

**Extensions to DKIM for Failure Reporting**  
**draft-ietf-marf-dkim-reporting-14**

Abstract

This memo presents extensions to the DomainKeys Identified Mail (DKIM) specification to allow for detailed reporting of message authentication failures in an on-demand fashion.

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 September 14, 2012.

Copyright Notice

Copyright (c) 2012 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.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Definitions . . . . .</a>	<a href="#">4</a>
<a href="#">2.1.</a>	<a href="#">Keywords . . . . .</a>	<a href="#">4</a>
<a href="#">2.2.</a>	<a href="#">Imported Definitions . . . . .</a>	<a href="#">4</a>
<a href="#">2.3.</a>	<a href="#">Notation . . . . .</a>	<a href="#">4</a>
<a href="#">2.4.</a>	<a href="#">Other Definitions . . . . .</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">Optional Reporting for DKIM . . . . .</a>	<a href="#">5</a>
<a href="#">3.1.</a>	<a href="#">Extension DKIM Signature Tag . . . . .</a>	<a href="#">5</a>
<a href="#">3.2.</a>	<a href="#">DKIM Reporting TXT Record . . . . .</a>	<a href="#">5</a>
<a href="#">3.3.</a>	<a href="#">DKIM Reporting Algorithm . . . . .</a>	<a href="#">7</a>
<a href="#">4.</a>	<a href="#">Optional Reporting Address for DKIM-ADSP . . . . .</a>	<a href="#">9</a>
<a href="#">5.</a>	<a href="#">Requested Reports . . . . .</a>	<a href="#">11</a>
<a href="#">5.1.</a>	<a href="#">Requested Reports for DKIM Failures . . . . .</a>	<a href="#">11</a>
<a href="#">5.2.</a>	<a href="#">Requested Reports for DKIM ADSP Failures . . . . .</a>	<a href="#">11</a>
<a href="#">6.</a>	<a href="#">Report Generation . . . . .</a>	<a href="#">13</a>
<a href="#">6.1.</a>	<a href="#">Report Format . . . . .</a>	<a href="#">13</a>
<a href="#">6.2.</a>	<a href="#">Other Guidance . . . . .</a>	<a href="#">13</a>
<a href="#">7.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">14</a>
<a href="#">7.1.</a>	<a href="#">DKIM Signature Tag Registration . . . . .</a>	<a href="#">14</a>
<a href="#">7.2.</a>	<a href="#">DKIM ADSP Tag Registration . . . . .</a>	<a href="#">14</a>
<a href="#">7.3.</a>	<a href="#">DKIM Reporting Tag Registry . . . . .</a>	<a href="#">14</a>
<a href="#">8.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">16</a>
<a href="#">8.1.</a>	<a href="#">Inherited Considerations . . . . .</a>	<a href="#">16</a>
<a href="#">8.2.</a>	<a href="#">Report Volume . . . . .</a>	<a href="#">16</a>
<a href="#">8.3.</a>	<a href="#">Deliberate Misuse . . . . .</a>	<a href="#">16</a>
<a href="#">8.4.</a>	<a href="#">Unreported Fraud . . . . .</a>	<a href="#">17</a>
<a href="#">9.</a>	<a href="#">References . . . . .</a>	<a href="#">18</a>
<a href="#">9.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">18</a>
<a href="#">9.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">19</a>
<a href="#">Appendix A.</a>	<a href="#">Acknowledgements . . . . .</a>	<a href="#">20</a>
<a href="#">Appendix B.</a>	<a href="#">Examples . . . . .</a>	<a href="#">21</a>
<a href="#">B.1.</a>	<a href="#">Example Use of DKIM Signature Extension Tag . . . . .</a>	<a href="#">21</a>
<a href="#">B.2.</a>	<a href="#">Example DKIM Reporting TXT Record . . . . .</a>	<a href="#">21</a>
<a href="#">B.3.</a>	<a href="#">Example Use of DKIM ADSP Extension Tags . . . . .</a>	<a href="#">22</a>
	<a href="#">Author's Address . . . . .</a>	<a href="#">23</a>



## **1. Introduction**

DomainKeys Identified Mail [[DKIM](#)] introduced a mechanism for message signing and authentication. It uses digital signing to associate a domain name with a message in a reliable (i.e. not easily forged) manner. The output is a verified domain name that can then be subjected to some sort of evaluation process (e.g., advertised sender policy, comparison to a known-good list, submission to a reputation service, etc.).

