Individual submission
Internet-Draft
Intended status: Standards Track
Expires: October 17, 2010

M. Kucherawy
Cloudmark

April 15, 2010

Reporting of DKIM Verification Failures
draft-kucherawy-dkim-reporting-07

Abstract

This memo presents an extension to the DomainKeys Identified Mail (DKIM) specifications to allow public keys for verification to include a reporting address to be used to report message verification issues, and extends an Internet Message reporting format to be followed when generating such reports.

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 October 17, 2010.

Table of Contents

1. Introduction

[DKIM] introduced a standard for digital signing of messages for the purposes of sender authentication. There exist cases in which a domain name owner might want to receive reports from verifiers that determine DKIM-signed mail apparently from its domain is failing to verify according to [DKIM] or fails to conform to the domain's published signing practices according to [ADSP].

This document extends [DKIM] and [ADSP] to add an optional reporting address to selector records, an optional means of specifying a desired report format, and furthermore extends [I-D.DRAFT-IETF-MARF-BASE] to add features required for DKIM reporting.

This memo presumes those specifications thus modified will issue as RFCs without these modifications. If the modifications are adopted prior to their publicatons, clearly those sections of this memo can be removed.

2. Definitions

2.1. Keywords

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 [KEYWORDS].

2.2. Imported Definitions

The ABNF token "qp-section" is imported from [MIME].

base64 is defined in [MIME].

3. Optional Key Reporting Address for DKIM

There exist cases in which a domain name owner employing [DKIM] for e-mail signing and authentication may want to know when signatures in use by specific keys are not successfully verifying. Currently there is no such mechanism defined.

This document adds the following two optional "tags" (as defined in [DKIM]) to the DKIM key records, using the form defined in that specification:

r= Reporting Address (plain-text; OPTIONAL; no default). The value MUST be a dkim-quoted-printable string containing the local-part of an e-mail address to which a report SHOULD be sent when mail signed with this key fails verification because either (a) the signature verification itself failed, or (b) the body hash test failed. The format of this reply is selected by the value of the "rf=" tag, defined below. To generate a complete address to which the report is sent, the verifier simply appends to this value an "@" followed by the domain found in the "d=" tag of the signature whose validation failed.

ABNF:

```
key-r-tag = %x72 *WSP "=" *WSP qp-section
```

rf= Reporting Format (plain-text; OPTIONAL; default is "arf"). The value MUST be a colon-separated list of tokens representing desired reporting formats in order of preference. Each element of the list MUST be a token that is taken from the registered list of DKIM report formats. See Section 8 for a description of the registry and Section 6 for a description of recognized formats. The verifier generating reports MUST generate a report using the first token in the list that represents a report format it is capable of generating.

ABNF:

```
rep-format = ( "arf" / "smtp" )

key-rf-tag = %x72 %x66 *WSP "=" *WSP rep-format *WSP 0*( ":" *WSP
rep-format )
```

ri= Requested Report Interval (plain-text; OPTIONAL; default is "0"). The value is an integer that specifies an interval during which no more than one report about a given type of incident should be generated. A value of "0" requests a report for every incident. Where the requested interval is not zero, the agent

generating a report SHOULD include an "Incidents:" field in the generated report so the receiving agent has some indication of how many reports were suppressed.

ABNF:

```
key-ri-tag = %x72 %x69 *WSP "=" *WSP 1*DIGIT
```

ro= Requested Reports (plain-text; OPTIONAL; default is "all"). The value MUST be a colon-separated list of tokens representing those conditions under which a report is desired. See Section 5.1 for a list of valid tags.

ABNF:

```
key-ro-type = ( "all" / "s" / "v" / "x" )

key-ro-tag = %x72 %x6f *WSP "=" *WSP key-ro-type *WSP 0* ( ":"
*WSP key-ro-type )
```

rs= Requested SMTP Error String (plain-text; OPTIONAL; no default). The value is a string the signing domain requests be included in SMTP error strings when messages are rejected.

ABNF:

```
key-rs-tag = %x72 %x73 *WSP "=" qp-section
```

4. Optional Key Reporting Address for DKIM-ADSP

There also exist cases in which a domain name owner employing [ADSP] for announcing signing practises with DKIM may want to know when messages are received without valid author domain signatures. Currently there is no such mechanism defined.

