

Individual Submission
Internet-Draft
Intended status: Standards Track
Expires: March 3, 2007

E. Allman
Sendmail, Inc.
M. Delany
Yahoo! Inc.
J. Fenton
Cisco Systems, Inc.
August 30, 2006

DKIM Sender Signing Practices
draft-allman-dkim-ssp-02

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](#).

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 March 3, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

DomainKeys Identified Mail (DKIM) defines a domain-level authentication framework for email using public-key cryptography and key server technology to permit verification of the source and contents of messages by either Mail Transport Agents (MTAs) or Mail User Agents (MUAs). The primary DKIM protocol is described in

[[I-D.ietf-dkim-base](#)].

This document describes the records that senders may use to advertise how they sign their outgoing mail, and how verifiers should access and interpret those results.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

(Unresolved Issues/To Be Done)

Security Considerations needs further work.

Need to check existing ABNF.

Text structure of document needs to be examined; this is a quick slash-and-burn approach.

Table of Contents

1.	Introduction	4
2.	Language and Terminology	5
2.1.	Terms Imported from DKIM-Base	5
2.2.	Valid Signature	5
2.3.	Originator Address	5
2.4.	Alleged Signer	6
2.5.	Alleged Originator	6
2.6.	Sender Signing Practices	6
2.7.	Originator Signature	6
2.8.	Suspicious	6
2.9.	Third-Party Signature	6
2.10.	Verifier Acceptable Third-Party Signature	7
3.	Operation Overview	7
4.	Detailed Description	8
4.1.	DNS Representation	8
4.2.	Record Syntax	9
4.3.	Sender Signing Practices Check Procedure	11
5.	Third-Party Signatures and Mailing Lists	12
5.1.	Mailing List Manager Actions	13
5.2.	Signer Actions	13
6.	IANA Considerations	14
7.	Security Considerations	14
7.1.	Fraudulent Sender Address	14
7.2.	DNS Attacks	14
8.	References	15
8.1.	Normative References	15
8.2.	Informational References	15
Appendix A.	Change Log	15
A.1.	Changes since -01	15
A.2.	Changes since -00	16
	Authors' Addresses	16
	Intellectual Property and Copyright Statements	18

1. Introduction

DomainKeys Identified Mail (DKIM) defines a mechanism by which email messages can be cryptographically signed, permitting a signing domain to claim responsibility for the introduction of a message into the mail stream. Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.

However, the legacy of the Internet is such that not all messages will be signed, and the absence of a signature on a message is not an a priori indication of forgery. In fact, during early phases of deployment it must be expected that most messages will remain unsigned. However, some domains may choose to sign all of their outgoing mail, for example, to protect their brand name. It is highly desirable for such domains to be able to advertise that fact to verifiers, and that messages claiming to be from them that do not have a valid signature are likely to be forgeries. This is the topic for sender signing practices.

In the absence of a valid DKIM signature on behalf of the "From" address [[RFC2822](#)], the verifier of a message MUST determine whether messages from that sender are expected to be signed, and what signatures are acceptable. In particular, whether a domain signs all outbound email must be communicated to the verifier. Without such a mechanism, the benefit of message signing techniques such as DKIM is limited since unsigned messages will always need to be considered to be potentially legitimate. This determination is referred to as a Sender Signing Practices check.

Sender Signing Practices MAY be expressed on behalf of an entity which may be a domain or an individual address. Expression of signing practices on behalf of individual addresses will, of course, entail additional transaction load.

Conceivably, such expressions might be imagined to be extended in the future to include information about what hashing algorithms a domain uses, what kind of messages might be sent (e.g., bulk vs. personal vs. transactional), etc. Such concerns are out of scope of this standard, because they can be expressed in the key record ("Selector") with which the signature is verified. Expressions of signing practice which require outside auditing are out of scope for this specification because they fall under the purview of reputation and accreditation.

This document refers extensively to [[I-D.ietf-dkim-base](#)], which should be read as a prerequisite to this document.

2. Language and Terminology

2.1. Terms Imported from DKIM-Base

Some terminology used herein is derived directly from [\[I-D.ietf-dkim-base\]](#). Briefly,

- o A "Signer" is the agent that signs a message. In many cases it will correspond closely with the original author of the message or an agent working on the author's behalf.