Deployers of message authentication technologies are increasingly seeking visibility into DKIM verification failures and conformance failures involving the published signing practices (e.g., Author Domain Signing Practices, [[ADSP](#)]) of an Administrative Management Domain (ADMD; see [[EMAIL-ARCH](#)]).

This document extends [[DKIM](#)] and [[ADSP](#)] to add an optional reporting address and some reporting parameters. Reports are generated using the format defined in [[I-D.IETF-MARF-AUTHFAILURE-REPORT](#)].



## **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](#)].

Numerous DKIM-specific terms used here are defined in [[DKIM](#)]. The definition of the ABNF token "domain-name" can also be found there.

### **2.3. Notation**

Certain properties of email messages described in this document are referenced using notation found in [[EMAIL-ARCH](#)] (e.g., "[RFC5322](#).From").

### **2.4. Other Definitions**

report generator: A report generator is an entity that generates and sends reports. For the scope of this memo, the term refers to Verifiers, as defined in Section 2.2 of [[DKIM](#)], designed also to generate authentication failure reports according to this specification.



### **3. Optional Reporting for DKIM**

A domain name owner employing [\[DKIM\]](#) for email signing and authentication might want to know when signatures that ought to be verifiable with specific public keys are not successfully verifying. Currently there is no such mechanism defined.

This document adds optional "tags" (as defined in [\[DKIM\]](#)) to the DKIM-Signature header field and the DKIM key record in the DNS, using the formats defined in that specification.

#### **3.1. Extension DKIM Signature Tag**

The following tag is added to DKIM-Signature header fields when a Signer wishes to request that reports of failed verifications be generated by a Verifier:

r= Reporting Requested (plain-text; OPTIONAL; no default). If present, this tag indicates that the Signer requests that Verifiers generate a report when verification of the DKIM signature fails. At present, the only legal value is the single character "y" (in either upper or lower case). A complete description and illustration of how this is applied can be found in [Section 3.3](#).

ABNF:

```
sig-r-tag = %x72 *WSP "=" *WSP "y"
```

#### **3.2. DKIM Reporting TXT Record**

When a Signer wishes to advertise that it wants to receive failed verification reports, it places in the DNS a TXT resource record (RR). The RR is made up of a sequence of tag-value objects (much like DKIM key records, as defined in Section 3.6.1 of [\[DKIM\]](#)), but it is entirely independent of those key records and is found at a different name. In the case of a record advertising the desire for authentication failure reports, the tags and values comprise the parameters to be used when generating the reports. A report generator will request the content of this record when it sees an "r=" tag in a DKIM-Signature header field.

Section 3.6.2.2 of [\[DKIM\]](#) provides guidance with respect to handling of a TXT RR that comprises multiple distinct strings ("character-strings" in the parlance of [\[DNS\]](#)). The same process MUST be applied here.

Implementations MUST support all tags defined in this document, and





any other tag found in the content of the record that is not recognized by an implementation MUST be ignored. See [Section 7.3](#) for details about finding or registering extension tags.

