

Network Working Group  
Internet-Draft  
Updates: 6376 (if approved)  
Intended status: Standards Track  
Expires: May 7, 2018

S. Kitterman  
Kitterman Technical Services  
November 3, 2017

Cryptographic Algorithm and Key Usage Update to DKIM  
draft-ietf-dcrup-dkim-usage-06

Abstract

The cryptographic algorithm and key size requirements included when DKIM was designed in the last decade are functionally obsolete and in need of immediate revision. This document updates DKIM requirements to those minimally suitable for operation with currently specified 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 May 7, 2018.

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. Discussion Venue . . . . .	2
2. Introduction . . . . .	2
3. Conventions Used in This Document . . . . .	3
4. DKIM Signing and Verification Algorithms . . . . .	3
4.1. DKIM Signing and Verification Algorithms . . . . .	3
4.2. Key Sizes . . . . .	3
5. Security Considerations . . . . .	4
6. IANA Considerations . . . . .	4
7. References . . . . .	4
7.1. Normative References . . . . .	4
7.2. Informative References . . . . .	4
7.3. URIs . . . . .	5
Appendix A. Acknowledgements . . . . .	5
Author's Address . . . . .	5

## 1. Discussion Venue

RFC EDITOR: Please remove this section before publication.

Discussion about this draft is directed to the dcrup@ietf.org [1] mailing list.

## 2. Introduction

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 [RFC8017], and recommends key sizes of 1024 to 2048 bits (but require verification of 512 bit keys). As discussed in US-CERT VU#268267 [VULNOTE], the operational community has recognized that shorter keys compromise the effectiveness of DKIM. 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 significantly longer than 1024 bits don't fit in 256 octets.

Due to the recognized weakness of the sha1 hash algorithm, see [RFC6194], and the wide availability of the sha256 hash algorithm (it has been a required part of DKIM [RFC6376] since it was originally standardized in 2007), the sha1 hash algorithm MUST NOT be used.

This is being done now to allow the operational community time to fully shift to sha256 in advance of any sha1 related crisis.

### 3. 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].

### 4. DKIM Signing and Verification Algorithms

Section 4.1 updates [RFC6376] Section 3.3.

Section 4.2 updates [RFC6376] Section 3.3.3.

The algorithm described in [RFC6376] Section 3.3.1 is now historic and no longer used by DKIM.

[RFC6376] Sections 3.3.2 and 3.3.4 are not affected.

#### 4.1. DKIM Signing and Verification Algorithms

DKIM supports multiple digital signature algorithms. Two algorithms are defined by this specification at this time: rsa-sha1 and rsa-sha256. Signers MUST sign using rsa-sha256. Verifiers MUST be able to verify using rsa-sha256. rsa-sha1 MUST NOT be used for signing or verifying.

DKIM signatures identified as having been signed with historic algorithms (currently rsa-sha1) have permanently failed evaluation as discussed in [RFC6376] Section 3.9.

#### 4.2. Key Sizes

Selecting appropriate key sizes is a trade-off between cost, performance, and risk. Since short RSA keys more easily succumb to off-line attacks, Signers MUST use RSA keys of at least 1024 bits for all keys. Signers SHOULD use RSA keys of at least 2048 bits. Verifiers MUST be able to validate signatures with keys ranging from 1024 bits to 4096 bits, and they MAY be able to validate signatures with larger keys. Verifier policies can use the length of the signing key as one metric for determining whether a signature is acceptable. Verifiers MUST NOT consider signatures using RSA keys of less than 1024 bits as valid signatures.

DKIM signatures with insufficient key sizes (currently rsa-sha256 with less than 1024 bits) have permanently failed evaluation as discussed in [RFC6376] Section 3.9.

## 5. Security Considerations

This document does not change the Security Considerations of [RFC6376]. It reduces the risk of signature compromise due to weak cryptography. The SHA-1 risks discussed in [RFC6194] Section 3 are resolved due to rsa-sha1 no longer being used by DKIM.

## 6. IANA Considerations

IANA is requested to update the "sha1" registration in the "DKIM Hash Algorithms" as follows:

TYPE	REFERENCE	STATUS
sha1	[RFC6376]	historic

Table 1: DKIM Hash Algorithms Changed Value

## 7. References

### 7.1. 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>>.
- [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>>.
- [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, <<http://www.rfc-editor.org/info/rfc8017>>.

### 7.2. Informative References

- [RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <<http://www.rfc-editor.org/info/rfc6194>>.
- [VULNOTE] US-CERT, "Vulnerability Note VU#268267, DomainKeys Identified Mail (DKIM) Verifiers may inappropriately convey message trust", October 2012.

### 7.3. URIs

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

### Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and comment on this proposal: Kurt Andersen, Murray S. Kucherawy, Martin Thomson, John Levine, Russ Housley, and Jim Fenton.

Thanks to John Levine for his DCRUP work that was the source for much of the introductory material in this draft.

### Author's Address

Scott Kitterman  
Kitterman Technical Services  
3611 Scheel Dr  
Ellicott City, MD 21042

Phone: +1 301 325-5475  
Email: [scott@kitterman.com](mailto:scott@kitterman.com)