- o A "Verifier" is the agent that verifies a message by checking the actual signature against the message itself and the public key published by the alleged signer. The Verifier also looks up the Sender Signing Practices published by the domain of the Originator Address if the message is not correctly signed by the Alleged Originator.

- o A "Selector" specifies which of the keys published by a signing domain should be queried. It is essentially a way of subdividing the address space to allow a single sending domain to publish multiple keys.

2.2. Valid Signature

A "Valid Signature" is any signature on a message which correctly verifies using the procedure described in section 6.1 of [\[I-D.ietf-dkim-base\]](#).

2.3. Originator Address

The "Originator Address" is the email address in the From header field of a message [\[RFC2822\]](#), or if and only if the From header field contains multiple addresses, the first address in the From header field.

NON-NORMATIVE RATIONALE: The alternative option when there are multiple addresses in the From header field is to use the value of the Sender header field. This would be closer to the semantics indicated in [\[RFC2822\]](#) than using the first address in the From header field. However, the large number of deployed Mail User Agents that do not display the Sender header field value argues against that. Multiple addresses in the From header field are rare in real life.

2.4. Alleged Signer

An "Alleged Signer" is the identity of the signer claimed in the DKIM-Signature header field in a message received by a Verifier; it is "alleged" because it has not yet been verified.

2.5. Alleged Originator

An "Alleged Originator" is the Originator Address of a message received by a Verifier; it is "alleged" because it has not yet been verified.

2.6. Sender Signing Practices

"Sender Signing Practices" (or just "practices") consist of a machine-readable record published by the domain of the Alleged Originator which includes information about whether or not that entity signs all of their email, and whether signatures from third parties are sanctioned by the Alleged Originator.

2.7. Originator Signature

An "Originator Signature" is any Valid Signature where the signing address (listed in the "i=" tag if present, otherwise the null address, representing an unknown user, followed by "@", followed by the value of the "d=" tag) matches the address in the "From" header field. If the signing address does not include a local-part, then only the domains must match; otherwise, the two addresses must be identical.

2.8. Suspicious

Messages that do not contain a valid Originator Signature and which are inconsistent with a Sender Signing Practices check (e.g., are received without a Valid Signature and the sender's signing practices indicate all messages from the entity are signed) are referred to as "Suspicious". The handling of such messages is at the discretion of the Verifier or final recipient. "Suspicious" applies only to the DKIM layer; a Verifier may decide the message should be accepted on the basis of other information beyond the scope of this document. Conversely, messages deemed non-Suspicious may be rejected for other reasons.

2.9. Third-Party Signature

A "Third-Party Signature" is a Valid Signature which is not an Originator Signature.

2.10. Verifier Acceptable Third-Party Signature

A Verifier Acceptable Third-Party Signature is a Third-Party Signature that the Verifier is willing to accept as meaningful for the message under consideration. The Verifier may use any criteria it deems appropriate for making this determination.

3. Operation Overview

Sender Signing Practices checks MUST be based on the Originator Address. If the message contains a valid Originator Signature, no Sender Signing Practices check need be performed: the Verifier SHOULD NOT look up the Sender Signing Practices and the message SHOULD be considered non-Suspicious.

Verifiers checking messages that do not have at least one valid Originator Signature MUST perform a Sender Signing Practices check on the domain specified by the Originator Address as described in [Section 4.3](#).

The result of a Sender Signing Practices check is one of five possible practices:

- (1) Some messages from this entity are not signed; the message SHOULD be presumed to be legitimate in the absence of a valid signature. This is the default.
- (2) All messages from this entity are signed; all messages from this entity SHOULD have a Valid Signature, either directly on behalf of the originator or on behalf of a third party (e.g., a mailing list or an outsourcing house) handling the message.
- (3) All valid messages from this entity are signed, and SHOULD have a Valid Signature from this entity. Third-Party Signatures SHOULD not be accepted.
- (4) Signing practices for this domain are expressed at the individual address level. A second Sender Signing Practices check MUST be performed specifying the individual address.
- (5) The domain does not exist.

If a message is encountered by a Verifier without a valid Originator Signature, the results MUST be interpreted as follows:

If the result of the check is practice (1) described above, the message MUST be considered non-Suspicious.

If the result of the check is practice (2), and any verifiable signature is present from some signer other than the Originator Address in the message, the message SHOULD be considered non-Suspicious.

If the result of the check is practice (3) or (5), the message MUST be considered Suspicious.

