Reporting of DKIM Verification Failures

draft-kucherawy-dkim-reporting-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79. This document may not be modified, and derivative works of it may not be created.

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.


This Internet-Draft will expire on June 13, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).
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 ........................................ 3
   1.1. Definitions ................................... 3
2. Optional Key Reporting Address for DKIM .................. 4
3. Optional Key Reporting Address for DKIM-SSP .......... 5
4. Requested Reports ..................................... 6
   4.1. Requested Reports for DKIM Failures .......... 6
   4.2. Requested Reports for DKIM SSP Failures .... 6
5. Reporting Formats ..................................... 7
6. Extension ARF Fields for DKIM Reporting .................. 8
   6.1. New ARF Feedback Type ......................... 8
   6.2. New ARF Header Names ......................... 8
   6.3. DKIM Failure Types ............................ 9
7. IANA Considerations .................................. 10
   7.1. DKIM Key Tag Registration .................... 10
   7.2. DKIM SSP Tag Registration ................... 10
   7.3. Updates to ARF Feedback Types ............... 10
   7.4. Updates to ARF Header Names ................. 10
8. Security Considerations ................................ 12
   8.1. Forgeries ................................... 12
   8.2. Automatic Generation ......................... 12
9. References ........................................... 13
   9.1. Normative References ......................... 13
   9.2. Informative References ....................... 13
Appendix A. Acknowledgements ........................... 14
Appendix B. Examples .................................... 15
   B.1. Example Use of DKIM Key Extension Tags ..... 15
   B.2. Example Use of DKIM SSP Extension Tags ..... 15
   B.3. Example Use of ARF Extension Headers ...... 15
Appendix C. To-Do List .................................. 16
Appendix D. Public Discussion ........................... 17
Author’s Address ...................................... 18
Intellectual Property and Copyright Statements .......... 19
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 publicatons, clearly those sections of this memo can be removed.

1.1. 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 [KEYWORDS].
2. 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.

- **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 7 for a description of the registry and Section 5 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.

- **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 4.1 for a list of valid tags.
3. Optional Key Reporting Address for DKIM-SSP

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 SSP 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 SSP.

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 7 for a description of the registry and Section 5 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.

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 4.2 for a list of valid tags.
4. 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.

4.1. 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.

4.2. Requested Reports for DKIM SSP Failures

The following report requests are defined for DKIM keys:

- all  All reports are requested.
- s   Reports are requested for messages for which the SSP algorithm determines the message is both signed and Suspicious.
- u   Reports are requested for messages for which the SSP algorithm determines the message is both unsigned and Suspicious.
5. Reporting Formats

This section lists reporting formats supported by this DKIM reporting mechanism. Currently only one format is supported:

arf: Abuse Reporting Format, as defined in [I-D.DRAFT-SHAFRANOVICH-FEEDBACK-REPORT], and as extended in Section 6.
6. 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.

6.1. 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 7.3 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.

6.2. 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 a "ssp" 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 a "ssp" failure.

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.

base64 is defined in [MIME].

6.3. DKIM Failure Types

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

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.

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

Supplementary data may be included in the form of [MAIL]-compliant comments. For example, "Failure: ssp" 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.
7. 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].

7.1. 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)     |
| ro   | (this document)     |
+-------------------------+

7.2. DKIM SSP Tag Registration

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

+-------------------------+
| TYPE | REFERENCE           |
+-------------------------+
| r    | (this document)     |
| rf   | (this document)     |
| ro   | (this document)     |
+-------------------------+

7.3. 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)

7.4. 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
8. Security Considerations

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

8.1. 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 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. This is under consideration.

8.2. 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. References

9.1. Normative References


9.2. 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
B.2. Example Use of DKIM SSP Extension Tags
B.3. Example Use of ARF Extension Headers
Appendix C. To-Do List

Things still to be done:

- ABNF
- Examples
Appendix D. 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
Sendmail, Inc.
6475 Christie Ave., Suite 350
Emeryville, CA  94608
US

Phone: +1 510 594 5400
Email: msk+ietf@sendmail.com
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).