This document adds the following two optional "tags" (as defined in [ADSP]) to the DKIM ADSP records, using the form defined in that specification:

r= Reporting Address (plain-text; OPTIONAL; no default). The value MUST be a dkim-quoted-printable string containing the local-part of an e-mail address to which a report SHOULD be sent when mail claiming to be from this domain failed the verification algorithm described in [ADSP], in particular because a message arrived without a signature that validates, which contradicts what the ADSP record claims, The format of this reply MUST be in the format specified by the "rf=" tag defined below. To generate a complete address to which the report is sent, the verifier simply appends to this value an "@" followed by the domain whose policy was queried in order to evaluate the sender's ADSP.

ABNF:

```
adsp-r-tag = %x72 *WSP "=" qp-section
```

ABNF:

```
key-r-tag = %x72 *WSP "=" qp-section
```

rf= Reporting Format (plain-text; OPTIONAL; default is "arf"). The value MUST be a colon-separated list of tokens representing desired reporting formats in decreasing order of preference. Each element of the list MUST be a token that is taken from the registered list of DKIM report formats. See Section 8 for a description of the registry and Section 6 for a description of recognized formats. The verifier generating reports MUST generate a report using the first token in the list that represents a report format it is capable of generating.

ABNF:

```
adsp-rf-tag = %x72 %x66 *WSP "=" *WSP rep-format *WSP 0*( ":" *WSP
rep-format )
```

ri= Requested Report Interval (plain-text; OPTIONAL; default is "0"). The value is an integer that specifies an interval during which no more than one report about a given type of incident should be generated. A value of "0" requests a report for every incident. Where the requested interval is not zero, the agent generating a report SHOULD include an "Incidents:" field in the generated report so the receiving agent has some indication of how many reports were suppressed.

ABNF:

```
adsp-ri-tag = %x72 %x69 *WSP "=" *WSP 1*DIGIT
```

ro= Requested Reports (plain-text; OPTIONAL; default is "all"). The value MUST be a colon-separated list of tokens representing those conditions under which a report is desired. See Section 5.2 for a list of valid tags.

ABNF:

```
adsp-ro-type = ( "all" / "s" / "u" )

adsp-ro-tag = %x72 %x6f *WSP "=" *WSP adsp-ro-type *WSP 0* ( ":"
*WSP adsp-ro-type )
```

rs= Requested SMTP Error String (plain-text; OPTIONAL; no default). The value is a string the signing domain requests be included in SMTP error strings when messages are rejected.

ABNF:

```
adsp-rs-tag = %x72 %x73 *WSP "=" qp-section
```

5. Requested Reports

This memo also includes, as the "ro" tags defined above, the means by which the sender can request reports for specific circumstances of interest. Verifiers MUST NOT generate reports for incidents that do not match a requested report, and MUST ignore requests for reports not included in this these lists.

5.1. Requested Reports for DKIM Failures

The following report requests are defined for DKIM keys:

all All reports are requested.

s Reports are requested for signature or key syntax errors.

v Reports are requested for signature verification failures or body hash mismatches.

x Reports are requested for signatures rejected by the verifier because the expiration time has passed.

5.2. Requested Reports for DKIM ADSP Failures

The following report requests are defined for DKIM keys:

all All reports are requested.

s Reports are requested for messages that have a valid [DKIM] signature but do not match the published [ADSP] policy.

u Reports are requested for messages that have no valid [DKIM] signature but do not match the published [ADSP] policy.

6. Reporting Formats

This section lists reporting formats supported by this DKIM reporting mechanism. Currently only two formats are supported:

arf: Abuse Reporting Format, as defined in [I-D.DRAFT-IETF-MARF-BASE], and as extended in Section 7.

smtp: An SMTP error with a string descriptive of the problem that caused the DKIM verification to fail. This explicitly requests evaluation of DKIM concurrent with the SMTP session, and rejection (if appropriate) whenever possible rather than acceptance of the message and later generation of a feedback report of some kind (e.g. "arf" above) when verification fails. The presence of an "rs" tag (see Section 3 and Section 4) further requests a specific substring be included in the reply to ease automatic handling of such errors by sending or relaying MTAs.

