

Individual Submission
Internet-Draft
Intended status: Experimental
Expires: August 16, 2009

J. Fenton
Cisco Systems, Inc.
February 12, 2009

DKIM Reputation Hint Extension
draft-fenton-dkim-reputation-hint-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 16, 2009.

Copyright Notice

Copyright (c) 2009 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.

Abstract

This document defines an extension to the DomainKeys Identified Mail (DKIM) specification to provide an identifier that may be used as a

Internet-Draft

DKIM Reputation Hint

February 2009

"hint" by reputation services using DKIM wanting to maintain reputation information at a finer level of granularity than that of the signing domain itself.

1. Introduction

DomainKeys Identified Mail (DKIM) [[RFC4871](#)] defines a simple, low cost, and effective mechanism by which email messages can be cryptographically signed, permitting a signing domain to claim responsibility for the use of a given email address. Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.

A frequently cited use for email authentication is that it provides a basis for associating a reputation with the entity claiming responsibility for the message. One way to do this is to associate the reputation with the signing domain itself (the d= value in the DKIM-Signature header field). However, many have expressed the desire to provide more fine-grained information to aid reputation maintainers and users in classifying their mail in a more detailed manner.

Several use cases have been proposed for identifiers of this sort:

- o A domain that supports multiple email addresses (personas) per user may want to apply the same label to all messages from that user so that an aggregate reputation of all of that user's messages may accrue.
- o A domain with a mixture of premium accounts (for which they charge) and free accounts may want to label mail from those accounts differently because of the higher potential for abuse of the free accounts.
- o A domain with a mixture of transactional and other mail may decide to label the transactional mail separately from the other mail because of the low potential of abuse for the transactional mail.

One approach to convey this identifier is to encode this information into the signing identity ("i=" value) in the signature. Since

[[RFC4871](#)] does not explicitly say that the signing identity is an email address (although it specifies an email address-like syntax for this value), either the local-part or the subdomain of the i= value might be available to convey information to reputation systems. However, this approach does not indicate the intent of the signer

that these fields be used for accruing and looking up reputation information, and conflicts with other uses for the signing identity value, such as to denote an email address.

Use of the reputation tag defined herein is entirely at the discretion of the verifier and any reputation algorithm or service that may be associated with the receive-side processing of the message. Verifiers MAY ignore the tag entirely or MAY use the reputation tag value when provided by domains they judge to be reliable.

In order to permit useful reputation accrual, the value of the reputation tag will typically need to be stable over a relatively long period of time. The use of a tag which is independent of other identifiers (such as email address) supports this need by providing continuity, even when other identifiers change.

[1.1](#). Requirements Notation

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](#)].

[2](#). DKIM-Signature r= Tag Specification

In the ABNF below, the FWS token is inherited from [[RFC5322](#)] with the exclusion of obs-FWS. The hyphenated-word token is inherited from [[RFC4871](#)] and the overall ABNF syntax is from [[RFC5234](#)].

The following new tag/value pair is defined for the DKIM-Signature header field:

r= Reputation hint (plain-text; OPTIONAL, default is null value).
This tag is a hint which MAY be used by verifiers and reputation systems for classifying messages at a level of granularity finer

than that of the signing domain. The value of this tag is significant only to the signer. Messages from the same signing domain (d= value) with equal r= values MAY be considered together when accruing and obtaining reputation information. The r= value is significant only within a given signing domain; messages with equal r= values but different d= values MUST NOT be considered together unless information relating the domains is available through a trusted out-of-band mechanism.

ABNF:

```
sig-r-tag    = %x72 [FWS] "=" [FWS] reputation-hint
reputation-hint = hyphenated-word
```

[3.](#) IANA Considerations

This document defines a new tag specification for the DKIM-Signature header field, for which a registry is defined in [\[RFC4871\]](#) [Section 7.1](#). Upon publication of this draft as an RFC, IANA is requested to add an additional tag specification, "r", citing this document as a reference.

[4.](#) Security Considerations

Like other information in DKIM-Signature header fields, the DKIM reputation hint is an assertion on the part of the signer of the message. Since bad actors as well as good actors are able to sign messages with DKIM, it is important to consider how these tags might be abused.

One thing a bad actor might seek to do is to diffuse an adverse reputation by encouraging reputation maintainers to accrue reputation on an extremely fine-grained basis. There is some evidence that bad actors are already signing using domains registered for the purpose of diffusing reputation; the r= value makes it potentially easier to

do that, since it can be changed without the overhead of registering a new domain.

The best defense against this attack is to make use of the r= value in conjunction with some other indication that the d= domain uses this value with good intent. This other indication could be in the form of an aggregate reputation for the signing domain as a whole, or in the form of an accreditation or other reliable out-of-band indication of the good intent of the signing domain's r= assertion.

[5.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4871](#), May 2007.

Fenton

Expires August 16, 2009

[Page 4]

Internet-Draft

DKIM Reputation Hint

February 2009

- [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), January 2008.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", [RFC 5322](#), October 2008.

Author's Address

Jim Fenton
Cisco Systems, Inc.
MS SJ-9/2
170 W. Tasman Drive
San Jose, CA 95134-1706
USA

Phone: +1 408 526 5914
Email: fenton@cisco.com
URI:

Fenton

Expires August 16, 2009

[Page 5]