed25519	[RFC8032]	active

Table 1: DKIM Key Type Registry Added Values

9. References

9.1. Normative References

[FIPS-180-4-2015]
U.S. Department of Commerce, "Secure Hash Standard", FIPS PUB 180-4, August 2015, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, DOI 10.17487/RFC3447, February 2003, <https://www.rfc-editor.org/info/rfc3447>.

9.3. URIs

[1] mailto:dcrup@ietf.org

Appendix A. Example of a signed message

This is a small message with both rsa-sha256 and ed25519-sha256 DKIM signatures. The signatures are independent of each other, so either signature would be valid if the other were not present.

A.1. Secret keys

Ed25519 secret key in base64. This is the secret key from [RFC8032] section 7.1 test 1, converted from hex to base64.

nWGxne/9WmC6hEr0kuwsxERJxWl7MmkZcDusAxyuf2A=

RSA secret key in PEM format.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDkHlOQoBTzWRiGs5V6NpP3idY6Wk08a5qhdR6wy5bdOKb2jLQi
Y/J16JYi0Qvx/byYzCNb3W91y3FutACDfzwQ/BC/e/8uBsCR+yz1Lxj+PL6lHvqM
KrM3rG4hstT5QjvHO9PzoxZyVYLzBfO2EeC3Ip3G+2kryOTIKT+l/K4w3QIDAQAB
AoGAH0cxOhFZDgzXWhDhnAJDw5s4roOXN4OhjiXa8W7Y3rhX3FJqmJSPuC8N9vQm
6SVbaLAE4SG5mLMueHlh4KXffEpuLEiNp9Ss3O4YfLiQpbRqE7Tm5SxKjvvQoZZe
zHorimOaChRL2it47iuWxzxSiRMv4c+j70GiWdxXnxe4UoECQQDzJB/0U58W7RZy
6enGVj2kWF732CoWFZWzi1FicudrBFoy63QwcowpoCazKtvZGMNlPWnC7x/6o8Gc
uSe0ga2xAkEA8C7PipPm1/1fTRQvj1o/dDmZp243044ZNyxjg+/OPN0oWCbXIGxy
WvmZbXriOWoSALJTjExEgraHEgnXssuk7QJBALl5ICsYMu6hMxO73gnfNayNgPxd
WFV6Z7ULnKyV7HSVYF0hgYOHjeYe9gaMtiJYoo0zGN+L3AAtNP9huqkWlzECQE1a
licIeVlo1e+qJ6Mgqr0Q7Aa7falZ448ccbSFYEPD6oFxiOl9Y9se9iYHZKKfIcst
o7DUw1/hz2Ck4N5JrgUCQQCyKveNvjzkkd8HjYs0SwM0fPjK16//5qDZ2UiDGnOe
uEzxBDAr518Z8VFbR41in3W4Y3yCDgQlLlcETrS+zYcL
-----END RSA PRIVATE KEY-----
```

A.2. Public key DNS records

The public key p= value in the first record is the public key from [RFC8032] section 7.1 test 1, converted from hex to base64.

```
brisbane._domainkey.football.example.com. IN TXT (
 "v=DKIM1; k=ed25519; p=11qYAYKxCrfVS/7TyWQHOg7hcvPapiMlrwIaaPcHURo=")

test._domainkey.football.example.com. IN TXT (
 "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDkHlOQoBTzWR"
 "iGs5V6NpP3idY6Wk08a5qhdR6wy5bdOKb2jLQiY/J16JYi0Qvx/byYzCNb3W91y3FutAC"
 "DfzwQ/BC/e/8uBsCR+yz1Lxj+PL6lHvqMKrM3rG4hstT5QjvHO9PzoxZyVYLzBfO2EeC3"
 "Ip3G+2kryOTIKT+l/K4w3QIDAQAB")
```

A.3. Signed Message

The text in each line of the message starts at the first position except for the continuation lines on the DKIM-Signature headers which start with a single space. A blank line follows the "Joe." line.

```
   DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/relaxed;
    d=football.example.com; i=@football.example.com;
    q=dns/txt; s=brisbane; t=1528637909; h=from : to :
    subject : date : message-id : from : subject : date;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=/gCrinpcQOoIfuHNQIbq4pgh9kyIK3AQUdt9OdqQehSwhEIug4D11Bus
    Fa3bT3FY5OsU7ZbnKELq+eXdp1Q1Dw==
   DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=football.example.com; i=@football.example.com;
    q=dns/txt; s=test; t=1528637909; h=from : to : subject :
    date : message-id : from : subject : date;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=F45dVWDfMbQDGHJFlXUNB2HKfbCeLRyhDXgFpEL8GwpsRe0IeIixNTe3
    DhCVlUrSjV4BwcVcOF6+FF3Zo9Rpo1tFOeS9mPYQTnGdaSGsgeefOsk2Jz
    dA+L10TeYt9BgDfQNZtKdN1WO//KgIqXP7OdEFE4LjFYNcUxZQ4FADY+8=
   From: Joe SixPack <joe@football.example.com>
   To: Suzie Q <suzie@shopping.example.net>
   Subject: Is dinner ready?
   Date: Fri, 11 Jul 2003 21:00:37 -0700 (PDT)
   Message-ID: <20030712040037.46341.5F8J@football.example.com>

   Hi.

   We lost the game.  Are you hungry yet?

   Joe.
```

Appendix B. Change log

12 to 13 Made example even less wrong.

11 to 12 Made example less wrong.

10 to 11 New example with both signatures, minor nits.

09 to 10 Improve abstract, minor nits.

08 to 09 Specify sha-256 for the extremely literal minded. Take out the prehash stuff. Add example.

07 to 08 Specify base64 key records. Style edits per Dave C.

06 to 07: Remove RSA fingerprints. Change Pure to hashed eddsa.

05 to 06: Editorial changes only.

04 to 05: Remove deprecation cruft and inconsistent key advice. Fix p= and k= text.

03 to 04: Change eddsa to ed25519. Add Martin's key regeneration issue. Remove hashed ed25519 keys. Fix typos and clarify text. Move syntax updates to separate section. Take out SHA-1 stuff.

01 to 02: Clarify EdDSA algorithm is ed25519 with Pure version of the signing. Make references to tags and fields consistent.

Author's Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886

Phone: +883.5100.01196712
Email: standards@taugh.com