7. Extension ARF Fields for DKIM Reporting

The current ARF format defined in [I-D.DRAFT-IETF-MARF-BASE] lacks some specific features required to do effective DKIM reporting. This section describes the extensions required to do so and thus required to conform to this specification.

7.1. New ARF Feedback Type

A new feedback type of "dkim" is defined as an extension to Section 8.2 of [I-D.DRAFT-IETF-MARF-BASE]. See Section 8.3 for details.

The field names listed in that draft which may appear for this new feedback type include all shown in the draft except "Reported-URI" and "Removal-Recipient" as they have no semantics relating to DKIM.

7.2. New ARF Header Names

The following new ARF header names are defined as extensions to Section 6.2 of [I-D.DRAFT-IETF-MARF-BASE]:

DKIM-ADSP-DNS: The contents of the DNS TXT record retrieved when trying to determine the author domain's signing practices via the protocol defined in [ADSP].

DKIM-Canonicalized-Body: A base64 encoding of the canonicalized body of the message as generated by the verifier. This header and value MUST be present for reports using feedback type "dkim" when reporting a "bodyhash" failure.

DKIM-Canonicalized-Headers: A base64 encoding of the canonicalized header of the message as generated by the verifier. This header and value MUST be present for reports using feedback type "dkim".

DKIM-Domain: The domain that signed the message, taken from the "d=" tag of the signature. This field value SHOULD be included to ease processing in those cases where reports for multiple domains may be funneled into a single tool.

DKIM-Failure: Indicates the type of DKIM failure that is being reported. The list of valid values is enumerated below. This header and value MUST be present for reports using feedback type "dkim".

DKIM-Identity: The identity of the signature that failed verification, taken from the "i=" tag of the signature. This header and value MUST be present for reports using feedback type "dkim" when reporting anything other than an "asp" failure.

DKIM-Selector: The selector of the signature that failed verification, taken from the "s=" tag of the signature. This header and value MUST be present for reports using feedback type "dkim" when reporting anything other than an "asp" failure.

DKIM-Selector-DNS: The contents of the DNS TXT record retrieved when trying to evaluate the DKIM signature (i.e. a TXT record whose name is assembled from the signature's "s=" and "d=" tags).

The values that are base64 encodings may contain FWS for formatting purposes as per the usual header field wrapping defined in [MAIL]. During decoding, any characters not in the base64 alphabet are ignored so that such line wrapping does not harm the value. The ABNF token "FWS" is defined in [DKIM].

7.3. DKIM Failure Types

The list of defined DKIM failure types, used in the "DKIM-Failure:" header (defined above), is as follows:

adsp: The message did not conform to the sender's published [ADSP] signing practises.

bodyhash: The body hash in the signature and the body hash computed by the verifier did not match.

granularity: The key referenced by the signature on the message was not authorized for use by the sender.

revoked: The key referenced by the signature on the message has been revoked.

signature: The signature on the message did not successfully verify against the header hash and public key.

Supplementary data may be included in the form of [MAIL]-compliant comments. For example, "Failure: asp" could be augmented by a comment to indicate that the failed message was rejected because it was not signed when it should have been. See Appendix B for examples.

8. IANA Considerations

As required by [IANA-CONSIDERATIONS], this section contains registry information for the new [DKIM] key tags, the new [ADSP] tags, and the extensions to [I-D.DRAFT-IETF-MARF-BASE].

8.1. DKIM Key Tag Registration

IANA is requested to update the DKIM Key Tag Specification Registry to include the following new items:

TYPE	REFERENCE
r	(this document)
rf	(this document)
ri	(this document)
ro	(this document)
rs	(this document)

8.2. DKIM ADSP Tag Registration

IANA is requested to update the DKIM ADSP Tag Specification Registry to include the following new items:

TYPE	REFERENCE
r	(this document)
rf	(this document)
ri	(this document)
ro	(this document)
rs	(this document)

8.3. Updates to ARF Feedback Types

The following feedback type is added to the Feedback Report Feedback Type Registry:

Feedback Type: dkim
Description: DKIM failure report
Registration: (this document)

8.4. Updates to ARF Header Names

The following headers are added to the Feedback Report Header Names Registry:

