Network Working Group
Internet-Draft
Updates: 6376 (if approved)
Intended status: Standards Track
Expires: June 4, 2018

J. Levine
Taughannock Networks

December 1, 2017

# A new cryptographic signature method for DKIM
# draft-ietf-dcrup-dkim-crypto-07

Abstract

DKIM was designed to allow new cryptographic algorithms to be added. This document adds a new signing 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 June 4, 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 where it is stored in a TXT record. The defining documents specify a single signing algorithm, RSA [RFC3447], and recommend key sizes of 1024 to 2048 bits.

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 [RFC2119].

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], and signs it with the Hash variant of Ed25519, as defined in in RFC 8032 section 5.1 [RFC8032]. The signing algorithm is HashEdDSA. (Even though the input to the signing algorithm has already been hashed, the PureEdDSA which does not do an additional hash is not widely implemented, and the extra hash causes no problems other than an insignificant slowdown.) The DNS record for the verification public key MUST have a "k=ed25519" tag to indicate that the key is an Ed25519 rather than RSA key.

Note: since Ed25519 keys are 256 bits long, 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"
```

## 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 MAY 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 will 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, so the security of DKIM signatures using new signing algorithms should be at least as good as those using old algorithms.

## 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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[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>.

### 9.2. URIs

[1] mailto:dcrup@ietf.org

## Appendix A. Change log

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: +1 831 480 2300
Email: standards@taugh.com