Internet Engineering Task Force (IETF)
Request for Comments: 8463
Updates: 6376
Category: Standards Track
ISSN: 2070-1721

J. Levine
Taughannock Networks

September 2018

A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)

Abstract

This document adds a new signing algorithm, Ed25519-SHA256, to "DomainKeys Identified Mail (DKIM) Signatures" (RFC 6376). DKIM verifiers are required to implement this algorithm.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8463.

Table of Contents

1. Introduction

DKIM [RFC6376] signs email messages by creating hashes of selected message header fields 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] (which has since been obsoleted by [RFC8017]).

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 key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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. It signs the hash with the PureEdDSA variant Ed25519, as defined in RFC 8032, Section 5.1 [RFC8032]. Example keys and signatures in Appendix A 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 an RSA key.

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

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 work even with DNS provisioning software that doesn’t handle multistring 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. Choice and Strength of Keys and Algorithms

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.

The example message in Appendix A has two signatures with the same d= and i= identifiers but different a= algorithms and s= selectors.

7. Security Considerations

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 has updated a registry as follows.

8.1. "DKIM Key Type" Registry

The following value has been added to the "DKIM Key Type" registry:

TYPE	REFERENCE	STATUS
ed25519	[RFC8032]	active

Table 1: Value Added to the "DKIM Key Type" Registry

9. References

9.1. Normative References

[FIPS-180-4-2015]
National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015, <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>.

[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>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[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>.

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 header fields, 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.
```

Author’s Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886
United States of America

Phone: +883.5100.01196712
Email: standards@taugh.com