Field Name: DKIM-ADSP-DNS
Description: Retrieved DKIM ADSP record
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Canonicalized-Body
Description: Canonicalized body, per DKIM
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Canonicalized-Headers
Description: Canonicalized headers, per DKIM
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Domain
Description: DKIM signing domain from "d=" tag
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Failure
Description: Type of DKIM failure
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Identity
Description: Identity from DKIM signature
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Selector
Description: Selector from DKIM signature
Multiple Appearances: No
Related "Feedback-Type": dkim

Field Name: DKIM-Selector-DNS
Description: Retrieved DKIM key record
Multiple Appearances: No
Related "Feedback-Type": dkim

9. Security Considerations

Security issues with respect to these DKIM reports are similar to those found in [DSN].

9.1. Inherited Considerations

Implementors are advised to consider the Security Considerations sections of [DKIM], [ADSP] and [I-D.DRAFT-IETF-MARF-BASE].

9.2. Forgeries

These reports may be forged as easily as ordinary Internet electronic mail. User agents and automatic mail handling facilities (such as mail distribution list exploders) that wish to make automatic use of DSNs of any kind should take appropriate precautions to minimize the potential damage from denial-of-service attacks.

Security threats related to forged DSNs include the sending of:

a. A falsified DKIM failure notification when the message was in fact delivered to the indicated recipient;

b. Falsified signature information, such as selector, domain, etc.

Perhaps the simplest means of mitigating this threat is to assert that DKIM reports should themselves be signed. On the other hand, if there's a problem with the DKIM infrastructure at the verifier, signing DKIM failure reports may produce reports that aren't trusted or even accepted by their intended recipients.

9.3. Automatic Generation

Automatic generation of these reports by verifying agents can cause a denial-of-service attack when a large volume of e-mail is sent that causes DKIM verification failures for whatever reason.

It is unclear what a good solution for this issue is. Limiting the rate of generation of these messages may be apropos but threatens to inhibit the distribution of important and possibly time-sensitive information.

9.4. Envelope Sender Selection

In the case of transmitted DKIM reports in the form of a new message, it is necessary to construct the message so as to avoid amplification attacks, deliberate or otherwise. Thus, per Section 2 of [DSN], the envelope sender address of the DKIM report SHOULD be chosen to ensure

that no delivery status reports will be issued in response to the DKIM report itself, and MUST be chosen so that these reports will not generate mail loops. Whenever an SMTP transaction is used to send a DKIM report, the MAIL FROM command MUST use a NULL return address, i.e. "MAIL FROM:<>".

9.5. Reporting Multiple Incidents

If it is known that a particular host generates abuse reports upon certain incidents, an attacker could forge a high volume of messages that will trigger such a report. The recipient of the report could then be innundated with reports. This could easily be extended to a distributed denial-of-service attack by finding a number of report-generating servers.

The incident count referenced in [I-D.DRAFT-IETF-MARF-BASE] provides a limited form of mitigation. The host generating reports may elect to send reports only periodically, with each report representing a number of identical or near-identical incidents. One might even do something inverse-exponentially, sending reports for each of the first ten incidents, then every tenth incident up to 100, then every 100th incident up to 1000, etc. until some period of relative quiet after which the limitation resets.

The use of this for "near-identical" incidents in particular causes a degradation in reporting quality, however. If for example a large number of pieces of spam arrive from one attacker, a reporting agent may decide only to send a report about a fraction of those messages. While this averts a flood of reports to a system administrator, the precise details of each incident are similarly not sent.

10. References

10.1. Normative References

[ADSP] Allman, E., Delany, M., Fenton, J., and J. Levine, "DKIM Sender Signing Practises", RFC 5617, August 2009.

[DKIM] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

[I-D.DRAFT-IETF-MARF-BASE] Shafranovich, Y., Levine, J., Hoffman, P., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", I-D DRAFT-IETF-MARF-BASE, April 2010.

[IANA-CONSIDERATIONS] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[MAIL] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

10.2. Informative References

[DSN] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, January 2003.

Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: JD Falk

Appendix B. Examples

This section contains examples of the use of each of the extensions defined by this memo.