The initial list of tags supported for the reporting TXT record is as follows:

ra= Reporting Address (plain-text; OPTIONAL). A dkim-quoted-printable string (see Section 2.11 of [\[DKIM\]](#)) containing the local-part of an email address to which a report SHOULD be sent when mail fails DKIM verification for one of the reasons enumerated below. The value MUST be interpreted as a local-part only. To construct the actual address to which the report is sent, the Verifier simply appends to this value an "@" followed by the domain name found in the "d=" tag of the DKIM-Signature header field. Therefore, an ADMD making use of this specification MUST ensure that an email address thus constructed can receive reports generated as described in [Section 6](#). ABNF:

```
rep-ra-tag = %x72.61 *WSP "=" *WSP qp-section
```

rp= Requested Report Percentage (plain-text; OPTIONAL; default is "100"). The value is an integer from 0 to 100 inclusive that indicates what percentage of incidents of signature authentication failures, selected at random, are to cause reports to be generated. The report generator SHOULD NOT issue reports for more than the requested percentage of incidents. Report generators MAY make use of the "Incidents:" field in [\[ARF\]](#) to indicate that there are more reportable incidents than there are reports. ABNF:

```
rep-rp-tag = %x72.70 *WSP "=" *WSP 1*3DIGIT
```

rr= 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:

```
rep-rr-type = ( "all" / "d" / "o" / "p" / "s" / "u" / "v" / "x" )
rep-rr-tag = %x72.72 *WSP "=" *WSP rep-rr-type
           *WSP 0* ( ":" *WSP rep-rr-type )
```

rs= Requested SMTP Error String (text; OPTIONAL; no default). The value is a dkim-quoted-printable string that the publishing ADMD requests be included in [\[SMTP\]](#) error strings if messages are rejected during the delivery SMTP session. ABNF:

```
rep-rs-tag = %x72.73 *WSP "=" qp-section
```



In the absence of an "ra=" tag, the "rp=" and "rr=" tags MUST be ignored, and the report generator MUST NOT issue a report.

### **3.3. DKIM Reporting Algorithm**

Report generators MUST apply the following algorithm, or one semantically equivalent to it, for each DKIM-Signature header field whose verification fails for some reason. Note that this processing is done as a reporting extension only; the outcome of the specified DKIM evaluation MUST be otherwise unaffected.

1. If the DKIM-Signature field did not contain a valid "r=" tag, terminate.
2. Issue a [\[DNS\]](#) TXT query to the name that results from appending the value of the "d=" tag in the DKIM-Signature field to the string "\_report.\_domainkey.". For example, if the DKIM-Signature header field contains "d=example.com", issue a DNS TXT query to "\_report.\_domainkey.example.com".
3. If the DNS query returns anything other than RCODE 0 (NOERROR), or if multiple TXT records are returned, terminate.
4. If the resultant TXT is in several string fragments, concatenate them as described in Section 3.6.2.2 of [\[DKIM\]](#).
5. If the TXT content is syntactically invalid (see [Section 3.2](#)), terminate.
6. If the reason for the signature evaluation failure does not match one of the report requests found in the "rr=" tag (or its default value), terminate.
7. If a report percentage ("rp=") tag was present, select a random number between 0 and 99, inclusive; if the selected number is not lower than the tag's value, terminate.
8. If no "ra=" tag was present, skip this step and the next one. Otherwise, determine the reporting address by extracting the value of the "ra=" tag and appending to it "@" followed by the domain name found in the "d=" tag of the DKIM-Signature header field.
9. Construct and send a report in compliance with [Section 6](#) of this memo that includes as its intended recipient the address constructed in the previous step.



10. If the [\[SMTP\]](#) session during which the DKIM signature was evaluated is still active and the SMTP server has not already given its response to the DATA command that relayed the message, and an "rs=" tag was present in the TXT record, the SMTP server SHOULD include the decoded string found in the "rs=" tag in its SMTP reply to the DATA command.

In order to thwart attacks that seek to convert report generators into unwitting denial-of-service attack participants, a report generator SHOULD NOT issue more than one report to any given domain as a result of a single message. Further, a report generator SHOULD establish an upper bound on the number of reports a single message can generate overall. For example, a message with three invalid signatures, two from example.com and one from example.net, would generate at most one report to each of those domains.