If the result of the check is practice (4), a second Sender Signing Practices check SHOULD be performed based on the entire Originator Address and interpreted using the above steps. If no signing practices are published at the user level, the signing practices of the domain should be used instead and interpreted as described above.

If the Sender Signing Practices record for the domain does not exist but the domain does exist, Verifier systems MUST assume that some messages from this entity are not signed and the message SHOULD NOT be considered to be Suspicious.

4. Detailed Description

4.1. DNS Representation

Sender Signing Practices records are published using the "DKIMP" DNS resource record type. The numeric record type for DKIMP is [[TBD]].

The RDATA for DKIMP resource records is textual in format, like that of TXT records but with specific syntax and semantics relating to their role in describing sender signing practices. The "Tag=Value List" syntax described in section 3.2 of [\[I-D.ietf-dkim-base\]](#) is used. Records not in compliance with that syntax or the syntax of individual tags described in [Section 4.2](#) MUST be ignored (considered equivalent to a NODATA result) for purposes of message disposition, although they MAY cause the logging of warning messages via an appropriate system logging mechanism.

SSP records for a domain are published at the domain's location (e.g., example.com) in the DNS hierarchy. SSP records for individual addresses are published at "<user>._user.<domain>" (e.g., jdoe._user.example.com), with any characters not permitted in DNS labels removed and with the resulting label truncated, if necessary, at 63 characters per [section 2.3.1 of \[RFC1035\]](#).

NON-NORMATIVE RATIONALE: Use of a separate resource record allows the Verifier to determine whether the domain exists in addition to the existence of an SSP record with a single query. Use of the

"_user" separator in the user-level query prevents the publication of practices for the subdomain `jdoe.example.com` from conflicting with user-level practices for `<jdoe@example.com>`.

Since the Domain Name System returns a NODATA, rather than an NXDOMAIN (nonexistent domain) response for any record, such as a hostname, for which there is a record of any resource record type, a query for the signing practices of such a name would indicate that there are no signing practices for the address, which might be undesirable. Conversely, the burden of publishing SSP records for all such names could be considerable.

To address this problem, when a domain-level SSP query returns a NODATA response, the Verifier MUST repeat the query to the next higher level of the domain hierarchy unless the query is already at the top-level. This allows hostnames and other identifiers that may be used in Originator Addresses to inherit the signing practices of their parent domain. Bona fide subdomains SHOULD publish separate SSP records; otherwise, hostnames and other identifiers in subdomains will result in the Verifier not finding the SSP record.

4.2. Record Syntax

Signing practices records follow the tag-value syntax described in section 3.2 of [[I-D.ietf-dkim-base](#)]. Tags used in SSP records are as follows. Unrecognized tags and tags with illegal values MUST be ignored. In the ABNF below, the FWS token is inherited from [[RFC2822](#)] with the exclusion of obs-FWS. The ALPHA and DIGIT tokens are imported from [[RFC4234](#)].

p= Outbound signing practices for the entity (plain-text; OPTIONAL, default is "unknown"). Possible values are as follows:

unknown The entity may sign some or all email.

all All mail from the entity is signed; unsigned email MUST be considered Suspicious. The entity may send messages through agents that may modify and re-sign messages, so email signed with a Verifier Acceptable Third-Party Signature SHOULD be considered non-Suspicious.

strict All mail from the entity is signed; messages lacking a valid Originator Signature MUST be considered Suspicious. The entity does not expect to send messages through agents that may modify and re-sign messages.

NON-NORMATIVE RATIONALE: Strict practices may be used by entities which send only transactional email to individual addresses and which are willing to accept the consequence of having some mail which is re-signed appear suspicious in return for additional control over their addresses. Strict practices may also be used by entities which do not send (and therefore do not sign) any email.

ABNF:

ssp-p-tag = %x70 [FWS] "=" [FWS] "unknown" / "all" / "strict"

u= User-level signing practices for the entity (plain-text; OPTIONAL, default is "no"). This tag MUST NOT be present in user-level SSP records. Possible values are as follows:

yes Repeat query at user level. The Verifier MUST look up the user-level Signing Practices by querying for a DKIMP record at "<user>._user.<domain>" where <user> is the local-part of the Originator Address (i.e., the portion of the address before the "@" character) with any characters not permitted in DNS labels removed and with the resulting label truncated, if necessary, at 63 characters per [section 2.3.1 of \[RFC1035\]](#) and <domain> is the domain-part of the Originator Address (i.e., the portion of the address after the "@" character). If no user-level SSP record is found (either a NODATA or NXDOMAIN response is received), the practices described in this record should be used.

no Do not repeat the query at user level; use the practices described in this record.

