Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

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 April 22, 2010.

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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
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.

Table of Contents

1. Introduction ........................................ 4
2. Definitions ........................................ 5
   2.1. Keywords ...................................... 5
   2.2. Imported Definitions .......................... 5
3. Optional Key Reporting Address for DKIM .................................. 6
4. Optional Key Reporting Address for DKIM-ADSP ............................. 8
5. Requested Reports ................................... 10
   5.1. Requested Reports for DKIM Failures .................. 10
   5.2. Requested Reports for DKIM ADSP Failures ........... 10
6. Reporting Formats ..................................... 11
7. Extension ARF Fields for DKIM Reporting ................................. 12
   7.1. New ARF Feedback Type ........................... 12
   7.2. New ARF Header Names ........................... 12
   7.3. DKIM Failure Types ............................. 13
8. IANA Considerations ................................... 14
   8.1. DKIM Key Tag Registration ......................... 14
   8.2. DKIM ADSP Tag Registration ....................... 14
   8.3. Updates to ARF Feedback Types ..................... 14
   8.4. Updates to ARF Header Names ..................... 15
9. Security Considerations .................................. 16
   9.1. Forgeries ..................................... 16
   9.2. Automatic Generation ........................... 16
   9.3. Envelope Sender Selection ....................... 16
   9.4. Reporting Multiple Incidents ..................... 17
10. References ............................................. 18
   10.1. Normative References ........................... 18
   10.2. Informative References .......................... 18
Appendix A. Acknowledgements .................................. 19
Appendix B. Examples ....................................... 20
  B.1. Example Use of DKIM Key Extension Tags .................. 20
  B.2. Example Use of DKIM ADSP Extension Tags ............... 20
  B.3. Example Use of ARF Extension Headers .................. 21
Appendix C. Public Discussion ................................ 22
Author’s Address .......................................... 23
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 is "Suspicious" according to [I-D.DRAFT-IETF-DKIM-SSP].

This document extends [DKIM] and [I-D.DRAFT-IETF-DKIM-SSP] to add an optional reporting address to selector records, an optional means of specifying a desired report format, and furthermore extends [I-D.DRAFT-SHAFRANOVICH-FEEDBACK-REPORT] 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 publications, 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:**

  \[
  \text{key-r-tag} = \text{%x72 *WSP "=" *WSP qp-section}
  \]

- **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 which 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 which represents a report format it is capable of generating.

  **ABNF:**

  \[
  \text{rep-format} = ( \text{"arf" / "smtp" })
  \]

  \[
  \text{key-rf-tag} = \text{%x72 %x66 *WSP "=" *WSP rep-format *WSP 0*( ":" *WSP rep-format )}
  \]

- **ri=** Requested Report Interval (plain-text; OPTIONAL; default is "0"). The value is an integer which 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:" header 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
[I-D.DRAFT-IETF-DKIM-SSP] for announcing signing practises with DKIM
may want to know when messages are received unsigned or signed with
third-party signatures contrary to the sender’s published policy.
Currently there is no such mechanism defined.

This document adds the following two optional "tags" (as defined in
[I-D.DRAFT-IETF-DKIM-SSP]) 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 [I-D.DRAFT-IETF-DKIM-SSP], in particular because a
message arrived unsigned or signed by a third-party signature in
violation of the sender’s published policy. 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 which 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 which represents a
report format it is capable of generating.

ABNF:
ri= Requested Report Interval (plain-text; OPTIONAL; default is "0"). The value is an integer which 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:" header 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 )
```

ds= 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 which do not match a requested report.

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 for which the ADSP algorithm determines the message is both signed and Suspicious.

u  Reports are requested for messages for which the ADSP algorithm determines the message is both unsigned and Suspicious.
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-SHAFFERNOVICH-REDOCK-REPORT], and as extended in Section 7.

smtp: An SMTP error with a string descriptive of the problem which 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-SHAFRANOVICH-FEEDBACK-REPORT] 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-SHAFRANOVICH-FEEDBACK-REPORT]. See Section 8.3 for details.

The header names listed in that draft which may appear for this new feedback type include all shown in the draft except "Relevant-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 8.1 of [I-D.DRAFT-SHAFRANOVICH-FEEDBACK-REPORT]:

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-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 which 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 which 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.
Incidents: A count of the number of times the cited incident occurred. This permits a limited form of aggregate reporting rather than sending one report message per incident. The absence of this field implies the report refers to a single incident.

The values which 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:

asp: The sender’s published signing practises determined the message is suspicious.

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 tag, the new [I-D.DRAFT-IETF-DKIM-SSP] tag, and the extensions to [I-D.DRAFT-SHAFRANOVICE-FEEDBACK-REPORT].

8.1. DKIM Key Tag Registration

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

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>(this document)</td>
</tr>
<tr>
<td>rf</td>
<td>(this document)</td>
</tr>
<tr>
<td>ri</td>
<td>(this document)</td>
</tr>
<tr>
<td>ro</td>
<td>(this document)</td>
</tr>
<tr>
<td>rs</td>
<td>(this document)</td>
</tr>
</tbody>
</table>

8.2. DKIM ADSP Tag Registration

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

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>(this document)</td>
</tr>
<tr>
<td>rf</td>
<td>(this document)</td>
</tr>
<tr>
<td>ri</td>
<td>(this document)</td>
</tr>
<tr>
<td>ro</td>
<td>(this document)</td>
</tr>
<tr>
<td>rs</td>
<td>(this document)</td>
</tr>
</tbody>
</table>

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-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-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: Incidents
Description: Incident count, for aggregate reporting
Multiple Appearances: No
Related "Feedback-Type": any
9. Security Considerations

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

9.1. 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.

9.2. 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.

9.3. 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:<>".

Kucherawy
Expires April 22, 2010
9.4. 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 which will trigger such a report. The recipient of the report could then be inundated 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 Section 7.2 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


10.2. Informative References

Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: (add names here)
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:

\[ v=DKIM1; k=rsa; t=y; r=dkim-errors; rf=arf; ro=v:x; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDh2vbhJTi jCs2qbyJcwRCa8WqDTxI+PisFJo faPtoDyQn41uNayCajfKADVcLqc87sXQS6GxfchPfzx7Vh9crYdxRbN/o/URCu ZsKmyml11IPTwRLcXSnuKS0XDslER2WQHY1XksUDgSHWOS3ZOlW5t/FLcZHpi l/80xs4QIDAQAB \]

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
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