Mandatory Tags for DKIM Signatures
draft-levine-dkim-conditional-02

Abstract

The DKIM protocol applies a cryptographic signature to an e-mail message. This specification extends DKIM to allow new signature tags that validators are required to evaluate. The first such tag specifies a second signature that must be present for a signature to be valid.

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 March 31, 2016.

Copyright Notice

Copyright (c) 2015 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.
1.  Introduction

DKIM [RFC6376] defines a cryptographic header field consisting of a series of tags and values. The values include signed hashes of some of the header fields and part or all of the body of a message. The signature contains a domain name that is responsible for the signature. The signature is valid if the hashes in the signature match the corresponding hashes of the message at validation time, the signature is validated by a public key retrieved from that responsible domain's DNS, and it is before the expiration time in the signature header field.

This specification defines the syntax for new tags in a signature header field that specify additional conditions that must be satisfied for a signature to be valid. The first such condition requires the presence of an additional signature from a specified different domain. It also defines a new version 2 of the DKIM protocol to support the new semantics of conditional signatures.

2.  Definitions

The 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 "ALPHA", "FWS", "tag-list" and "domain-name" are defined as in [RFC6376].
3. Mandatory DKIM header tags

The current DKIM specification defines a set of header tags, some of which are required to appear in every signature and some of which are optional. It also allows a signer to include private tags that don’t conflict with the registered ones. Since verifiers ignore tags that they don’t understand, new tags can only provide new information about the message, or enable new verification schemes for signatures that would otherwise be considered invalid.

A Mandatory Tag is a new kind of tag prefixed with an exclamation point. Its syntax is otherwise identical to an ordinary tag.

ABNF:

tag-spec = / [FWS] "!" tag-name [FWS] "=" [FWS] tag-value [FWS]

3.1. Signature version numbers

Any DKIM signature with a mandatory tag MUST have version "2" in the signature’s version tag.

All valid DKIM version 1 signatures are also valid version 2 signatures, with "v=1" replaced by "v=2" in the DKIM-Signature header. Signatures without mandatory tags SHOULD continue to use version "1" for backward compatibility.

3.2. Processing mandatory tags

When a verifier encounters a mandatory tag in a signature, it MUST process the tag according to the tag’s definition. If the verifier is unable to process the tag the verifier MUST return PERMFAIL for that signature. If there are multiple signatures on a message, the verifier continues to verify other signatures as usual. It is valid to have a mixture of version "1" and version "2" signatures on a single message.

3.3. Forward signature (!fs) tag

The "!fs" mandatory tag means that the signature is only valid if an additional signature is present in the message. The value of the !fs tag is a domain name that is the value of the d= tag of the additional signature. The condition is satisfied if the message includes at least one valid DKIM signature header field with responsible domain (the d= tag) being one specified by the !fs tag.
Chained !fs tags are valid and may be useful in scenarios with multiple levels of forwarders. DKIM verifiers SHOULD handle at least three levels of !fs chaining.

4. Typical application scenario

A sender that expects a message to be forwarded might put both a conventional DKIM signature and a signature with a !fs tag that refers to the domain name of the expected forwarder. At the time the message is forwarded, the forwarder uses the conventional signature to assess the message, edits the message, and then signs the outgoing message with its own signature. Subsequent recipients observe both the forwarder’s signature and the signature with the !fs tag that matches the other signature, and use either or both to assess the message. If a message arrives with signature containing a !fs but no forwarding signature, the recipient would ignore that signature. That signature would typically be a "weak" signature that covers the From, To, Date, and Message-ID headers but does not cover the Subject header or the message body, so that it would remain valid even if the forwarder makes changes typical of forwarders such as mailing lists.

5. IANA Considerations

IANA is requested to add this entry to the "DKIM-Signature Tag Specifications" registry.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REFERENCE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>!fs</td>
<td>(this document)</td>
<td>active</td>
</tr>
</tbody>
</table>

Table 1: DKIM-Signature Tag Specifications additions

6. Security Considerations

DKIM was designed to provide assurances that a message with a valid signature was received in essentially the same form that it was sent. The forwarding signature condition deliberately creates a loophole for messages intended to be forwarded by entities that edit the message. It opens up a variety of obvious replay attacks that may or may not be important depending on both the selection of target domains for messages to be forwarded, and the behavior of forwarders that receive messages with conditional signatures.

A sender can limit the conceptual size of the loophole by being selective about what other domains it allows in its !fs tags, and by
using the x= tag to limit the time during which forwarded signatures are valid.

7. Change Log

Please remove this section before publication.

7.1. -01 to -02

Change tag character from @ to ! per Murray.

Add suggestions about limiting the forwarding loophole.

8. Normative References


Author’s Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY  14886

Phone: +1 831 480 2300
Email: standards@taugh.com
URI:  http://jl.ly