Cryptographic Update to DKIM
draft-levine-dcrup-dkim-crypto-00

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.

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 September 30, 2017.

Table of Contents

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 1024 bits don't fit in 256 octets.

   This document adds a new signing algorithm, Elliptic Curve Diffie-
   Hellman (ECDH), 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. **ECDH-SHA256 Signing Algorithm**

   The ecdh-sha256 signing algorithm computes a message hash as defined
   in section 3 of [RFC6376], and signs it using the ECDH algorithm
   defined in [RFC7748]. 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.

   ECDH signatures MUST NOT use SHA-1 hashes.

   The syntax of DKIM signature tags is updated as follows:

        ABNF:

        sig-a-tag-k = "rsa" / "rsafp" / "ecdh" / "ecdhfp" x-sig-a-tag-k

   The syntax of DKIM key tags is updated as follows:

        ABNF:

        key-k-tag-type = "rsa" / "rsafp" / "ecdh" / "ecdhfp"
              / 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 rsafp-sha256, or for
   an ECDH signature the Signing Algorithm is ecdhfp-sha256. The
   corresponding public key is included in the signature as a k= tag.

   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=rsafp 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. 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.

6. Security Considerations

   ECDH 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.

7. IANA Considerations

   IANA is requested to update registries as follows.

7.1. 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

7.2. DKIM Key Type registry

   The following values is added to the DKIM Key Type Registry

```
            +--------+-----------+--------+
            |  TYPE  | REFERENCE | STATUS |
            +--------+-----------+--------+
            | rsafp  | [RFC3447] | active |
            |  ecdh  | [RFC7748] | active |
            | ecdhfp | [RFC7748] | active |
            +--------+-----------+--------+
```

             Table 2: DKIM Key Type Registry Added Values

8. References

8.1. 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>.

   [RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves
              for Security", RFC 7748, DOI 10.17487/RFC7748, January
              2016, <http://www.rfc-editor.org/info/rfc7748>.

8.2. URIs

   [1] mailto:we-need-a-list

Author's Address

   John Levine
   Taughannock Networks
   PO Box 727
   Trumansburg, NY 14886

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