DKIM Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 19, 2007

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

June 17, 2007

DKIM Sender Signing Practices
draft-ietf-dkim-ssp-00

Status of this Memo

Copyright Notice

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

[RFC4871].

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.

Table of Contents

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.

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. In contrast, this specification focuses on information which is relevant in the absence of a valid signature. Expressions of signing practice which require outside auditing are similarly out of scope for this specification because they fall under the purview of reputation and accreditation.

The detailed requirements for Sender Signing Practices are given in [I-D.ietf-dkim-ssp-requirements], which the protocol described in this document attempts to satisfy. This document refers extensively to [RFC4871], which should be read as a prerequisite to this document.

2. Language and Terminology

2.1. Terms Imported from DKIM Signatures Specification

Some terminology used herein is derived directly from [RFC4871]. Briefly,

- 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.

- 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.

- 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 [RFC4871].

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 a 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 its default value, consisting of 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 evaluation of the message; 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 4.4.

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

1. Some messages from this domain 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 domain are signed; all messages from this domain should have a Valid Signature. Signatures on behalf of a third party (e.g., a mailing list) handling the message MAY be accepted at the discretion of the verifier.

   NON-NORMATIVE RATIONALE: Third-party signatures, since they can potentially represent any domain, are considered more likely to be abused by attackers seeking to spoof a specific address. It may therefore be desirable for verifiers to apply other criteria outside the scope of this specification in deciding to accept a given third-party signature. For example, a list of known mailing list domains used by addresses served by the verifier might be specifically considered acceptable third-party signers.

3. All valid messages from this domain are signed, and SHOULD have a Valid Signature from this domain. Third-Party Signatures SHOULD NOT be accepted. This practice would typically be used by domains which send only transactional email (i.e., do not use mailing lists and such that are likely to break signatures) and

which wish to emphasize security over deliverability of their

messages.

4. The domain does not exist; the message SHOULD be presumed not to be legitimate.

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 (4), the message MUST be considered Suspicious.

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 DNS TXT resource record type.

NON-NORMATIVE DISCUSSION: There has been considerable discussion on the DKIM WG mailing list regarding the relative advantages of TXT and a new resource record (RR) type. The existence of DNS server and resolver implementations which are unable to support resource record types other than a specific well-known set is cited as a requirement for support of TXT records regardless of whether a new RR is defined. However, without a "flag day" on which SSP TXT record support is to be withdrawn, such support is likely to continue indefinitely. As a result, this specification defines no new RR type for SSP.

Another alternative proposed by P. Hallam-Baker is the publication of both a TXT record and, when implementations permit, a new RR, referred to as XPTR, which gives the location from which SSP and other policy information relating to a give domain can be

retrieved. This has the advantage of supporting a variety of policies in a scalable manner, with better handling of wildcards and centralized publication of policy records, with caching advantages. However, the above implementation issues also apply to XPTR, and an additional lookup is required to retrieve SSP via the XPTR method. At the time of publication of this draft, consensus on this proposal was unclear.

The RDATA for SSP resource records is textual in format, 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 [RFC4871] is used. Records not in compliance with that syntax or the syntax of individual tags described in Section 4.3 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 a location in the domain's DNS hierarchy prefixed by _ssp._domainkey; e.g., the SSP record for example.com would be a TXT record whcih is published at _ssp._domainkey.example.com.

4.2. Publication of SSP Records

Sender Signing Policy is intended to apply to all mail allegedly sent from a given Originating Domain, and to the greatest extent possible, to all subdomains of that domain. There are several cases that need to be considered in that regard:

- The domain itself
- Subdomains which may or may not be used for email
- Hostnames which may or may not be used for email
- Other named resource records in the domain
- Multi-level examples of the above, e.g., a.b.example.com
- Non-existent cases, i.e., a subdomain or hostname that does not actually exist within the domain

In all of these cases, the records may be published either in separate DNS zones or as records within a parent zone.

Normally, a domain expressing Sender Signing Practices will want to

do so for both itself and its all of its "descendents" (child domains, and hosts, at all lower levels). Domains wishing to do so

MUST publish SSP records as follows:

Publish an SSP record for the domain itself

Publish an SSP record for any existing subdomain

Publish an SSP record for any multilevel name within the subdomain. For example, it is necessary to publish a record for a.b.example.com even if the b.example.com subdomain does not exist in the sense of being explicitly delegated.

Note that since the lookup algorithm described below references the immediate parent of the alleged originating domain, it is not necessary to publish SSP records for every single-level label within the domain. This has been done to relieve domain administrators of the burden of publishing an SSP record for every other record in the zone, which would be otherwise required.

