Network Working Group   J. Levine
Internet-Draft   Taughannock Networks
Updates: 6376 (if approved)   May 10, 2018
Intended status: Standards Track
Expires: November 11, 2018

              A new cryptographic signature method for DKIM
                    draft-ietf-dcrup-dkim-crypto-09

Abstract

   This document adds a new signing algorithm to DKIM.

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 November 11, 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
   [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 in RFC 8032 section 5.1 [RFC8032]. Example keys and
signatures in Appendix XX 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 only DNS key record data will generally fit in a
single 255 byte TXT string, and will work 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, mignt be:

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

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

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

[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](). Example of a signed message

This is a small message with an ed25519-rsa DKIM signature.

[A.1](). Secret key

Ed25519 secret key in base64.

fL+5V9EquCZAovKik3pA6Lk9zwCzoEtjIuIqK9ZXHHA=

[A.2](). **Public key DNS record**

```
test._domainkey.example.com IN TXT
           "k=ed25519; p=yi50DjK5O9pqbFpNHklsv9lqaS0ArSYu02qp1S0DW1Y="
```

[A.3](). **Signed Message**

   The text in each line of the message start at the first position
   except for the five continuation lines on the DKIM-Signature which
   start with a single space.

```
   DKIM-Signature: v=1; a=ed25519; c=relaxed/simple; d=example.com;
    i=@example.com; q=dns/txt; s=test; t=5; h=message-id :
    date : from : to : subject : date : from : subject;
    bh=wE7NXSkgnx9PGiavN4OZhJztvkqPDlemV3OGuEnLwNo=;
    b=wt7P+9DoBwcln1RKE3LN7069ZEEiSyVE/NH1YXnqnJy4JcrSCZUbeIEh
    vXssPHelX4yNSXG9eTGTwwk5NxYqBw==
   Received: from localhost
   Message-ID: <example@example.com>
   Date: Mon, 01 Jan 2011 01:02:03 +0400
   From: Test User <test@example.com>
   To: somebody@example.com
   Subject: Testing

   This is a test message.
```

[Appendix B](). **Change log**

   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