B.1. Example Use of DKIM Key Extension Tags

A DKIM key record including use of the extensions defined by this memo:

```
v=DKIM1; k=rsa; t=y; r=dkim-errors; rf=arf; ro=v:x; p=MIGfMA0GCS
qGSIb3DQEBAQUAA4GNADCBiQKBgQDh2vbhJTijCs2qbyJcwRCa8WqDTxI+PisFJo
faPtoDJy0Qn41uNayCajfKADVcLqc87sXQS6GxfchPfzx7Vh9crYdxRbN/o/URCu
ZsKmym1i1IPTwRLcXSnuKS0XDs1eRW2WQHGYlXksUDqSHWOS3ZO1W5t/FLcZHpIl
l/80xs4QIDAQAB
```

Example 1: DKIM key record using these extensions

This example DKIM key record contains the following data in addition to the basic DKIM key data:

- Reports about signature evaluation failures should be send to the address "dkim-errors" at the sender's domain;
- The sender's domain requests reports in the "arf" format;
- Only reports about signature verification failures and expired signatures should be generated.

B.2. Example Use of DKIM ADSP Extension Tags

A DKIM ADSP record including use of the extensions defined by this memo:

```
dkim=all; r=dkim-adsp-errors; rf=arf; ro=u
```

Example 2: DKIM ADSP record using these extensions

This example ADSP record makes the following assertions:

- The sending domain (i.e. the one that is advertising this policy) signs all mail it sends;
- Reports about ADSP evaluation failures should be send to the address "dkim-adsp-errors" at the sender's domain;
- The sender's domain requests reports in the "arf" format;

- Only reports about unsigned messages should be generated.

B.3. Example Use of ARF Extension Headers

An ARF-formatted report using some of the proposed ARF extension fields:

```
From: arf-daemon@example.com
To: recipient@example.net
Subject: This is a test
Date: Wed, 14 Apr 2010 12:17:45 -0700 (PDT)
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
    boundary="part1_13d.2e68ed54_boundary"

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

This is an email abuse report for an email message received
from IP 192.0.2.1 on Wed, 14 Apr 2010 12:15:31 PDT. For more
information about this format please see
http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: dkim
User-Agent: SomeDKIMFilter/1.0
Version: 1.0
Original-Mail-From: <randomuser@example.net>
Original-Rcpt-To: <user@example.com>
Received-Date: Wed, 14 Apr 2010 12:15:31 -0700 (PDT)
Source-IP: 192.0.2.1
Authentication-Results: mail.example.com; dkim=fail
    header.d=example.net
Reported-Domain: example.net
DKIM-Domain: example.net
DKIM-Failure: bodyhash

--part1_13d.2e68ed54_boundary
Content-Type: message/rfc822

DKIM-Signature: v=1; c=relaxed/simple; a=rsa-sha256;
    s=testkey; d=example.net; h=From:To:Subject:Date;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
     4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
```

```
        KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
        4bmp/YzhwvcubU4=
    Received: from smtp-out.example.net by mail.example.com
        with SMTP id o3F52gxO029144;
        Wed, 14 Apr 2010 12:15:31 -0700 (PDT)
    Received: from internal-client-001.example.com
        by mail.example.com
        with SMTP id o3F3BwdY028431;
        Wed, 14 Apr 2010 12:12:09 -0700 (PDT)
    From: randomuser@example.net
    To: user@example.com
    Date: Wed, 14 Apr 2010 12:12:09 -0700 (PDT)
    Subject: This is a test

    Hi, just making sure DKIM is working!

    --part1_13d.2e68ed54_boundary--
```

Example 3: Example ARF report using these extensions

This example ARF message is making the following assertion:

- DKIM verification of the signature added within "example.net" failed when it was processed on arrival at "mail.example.com".

- The cause for the verification failure was a mismatch between the body contents observed at the verifier and the body hash contained in the signature.

Appendix C. Public Discussion

[REMOVE BEFORE PUBLICATION]

Public discussion of this proposed specification is handled via the mail-vet-discuss@mipassoc.org mailing list. The list is open. Access to subscription forms and to list archives can be found at http://mipassoc.org/mailman/listinfo/mail-vet-discuss.

Author's Address

Murray S. Kucherawy
Cloudmark
128 King St., 2nd Floor
San Francisco, CA 94107
US

Phone: +1 415 946 3800
Email: msk@cloudmark.com