This algorithm has the following advantages over previous pre-standardization implementations, such as early versions of [\[OPENDKIM\]](#):

- a. If the DKIM signature fails to verify, no additional DNS check is made to see if reporting is requested; the request is active in that it is included in the DKIM-Signature header field. (Previous implementations included the reporting address in the DKIM key record, which is not queried for certain failure cases. This meant, for full reporting, that the key record had to be retrieved even when it was not otherwise necessary.)
- b. The request is confirmed by the presence of a corresponding TXT record in the DNS, since the Signer thus provides the parameters required to construct and send the report. This means a malicious Signer cannot falsely assert that someone else wants failure reports and cause unwanted mail to be generated. It can cause additional DNS traffic against the domain listed in the "d=" signature tag, but negative caching of the requested DNS record will help to mitigate this issue.
- c. It is not possible for a Signer to direct reports to an email address outside of its own domain, preventing distributed email-based denial-of-service attacks.

See [Section 8.4](#) for some considerations regarding limitations of this mechanism.



#### 4. Optional 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 optional "tags" (as defined in [ADSP]) to the DKIM ADSP records, using the form defined in that specification:

ra= Reporting Address (plain-text; OPTIONAL; no default). The value MUST be a dkim-quoted-printable string containing the local-part of an email 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 value MUST be interpreted as a local-part only. To construct the actual 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, i.e., the RFC5322.From domain of the message under evaluation. Therefore, a signer making use of this extension tag MUST ensure that an email address thus constructed can receive reports generated as described in Section 6. ABNF:

```
adsp-ra-tag = %x72.61 *WSP "=" qp-section
```

rp= Requested Report Percentage (plain-text; OPTIONAL; default is "100"). The value is a single integer from 0 to 100 inclusive that indicates what percentage of incidents of ADSP evaluation failures, selected at random, should cause reports to be generated. The report generator SHOULD NOT issue reports for more than the requested percentage of incidents. An exception to this might be some out-of-band arrangement between two parties to override it with some mutually agreed value. Report generators MAY make use of the "Incidents:" field in [ARE] to indicate that there are more reportable incidents than there are reports. ABNF:

```
adsp-rp-tag = %x72.70 *WSP "=" *WSP 1*3DIGIT
```