ABNF:

ssp-u-tag = %x75 [FWS] "=" [FWS] "yes" / "no"

t= Flags, represented as a colon-separated list of names (plain-text; OPTIONAL, default is that no flags are set). Flag values are:

- y The entity is testing signing practices, and the Verifier SHOULD NOT consider a message suspicious based on the record.
- s The signing practices apply only to the named domain, and not to subdomains.

ABNF:

```
ssp-t-tag      = %x75 [FWS] "=" [FWS] ssp-t-tag-flag
                  0*( [FWS] ":" [FWS] ssp-t-tag-flag )
ssp-t-tag-flag = "y" / "s" / hyphenated-word ; for future extension
hyphenated-word = ALPHA [ *(ALPHA / DIGIT / "-") (ALPHA / DIGIT) ]
```

Unrecognized flags MUST be ignored.

4.3. Sender Signing Practices Check Procedure

The Sender Signing Practices check SHOULD be performed after DKIM signature(s), including any where the Alleged Signer is the Alleged Originator, have been verified. Verifiers MUST produce a result that is semantically equivalent to applying the following steps in the order listed. In practice, several of these steps can be performed in parallel in order to improve performance.

1. If a valid Originator Signature exists, the message is non-Suspicious, and the algorithm terminates.
2. The Verifier MUST query DNS for a DKIMP record corresponding to the domain part of the Originator Address. If the result of this query is a NODATA response, proceed to step 10. If the result of this query is a NXDOMAIN response, the message is Suspicious and the algorithm terminates. Otherwise, proceed to the following steps using the record retrieved by the query.
3. If the SSP "t" tag exists and any of the flags is "y" (indicating testing), the message is non-Suspicious and the algorithm terminates.
4. If the SSP "u" tag exists and the value is "yes", retain the value of the "p" tag; otherwise proceed to step 7.
5. The Verifier MUST query DNS for a user-level DKIMP record at the location defined in [Section 4.1](#). If the result of this query is a NODATA or NXDOMAIN response, then a user-level SSP record was not found; go to step 7 and proceed using the retained value of the "p" tag from the domain-level practices.
6. Proceed using the value of the "p" tag from the user-level query.
7. If the value of the SSP "p" tag is "unknown", the message is non-Suspicious and the algorithm terminates.

8. If the value of the SSP "p" tag is "all", and one or more Valid Signatures are present on the message, the message is Not Suspicious and the algorithm terminates.
9. The message is Suspicious and the algorithm terminates.
10. (check for parent domain policy) If the domain of the Originator Address is a top-level domain (e.g., a country code), then an SSP record was not found and the message is Not Suspicious.
11. The Verifier MUST query DNS for a DKIMP record corresponding to the immediate parent of the Originator Address. If the result of this query is a NODATA response, then an SSP record was not found and the message is non-Suspicious.
12. If the SSP "t" tag exists and any of the flags is "y" (indicating testing) or "s" (indicating that the record should not be used apply to a subdomain), the message is non-Suspicious and the algorithm terminates. Otherwise proceed to step 4.

5. Third-Party Signatures and Mailing Lists

There are several forms of mailing lists, which interact with signing in different ways.

- o "Verbatim" mailing lists send messages without modification whatsoever. They are often implemented as MTA-based aliases. Since they do not modify the message, signatures are unaffected and will continue to verify. There is no reason for the forwarder to re-sign the message.
- o "Digesting" mailing lists collect together one or more postings and then retransmit them, often on a nightly basis, to the subscription list. These are essentially entirely new messages which must be independently authored (that is, they will have a "From" header field referring to the list, not the submitters) and signed by the Mailing List Manager itself, if they are signed at all.
- o "Resending" mailing lists receive a message, modify it (often to add "unsubscribe" information or advertising), and immediately resend that message to the subscription list. They are problematic because they usually do not change the "From" header field of the message, but they do invalidate the signature in the process of modifying the message.

The first two cases act in obvious ways and do not require further

discussion. However, the third case is problematic. The remainder of this session applies only to that case.

