A new cryptographic signature method for DKIM

draft-ietf-dcrup-dkim-crypto-11

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 7, 2018.

Copyright Notice

Copyright (c) 2018 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 (https://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

1.  Introduction .................................................. 2
2.  Conventions Used in This Document .......................... 2
3.  Ed25519-SHA256 Signing Algorithm .......................... 3
4.  Signature and key syntax ....................................... 3
   4.1.  Signature syntax ........................................ 3
   4.2.  Key syntax ................................................ 3
5.  Key and algorithm choice and strength ...................... 4
6.  Transition Considerations ..................................... 4
7.  Security Considerations ....................................... 4
8.  IANA Considerations .......................................... 4
   8.1.  DKIM Key Type registry ................................... 4
9.  References ..................................................... 5
   9.1.  Normative References .................................... 5
   9.2.  Informative References ................................... 5
   9.3.  URIs ...................................................... 5
Appendix A.  Example of a signed message ....................... 5
   A.1.  Secret keys ............................................... 6
   A.2.  Public key DNS records ................................... 6
   A.3.  Signed Message ............................................ 6
Appendix B.  Change log ............................................ 7
Author’s Address .................................................. 8

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
[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] using SHA-256 [FIPS-180-4-2015] as the hash-alg, and signs it with the PureEdDSA variant Ed25519, as defined 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 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. For example, a key record using the public key in [RFC8032] Section 7.1, Test 1, might be:
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, so the security of DKIM signatures using new signing algorithms should be at least as good as those using old algorithms.

All of the security advice in [RFC6376] continues to apply except that the advice 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

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REFERENCE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ed25519</td>
<td>[RFC8032]</td>
<td>active</td>
</tr>
</tbody>
</table>

Table 1: DKIM Key Type Registry Added Values
9. References

9.1. Normative References


9.2. Informative References


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.

fL+5V9EcuCZoVki3pA6bK9zwCzoEtj1uIqK9ZHXHA=

RSA secret key in PEM format.

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDkHlOQoBTszWRIgS5V6NpP3i6Y6wK08a5qhdR6wy5bdOKb2jLQiY/J16Jy1Qvx/lyZyCNb3W91y3FutACDfzwq/BC/e/8ub3CR+yzl1xj+PL61HvqMKrMrG4hstT5QjvH09PzoxZyVYLzBf02EeC3Ip3G+2kryOTIKT+1/K4w3QIDAQAB AoGAH0cxOFZDgzXWdhNnAJDMs4ro0XN40hjix8aW7Y3rhX3FJqmsJSPcuC8N9vQm6SVbaLEAS5G5LMueHh4KXffEpULi9nP9S304YfLIQpbRqE7Tm5SxKjvQoZZe
zHorim0aChRL2it47iuWwxxSIRMV4+c+j70GliWdxXnxe4U0ECQQDz/0J058W7Ry6enGvJ2kWF732CoWF2Zwi1FicudrBFOy63QwcowpoCazKtvZGMN1PWwC7x/6o8GcuSe0ga2xaKEA8C7pipM1/1TPRQvjk/d0M2p2430442Nyjxjg/+0PNO0WCBX1GxY
WvmZbHxriW0oSALJtjExEgraHEgnXssuk7QJBal15eSMy6hMx073gnfNayNgPxdWFV67ULkV7HsVYF0hyOHjyeYe9gaMtjYoolo9zGN/L3AAtnp9huqWlzECEQLa1licmEvI0e+qJ6MgggQ0Q7Aa7fa2448ccbSFYEPD6oFxiOl9Y9se9iYH2KkFjct07DUw1/hz2Ck4N5rjgUCQCCyKveNvjkkd8Hjys0swM0fPjK16/5qDZ2UiDgnOe
uEzxBDAr518Z8VFB4r1in3W4Y3yCDgQ1LlETrS+zYcL
-----END RSA PRIVATE KEY-----

A.2. Public key DNS records

brisbane._domainkey.example.com IN TXT ("v=dkim1; k=ed25519; p=y150dj590qbpFpNKh1sv91qaS0ArSYu02gp180DW1y=")

test._domainkey.example.com IN TXT ("v=dkim1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDkHlOQoBTszWRIgS5V6NpP3i6Y6wK08a5qhdR6wy5bdOKb2jLQiY/J16Jy1Qvx/lyZyCNb3W91y3FutACDfzwq/BC/e/8ub3CR+yzl1xj+PL61HvqMKrMrG4hstT5QjvH09PzoxZyVYLzBf02EeC3Ip3G+2kryOTIKT+1/K4w3QIDAQAB AoGAH0cxOFZDgzXWdhNnAJDMs4ro0XN40hjix8aW7Y3rhX3FJqmsJSPcuC8N9vQm6SVbaLEAS5G5LMueHh4KXffEpULi9nP9S304YfLIQpbRqE7Tm5SxKjvQoZZe
zHorim0aChRL2it47iuWwxxSIRMV4+c+j70GliWdxXnxe4U0ECQQDz/0J058W7Ry6enGvJ2kWF732CoWF2Zwi1FicudrBFOy63QwcowpoCazKtvZGMN1PWwC7x/6o8GcuSe0ga2xaKEA8C7pipM1/1TPRQvjk/d0M2p2430442Nyjxjg/+0PNO0WCBX1GxY
WvmZbHxriW0oSALJtjExEgraHEgnXssuk7QJBal15eSMy6hMx073gnfNayNgPxdWFV67ULkV7HsVYF0hyOHjyeYe9gaMtjYoolo9zGN/L3AAtnp9huqWlzECEQLa1licmEvI0e+qJ6MgggQ0Q7Aa7fa2448ccbSFYEPD6oFxiOl9Y9se9iYH2KkFjct07DUw1/hz2Ck4N5rjgUCQCCyKveNvjkkd8Hjys0swM0fPjK16/5qDZ2UiDgnOe
uEzxBDAr518Z8VFB4r1in3W4Y3yCDgQ1LlETrS+zYcL
-----END RSA PRIVATE KEY-----

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.
DKIM-Signature: v=1; a=ed25519-sha256; c=simple/simple;
d=football.example.com; i=@football.example.com;
q=dns/txt; s=brisbane; t=1518460054; h=from : to :
subject : date : message-id : from : subject : date;
bh=4bLNXImK9drULnmePzZNEB1eUanJXC5PlsDIfH4HTQ==;
b=9/dsDChY0YMTtD5Eyw3wx7x22B15JP7M5ECbJ7GWrR45nX1TCGb810YB
o0wBLR++X5LqmsxXa0JLLje46110A==
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;
d=football.example.com; i=@football.example.com;
q=dns/txt; s=test; t=1527915362; h=from : to : subject :
date : message-id : from : subject : date;
bh=4bLNXImK9drULnmePzZNEB1eUanJXC5PlsDIfH4HTQ==;
b=iKcL5SEYYXJ95f1vWE8FT6h15iqd8MC/LEKYH0QjsqYy6MO/4pgVNCZH
1/RAXAaADxe/40Fg7uT1xwwD1hJN2P1e6J//cJfs1BdDOq6zTVbne1dqt1
N0at7iamJ1AfRqyG+ja7a2AZzrpUuJ7VA60+0zRYPqwpMEkEFIzI9i/Xk=
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

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