rr= 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-rr-type = ( "all" / "o" / "p" / "s" / "u" )
adsp-rr-tag = %x72.72 *WSP "=" *WSP adsp-rr-type
```





\*WSP 0\* ( ":" \*WSP adsp-rr-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 during a single  
SMTP session. ABNF:

adsp-rs-tag = %x72.73 \*WSP "=" qp-section

In the absence of an "ra=" tag, the "rp=" and "rr=" tags MUST be  
ignored, and the report generator MUST NOT issue a report.

## **5. Requested Reports**

This memo also includes, as the "rr" tags defined above, the means by which the signer 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 list.

### **5.1. Requested Reports for DKIM Failures**

The following report requests are defined for DKIM keys:

all All reports are requested.

- d Reports are requested for signature evaluation errors that resulted from DNS issues (e.g., key retrieval problems).
- o Reports are requested for any reason related to DKIM signature evaluation not covered by other report requests listed here.
- p Reports are requested for signatures that are rejected for local policy reasons at the Verifier that are related to DKIM signature evaluation.
- s Reports are requested for signature or key syntax errors.
- u Reports are requested for signatures that include unknown tags in the signature field.
- 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 ADSP records:

all All reports are requested.

- o Reports are requested for any [\[ADSP\]](#)-related failure reason not covered by other report requests listed here.
- p Reports are requested for messages that are rejected for local policy reasons at the Verifier that are related to [\[ADSP\]](#).



- 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 and do not match the published [[ADSP](#)] policy.

## **6. Report Generation**

This section describes the process for generating and sending reports in accordance with the request of the signer and/or sender as described above.

### **6.1. Report Format**

All reports generated as a result of requests contained in these extension parameters MUST be generated in compliance with [\[ARF\]](#) and its extension specific to this work, [\[I-D.IETF-MARF-AUTHFAILURE-REPORT\]](#).

### **6.2. Other Guidance**

Additional guidance about the generation of these reports can be found in [\[I-D.IETF-MARF-AS\]](#), especially [Section 9](#).



## 7. IANA Considerations

As required by [[IANA-CONSIDERATIONS](#)], this section contains registry information for the new [[DKIM](#)] signature tags, and the new [[ADSP](#)] tags. It also creates a DKIM reporting tag registry.

### 7.1. DKIM Signature Tag Registration

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

+-----+	+-----+	+-----+
TYPE	REFERENCE	STATUS
+-----+	+-----+	+-----+
r	(this document)	active
+-----+	+-----+	+-----+

### 7.2. DKIM ADSP Tag Registration

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

+-----+	+-----+
TYPE	REFERENCE
+-----+	+-----+
ra	(this document)
rp	(this document)
rr	(this document)
rs	(this document)
+-----+	+-----+

### 7.3. DKIM Reporting Tag Registry

IANA is requested to create a sub-registry of the DKIM Parameters registry called "DKIM Reporting Tags". Additions to this registry follow the "Specification Required" rules, with the following columns required for all registrations:

Type: The name of the tag being used in reporting records

Reference: The document that specifies the tag being defined

Status: The status of the tag's current use, either "active" indicating active use, or "historic" indicating discontinued or deprecated use

The initial registry entries are as follows:





+-----+-----+-----+		
TYPE	REFERENCE	STATUS
+-----+-----+-----+		
ra	(this document)	active
rp	(this document)	active
rr	(this document)	active
rs	(this document)	active
+-----+-----+-----+		

## **8. Security Considerations**

Security issues with respect to these reports are similar to those found in [\[DSN\]](#).

### **8.1. Inherited Considerations**

Implementers are advised to consider the Security Considerations sections of [\[DKIM\]](#), [\[ADSP\]](#), [\[I-D.IETF-MARF-AS\]](#), and [\[I-D.IETF-MARF-AUTHFAILURE-REPORT\]](#). Many security issues related to this draft are already covered in those documents.

### **8.2. Report Volume**

It is impossible to predict the volume of reports this facility will generate when enabled by a report receiver. An implementer ought to anticipate substantial volume, since the amount of abuse occurring at receivers cannot be known ahead of time, and may vary rapidly and unpredictably.

### **8.3. Deliberate Misuse**

Some threats caused by deliberate misuse of this mechanism are discussed in [Section 3.3](#), but they warrant further discussion here.

Negative caching offers some protection against this pattern of abuse, although it will work only as long as the negative time-to-live on the relevant SOA record in the DNS.

The presence of the DNS record that indicates willingness to accept reports opens the recipient to abuse. In particular, it is possible for an attacker to attempt to cause a flood of reports toward the domain identified in a signature's "d=" tag in one of these ways:

1. Alter existing DKIM-Signature header fields by adding an "r=y" tag (and possibly altering the "d=" tag to point at the target domain);
2. Add a new but bogus signature bearing an "r=y" tag and a "d=" tag pointing at the target domain;
3. Generate a completely new message bearing an "r=y" tag and a "d=" tag pointing at the target domain.

Consider, for example, the situation where an attacker sends out a multi-million-message spam run, and includes in the messages a fake DKIM signature containing "d=example.com; r=y". It won't matter that those signatures couldn't possibly be real: each will fail



verification, and any implementations that support this specification will report those failures, in the millions and in short order, to example.com.

Implementers are therefore strongly advised not to advertise that DNS record except when reports desired, including the risk of receiving this kind of attack.

Positive caching of this DNS reply also means turning off the flow of reports by removing the record is not likely to have immediate effect. A low time-to-live on the record needs to be considered.

#### **8.4. Unreported Fraud**

An attacker can craft fraudulent DKIM-Signature fields on messages, without using "r=" tags, and avoid having these reported. The procedure described in [Section 3.3](#) does not permit the detection and reporting of such cases.

It might be useful to some Signers to receive such reports, but the mechanism does not support it. To offer such support, a Verifier would have to violate the first step in the procedure and continue even in the absence of an "r=" tag. Although that would enable the desired report, it would also create a possible denial-of-service attack: such Verifiers would always look for the reporting TXT record, so a generator of fraudulent messages could simply send a large volume of messages without an "r=" tag to a number of destinations. To avoid that outcome, reports of fraudulent DKIM-Signature header fields are not possible using the published mechanism.



## **9. References**

### **9.1. Normative References**

- [ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 5234](#), January 2008.
- [ADSP] Allman, E., Delany, M., Fenton, J., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", [RFC 5617](#), August 2009.
- [ARF] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", [RFC 5965](#), August 2010.
- [DKIM] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", [RFC 6376](#), September 2011.
- [DNS] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", [RFC 5598](#), October 2008.
- [I-D.IETF-MARF-AS] Falk, J. and M. Kucherawy, Ed., "Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF)", [draft-ietf-marf-as](#) (work in progress), January 2012.
- [I-D.IETF-MARF-AUTHFAILURE-REPORT] Fontana, H., "Authentication Failure Reporting using the Abuse Report Format", [draft-ietf-marf-authfailure-report](#) (work in progress), January 2012.
- [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.
- [MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", [RFC 2045](#), November 1996.





[SMTP] Klensin, J., "Simple Mail Transfer Protocol", [RFC 5321](#), October 2008.

## **9.2. Informative References**

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

[OPENDKIM] Kucherawy, M., "OpenDKIM -- Open Source DKIM Library and Filter", August 2009, <<http://www.opendkim.org>>.

**[Appendix A](#). Acknowledgements**

The authors wish to acknowledge the following for their review and constructive criticism of this proposal: Steve Atkins, Monica Chew, Dave Crocker, Tim Draegen, Frank Ellermann, JD Falk, John Levine, Scott Kitterman, and Andrew Sullivan.

## [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 Signature Extension Tag

A DKIM-Signature field including use of the extension tag defined by this memo:

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;  
                d=example.com; s=jan2012; r=y;  
                h=from:to:subject:date:message-id;  
                bh=YJAYwiNdc3wMh6TD8FjVhtmxahYHo7Z/06kHQYvQ4tQ=;  
                b=jHF3tpgqr6nH/icHKIqFK2IJPtCLF0CRJaz2Hj1Y8yNwTJ  
                IMYIZtLccho3ymGF2GYqvTl2nP/cn4dH+55rH5pqkWNnuJ  
                R9z54CFcanoKKcl9wOZzK9i5KxM0DTzfs0r8
```