5.1. Mailing List Manager Actions

Mailing List Managers should make every effort to ensure that messages that they relay and which have Valid Signatures upon receipt also have Valid Signatures upon retransmission. In particular, Mailing List Managers that modify the message in ways that break existing signatures SHOULD:

- o Verify any existing DKIM Signatures. A DKIM-aware Mailing List Manager MUST NOT re-sign an improperly signed message in such a way that would imply that the existing signature is acceptable.
- o Apply regular anti-spam policies. A Mailing List Manager SHOULD apply message content security policy just as they would messages destined for an individual user's mailbox. In fact, a Mailing List Manager might apply a higher standard to messages destined to a mailing list than would normally be applied to individual messages.

NON-NORMATIVE RATIONALE: Since reputation will accrue to signers, Mailing List Managers should verify the source and content of messages before they are willing to sign lest their reputation be sullied by nefarious parties.

- o Add a Sender header field using a valid address pointing back to the Mailing List Administrator or an appropriate agent (such as an "owner-" or a "-request" address).
- o Sign the resulting message with a signature that is valid for the Sender header field address. The Mailing List Manager SHOULD NOT sign messages for which they are unwilling to accept responsibility.

Mailing List Managers MAY:

- o Reject messages with signatures that do not verify or are otherwise Suspicious.

5.2. Signer Actions

All Signers SHOULD:

- o Include any existing Sender header field in the signed header field list, if the Sender header field exists.

Signers wishing to avoid the use of Third-Party Signatures SHOULD do everything listed above, and also:

- o Include the Sender header field name in the header field list ("h=" tag) under all circumstances, even if the Sender header field does not exist in the header block. This prevents another entity from adding a Sender header field.
- o Publish Sender Signing Practices that does not sanction the use of Third-Party Signatures

6. IANA Considerations

Use of the _user prefix in DKIMP DNS records will require registration by IANA.

The DKIMP RR type must be registered by IANA.

7. Security Considerations

Security considerations in the Sender Signing Practices are mostly related to attempts on the part of malicious senders to represent themselves as other senders, often in an attempt to defraud either the recipient or the Alleged Originator.

7.1. Fraudulent Sender Address

[[Assuming 3rd party signature is based on Sender header field]] If the Sender Signing Practices sanction third-party signing, an attacker can create a message with a From header field of an arbitrary sender and a legitimately signed Sender header field

7.2. DNS Attacks

An attacker might attack the DNS infrastructure in an attempt to impersonate SSP records. However, such an attacker is more likely to attack at a higher level, e.g., redirecting A or MX record lookups in order to capture traffic that was legitimately intended for the target domain. Domains concerned about this should use DNSSEC [[RFC4033](#)].

8. References

8.1. Normative References

- [I-D.ietf-dkim-base]
Allman, E., "DomainKeys Identified Mail (DKIM) Signatures", [draft-ietf-dkim-base-05](#) (work in progress), August 2006.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2822] Resnick, P., "Internet Message Format", [RFC 2822](#), April 2001.
- [RFC4234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 4234](#), October 2005.

8.2. Informational References

- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.

Appendix A. Change Log

A.1. Changes since -01

- o Changed term "Sender Signing Policy" to "Sender Signing Practices".
- o Changed query methodology to use a separate DNS resource record type, DKIMP.
- o Changed tag values from SPF-like symbols to words.
- o User level policies now default to that of the domain if not specified.
- o Removed the "Compliance" section since we're still not clear on what goes here.
- o Changed the "parent domain" policy to only search up one level (assumes that subdomains will publish SSP records if appropriate).

- o Added detailed description of SSP check procedure.

[A.2.](#) Changes since -00

From a "diff" perspective, the changes are extensive. Semantically, the changes are:

- o Added section on "Third-Party Signatures and Mailing Lists"
- o Added "Compliance" (transferred from -base document). I'm not clear on what needs to be done here.
- o Extensive restructuring.

Authors' Addresses

Eric Allman
Sendmail, Inc.
6425 Christie Ave, Suite 400
Emeryville, CA 94608
USA

Phone: +1 510 594 5501
Email: eric+dkim@sendmail.org
URI:

Mark Delany
Yahoo! Inc.
701 First Avenue
Sunnyvale, CA 94089
USA

Phone: +1 408 349 6831
Email: markd+dkim@yahoo-inc.com
URI:

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

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

Full Copyright Statement

Copyright (C) The Internet Society (2006).

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 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).