Wildcards within a zone, including but not limited to wildcard MX records, pose a particular problem. While referencing the immediate parent domain allows the discovery of an SSP record corresponding to an unintended immediate-child subdomain, wildcard records apply at multiple levels. For example, if there is a wildcard MX record for example.com, the domain foo.bar.example.com can receive mail through the named mail exchanger. Conversely, the existence of the record makes it impossible to tell whether foo.bar.example.com is a legitimate name since a query for that name will not return an NXDOMAIN error. For that reason, SSP coverage for subdomains of domains containing a wildcard record is incomplete.

4.3. Record Syntax

Signing practices records follow the tag-value syntax described in section 3.2 of [RFC4871]. 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].

dkim= 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-dkim-tag     = "dkim" [FWS] "=" [FWS] "unknown" / "all" / "strict"
```

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.

4.4. 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 TXT record corresponding to the domain part of the Originator Address prefixed by "_ssp._domainkey.". If the result of this query is a NOERROR response with one or more answer which is a syntactically-valid SSP response, proceed to step 6.

3. The Verifier MUST query DNS for a TXT record corresponding to the domain part of the Originator Address (with no prefix). This query is made only to check the existence of the domain name and MAY be done in parallel with the query made in step 2. If the result of this query is an NXDOMAIN error, the message is Supsicious and the algorithm terminates.

4. If the immediate parent of the domain part of the domain part of the Originator Address is a top-level domain, then the message is non-Suspicious (because no SSP record was found) and the algorithm terminates. The verifier MAY also compare the parent domain against a locally-maintained list of known address suffixes (e.g., .co.uk) and terminate the algorithm with a non-Suspicious result if the parent domain matches an entry on the list.

5. The Verifier MUST query DNS for a TXT record forthe immediate parent domain, prefixed with "_ssp._domainkey." If the result of this query is a NOERROR response which does not contain one or

more answers which is a syntactically-valid SSP response, or the "t" tag exists and any of the flags is "s" (indicating it should not apply to a subdomain), the message is non-Suspicious and the algorithm terminates.

6. If the SSP "t" tag exists and any of the flags is "y" (indicating testing), the message is non-Suspicious and the algorithm terminates.

7. If the value of the SSP "dkim" tag is "unknown", the message is non-Suspicious and the algorithm terminates.

8. If the value of the SSP "dkim" tag is "all", and one or more Valid Signatures are present on the message, the message is non-Suspicious and the algorithm terminates.

9. The message is Suspicious and the algorithm terminates.

5. Third-Party Signatures and Mailing Lists

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

- "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. It is not necessary for the forwarder to re-sign the message; however, some may choose to do so in order to certify that the message was sent through the list.

- "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.

- "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. The remainder of this session applies only to the third 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:

- 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.

- 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.

- 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).

- 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:

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

5.2. Signer Actions

All Signers SHOULD:

- 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:

- 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.

- Publish Sender Signing Practices that does not sanction the use of Third-Party Signatures

6. IANA Considerations

IANA is requested to create a "DKIM selector name" registry and to reserve the selector name "_ssp" to avoid confusion between DKIM key records and SSP records.

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.

Additional security considerations regarding Sender Signing Practices may be found in the DKIM threat analysis [RFC4686].

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].

Because SSP operates within the framework of the legacy e-mail system, the default result in the absence of an SSP record is that the domain does notsign all of its messages. Therefore, a DNS attack which is successful in suppressing the SSP response to the verifier is sufficient to cause the verifier to see unsigned messages as non-suspicious, even when that is not intended by the alleged originating domain.

8. References

8.1. Normative References

[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.

[RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

8.2. Informative References

[I-D.ietf-dkim-ssp-requirements]
Thomas, M., "Requirements for a DKIM Signing Practices Protocol", draft-ietf-dkim-ssp-requirements-04 (work in progress), April 2007.

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

[RFC4686] Fenton, J., "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)", RFC 4686, September 2006.

Appendix A. Change Log

A.1. Changes since -allman-ssp-02

- Removed user-granularity SSP and u= tag.
- Replaced DKIMP resource record with a TXT record.
- Changed name of the primary tag from "p" to "dkim".
- Replaced lookup algorithm with one which traverses upward at most one level.
- Added description of records which must be published, and effect of wildcard records within the domain, on SSP.

A.2. Changes since -allman-ssp-01

- Changed term "Sender Signing Policy" to "Sender Signing Practices".
- Changed query methodology to use a separate DNS resource record type, DKIMP.
- Changed tag values from SPF-like symbols to words.
- User level policies now default to that of the domain if not specified.
- Removed the "Compliance" section since we're still not clear on what goes here.

- Changed the "parent domain" policy to only search up one level (assumes that subdomains will publish SSP records if appropriate).

- Added detailed description of SSP check procedure.

A.3. Changes since -allman-ssp-00

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

- Added section on "Third-Party Signatures and Mailing Lists"

- Added "Compliance" (transferred from -base document). I'm not clear on what needs to be done here.

- 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

Intellectual Property

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).