Example 1: DKIM-Signature field using this extension

This example DKIM-Signature field contains the "r=" tag that indicates reports are requested on verification failure.

Assuming the public key retrieved from the DNS and processed according to [\[DKIM\]](#) would determine that the signature is invalid, a TXT query will be sent to "\_report.\_domainkey.example.com" to retrieve a reporting address and other report parameters as described in [Section 3.3](#).

### [B.2](#). Example DKIM Reporting TXT Record

An example DKIM Reporting TXT Record as defined by this memo:

```
ra=dkim-errors; rp=100; rr=v:x
```

Example 2: Example DKIM Reporting TXT Record

This example, continuing from the previous one, shows a message that might be found at "\_report.\_domainkey.example.com" in a TXT record. It makes the following requests:

- o Reports about signature evaluation failures should be sent to the address "dkim-errors" at the signer's domain;
- o All (100%) incidents should be reported;
- o Only reports about signature verification failures and expired signatures should be generated.



### **B.3. Example Use of DKIM ADSP Extension Tags**

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

```
dkim=all; ra=dkim-adsp-errors; rr=u
```

Example 3: DKIM ADSP record using these extensions

This example ADSP record makes the following assertions:

- o The sending domain (i.e. the one that is advertising this policy) signs all mail it sends;
- o Reports about ADSP evaluation failures should be send to the address "dkim-adsp-errors" at the Author's domain;
- o Only reports about unsigned messages should be generated.



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