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.

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.
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:

<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: Value Added to the "DKIM Key Type" Registry
9. References

9.1. Normative References


9.2. Informative References

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-----
MIICXQIBAAKBgQDkHlOQoBTzWRIgs5V6Np3idY6Wk08a5qhdR6w5b0dOkb2jLQi
Y/J16JYi10Qvx/byYzCNb3W9ly3FutACDfzwQ/BC/e/8uBSR+yzILxj+PL6lHvqM
KrM3rG4hstT5qjvHO9PzozZyVLYzBfO2EeC3ip3G+2kryOITKT+1/K4w3QIDAQAB
AoGAH0cxhFZDgzXWhDhnAjDw5s4roXN40hiXa8WY73rhX3FJqmJSFuc8N9vQm
65VbalaE45G5mlMueHlh4KxfEFepuELINp9s304Yf1QpbRqE77m5sxjvvpOoZZe
zhorImoaChRL2lt47iuxzslRMv4+c+j70GiWdxxNnxen400ECCQDzJB/0U58W7R2y
6enGVj2kWF732CoWFZwl1FicudrBFoy63WccwpoCazKtvZGMNIpWNc7x/6oBgc
uSe0g2a2xAKeA8C7PipMl/1fTRqvj0/0dSmZp2430442Nyxjg+/0PN0oWCbXIgx
WvmZbXr1oWoALJTjExEgraHEgnXssuk7QJBAL15Cs1Mu6hMx073gnfNayNgPxd
WFV627ULnKyV7H5yF0qyYOHeYe9gaMtiYjYoo0zGN+L3AAeNF9huqkWlzECQE1a
licleVtole+qJ6Mqgr0Q7Aa7falZ448ccbSFYEPEd6c0xi09Y9se9iYHZKfIcst
o7DUw1/hz2Ck4N5JrgUCQCYeVenVjzkkd8HjYsOswM0fPJrK16/5qBZ2UIdGNoe
uEzwBDAr518Z8V8bR41in3W4y3yCDgQLLceETrS+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/7TyWQHOg7hcvPapiMlrwIaapChUreo=")

test._domainkey.football.example.com. IN TXT ("v=DKIM1; k=rsa; p=MIgFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQQDkHlOQoBTzWR"
"iGs5V6Np3idY6Wk08a5qhdR6w5b0dOkb2jLQiY/J16JYi10Qvx/byYzCNb3W9ly3FutAC"
"DfzwQ/BC/e/8uBSR+yzILxj+PL6lHvqMKrM3rG4hstT5qjvHO9PzozZyVLYzBFQ2EeC3"
"Ip3G+2kryOITKT+1/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.

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