

Network Working Group
Internet-Draft
Updates: [6376](#) (if approved)
Intended status: Standards Track
Expires: December 13, 2017

J. Levine
Taughannock Networks
June 11, 2017

Cryptographic Update to DKIM
draft-ietf-dcrup-dkim-crypto-01

Abstract

DKIM was designed to allow new cryptographic algorithms to be added. This document adds a new algorithm and a new way to represent signature validation keys, and deprecates obsolete signing algorithms.

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 <http://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 13, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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.	EdDSA-SHA256 Signing Algorithm	3
4.	Public key fingerprints	3
5.	Key and algorithm choice and strength	4
6.	Transition Considerations	4
7.	Security Considerations	4
8.	IANA Considerations	4
8.1.	DKIM Signature Tag Registry	4
8.2.	DKIM Hash Algorithms Registry	5
8.3.	DKIM Key Type registry	5
9.	References	5
9.1.	Normative References	5
9.2.	URIs	6
	Author's Address	6

[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 content 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 recommends key sizes of 1024 to 2048 bits. While 1024 bit signatures are common, stronger signatures are not. Widely used DNS configuration software places a practical limit on key sizes, because the software only handles a single 256 octet string in a TXT record, and RSA keys longer than 1156 bits don't fit in 256 octets.

This document adds a new signing algorithm, Edwards-Curve Digital Signature Algorithm (EdDSA), which has much shorter keys than RSA for similar levels of security. It also adds a new key representation, with the key itself in the signature and a shorter key fingerprint in the DNS.

[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, key-k-tag-type, and base64tring are imported from [RFC6376].

3. EdDSA-SHA256 Signing Algorithm

The eddsa-sha256 signing algorithm computes a message hash as defined in [section 3 of \[RFC6376\]](#), and signs it using the EdDSA algorithm defined in [RFC8032]. The DNS record for the verification public key MUST have a "k=ecdh" or "k=ecdhfp" tag to indicate that the key is an ECDH rather than RSA key.

The syntax of DKIM signature tags is updated as follows:

ABNF:

```
sig-a-tag-k = "rsa" / "rsaftp" / "eddsa" / "eddsaftp" x-sig-a-tag-k
```

The syntax of DKIM key tags is updated as follows:

ABNF:

```
key-k-tag-type = "rsa" / "rsaftp" / "eddsa" / "eddsaftp"  
                / x-key-k-tag-type
```

4. Public key fingerprints

Rather than using a public key stored in the DNS, a signature MAY include the corresponding public key, with a fingerprint in the DNS. For an RSA signature, the Signing Algorithm is rsaftp-sha256, or for an EdDSA signature the Signing Algorithm is eddsaftp-sha256. The corresponding public key is included in the signature as a base64 encoded string with a k= tag. The key in the tag is the same one that would be published in a non-fingerprint key record.

The DNS record contains a sha-256 hash of the public key, stored in base64 in the p= tag. The key type tag MUST be present and contains k=rsaftp or k=ecdhfp.

k= The public key (base64; REQUIRED). Whitespace is ignored in this value and MUST be ignored when reassembling the original key.

ABNF:

```
sig-k-tag      = %x6b [FWS] "=" [FWS] sig-k-tag-data  
sig-k-tag-data = base64string
```


5. Key and algorithm choice and strength

[[splice in text from Scott K's draft to taste here]]

[Section 3.3 of \[RFC6376\]](#) describes DKIM's hash and signature algorithms. It is updated as follows:

Signers MUST NOT implement and verifiers SHOULD NOT implement the rsa-sha1 algorithm. Signers SHOULD implement and verifiers MUST implement the rsafp-256, ecdh-sha256, and ecdhfp-sha256 algorithms.

Signers that use rsa-sha256 signatures MUST use keys at least 1024 bits long and SHOULD use keys 2048 bits long. Verifiers MUST NOT accept rsa-sha256 signatures with keys less than 1024 bits long.

[[is there any reason to allow or require RSA keys longer than 2048 ?]]

6. Transition Considerations

For backward compatibility, signers MAY add multiple signatures that use old and new signing algorithms or key representations. 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

EdDSA and key fingerprints are widely used cryptographic techniques, so the security of DKIM signatures using new signing algorithms should be at least as good as those using old algorithms. Since key fingerprints make it possible to publish verification records for RSA keys of any length, rsafp signatures SHOULD use key lengths of 1536 or 2048 bits.

8. IANA Considerations

IANA is requested to update registries as follows.

8.1. DKIM Signature Tag Registry

The following value is added to the DKIM Signature Tag Registry

TYPE	REFERENCE	STATUS
k	(this document)	active

Table 1: DKIM Signature Tag Registry Added Value

8.2. DKIM Hash Algorithms Registry

The following value is updated in the DKIM Hash Algorithms Registry

TYPE	REFERENCE	STATUS
sha1	[FIPS-180-3-2008]	historic

Table 2: DKIM Hash Algorithms Registry Updated Value

8.3. DKIM Key Type registry

The following values is added to the DKIM Key Type Registry

TYPE	REFERENCE	STATUS
rsaftp	[RFC3447]	active
eddsa	[RFC8032]	active
eddsaftp	[RFC8032]	active

Table 3: 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, <<http://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, <<http://www.rfc-editor.org/info/rfc3447>>.

- [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, <<http://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, <<http://www.rfc-editor.org/info/rfc8032>>.

9.2. URIs

[1] <mailto:dcrup@ietf.org>

Author's Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886

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

