Internet Engineering Task Force (IETF)
Request for Comments: 8301
Updates: 6376
Category: Standards Track
ISSN: 2070-1721

S. Kitterman
Kitterman Technical Services

January 2018

Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)

Abstract

The cryptographic algorithm and key size requirements included when DomainKeys Identified Mail (DKIM) was designed a decade ago 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 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/rfc8301.

Table of Contents

1. Introduction

DKIM [RFC6376] signs email 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, RFC 6376 [RFC6376] and its predecessors, specify a single signing algorithm, RSA [RFC8017], and recommend key sizes of 1024 to 2048 bits (but require verification of 512-bit keys). As discussed in US-CERT Vulnerability Note 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 SHA-1 hash algorithm (see [RFC6194]) and the wide availability of the SHA-256 hash algorithm (it has been a required part of DKIM [RFC6376] since it was originally standardized in 2007), the SHA-1 hash algorithm MUST NOT be used. This is being done now to allow the operational community time to fully shift to SHA-256 in advance of any SHA-1-related crisis.

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.

3. Updates to DKIM Signing and Verification Requirements

This document updates [RFC6376] as follows:

- Section 3.1 of this document updates Section 3.3 of [RFC6376].
- Section 3.2 of this document updates Section 3.3.3 of [RFC6376].
- The algorithm described in Section 3.3.1 of [RFC6376] is now historic and no longer used by DKIM.

Sections 3.3.2 and 3.3.4 of [RFC6376] are not affected.

3.1. 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 Section 3.9 of [RFC6376].

3.2. 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 Section 3.9 of [RFC6376].

4. 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 Section 3 of [RFC6194] are resolved due to rsa-sha1 no longer being used by DKIM.

5. IANA Considerations

IANA has updated the Reference and Status fields of the "sha1" registration in the "DKIM Hash Algorithms" registry. The registration now appears as follows:

Type	Reference	Status
sha1	[RFC6376] [RFC8301]	historic

6. References

6.1. 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, <https://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, <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>.

[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>.

6.2. 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, <https://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, <http://www.kb.cert.org/vuls/id/268267>.

Acknowledgements

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

Thanks to John Levine for his DKIM Crypto Update (DCRUP) work that was the source for much of the introductory material in this document.

Author's Address

Scott Kitterman
Kitterman Technical Services
3611 Scheel Dr
Ellicott City, MD 21042
United States of America

Phone: +1 301 325-5475
Email: scott@kitterman.com