DKIM Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 4, 2008

E. Allman
Sendmail, Inc.
M. Delany
Yahoo! Inc.
J. Fenton
Cisco Systems, Inc.
February 1, 2008

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

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 authors' domains can use to advertise their practices regarding signing their outgoing mail, and how other hosts can access, parse and interpret those records.

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)

- Need to consider handling of multiple responses to a DNS query for the SSP record.
- Security Considerations needs a detailed examination.
- IANA Considerations should be formalized (e.g., as in 4871).
- Check over the references.

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. Therefore, the absence of a signature is not an a priori indication of forgery. In fact, during early phases of DKIM deployment it must be expected that most messages will remain unsigned. Nevertheless, some domains may find it highly desirable to advertise that they sign all of their outgoing mail making the absence of a valid signature a potential indication of forgery. Without a mechanism to do so, the benefits of DKIM are limited to cases in which a valid signature exists and cannot be extended to cases in which signatures are missing or are invalid. Defining such a mechanism is the purpose of Sender Signing Practices (SSP).

This specification focuses on information which is relevant in the absence of an acceptable signature. 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. Sender Signing Practices can be extended in the future to include additional information that a receiver might use as input to a processing decision.

More specifically, this specification defines the SSP Checker, a module that retrieves the SSP information for a given domain, and the format of the data returned. An module called the Evaluator combines information from DKIM signatures, SSP Checker results, and any other data sources it cares to use in order to make a decision regarding how the message should be processed. The Evaluator is explicitly out of scope of this document, and is described herein in order to make the limits of this specification clear.

The detailed requirements for Sender Signing Practices are given in [RFC5016], 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.

- "Selectors" describe the keys published by a signing domain. Signing domains may have multiple Selectors. Selectors subdivide the address space to allow a single sending domain to publish multiple keys.

- A "Verifier" is the agent that verifies a message by checking actual signature(s) in the message header against the message itself using the public key published in the Selector referenced by a given signature.

2.2. Evaluator

The "Evaluator" is the module that makes the ultimate decision on how

an incoming message should be processed at a given site. In some cases it may be colocated with the Verifier. The Evaluator combines information from the DKIM signature(s) (if any), the output of the SSP Checker, and any other information it cares to consult in order to make a processing decision about the message. The specification of the Evaluator is out of scope of this document.

2.3. SSP Checker

The "SSP Checker" module performs the SSP queries on behalf of the Evaluator. It is the primary module defined by this document. The input to the SSP Checker is an address extracted from the From header field of the message being evaluated; the output is either the Sender Signing Practices associated with that domain, or an error code.

2.4. Valid Signature

A "Valid Signature" is any signature on a message which correctly verifies using the procedure described in section 6.1 of [RFC4871].

2.5. Alleged Author

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

2.6. Author Address

The "Author Address" is an email address in the From header field of a message [RFC2822]. If the From header field contains multiple addresses, the message has multiple Author Addresses, which may potentially cause the Evaluator to perform multiple SSP Checks for a given message.

2.7. Author Domain

The "Author Domain" is everything to the right of the "@" in the Author Address (excluding the "@" itself).

2.8. Author Signature

An "Author Signature" is any Valid Signature where the identity of the user or agent on behalf of which the message is signed (listed in the "i=" tag or its default value from the "d=" tag) matches an Author Address in the message.

2.9. Sender Signing Practices Record

A "Sender Signing Practices Record" consists of a machine-readable record published by the domain of an Alleged Author which includes information on whether that domain signs all of their email, and related information. That record is defined in detail in section Section 3.3.

3. Operational Description

The use of Sender Signing Practices consists of two parts:

Publication of SSP records by author domains wishing to do so

Lookup of SSP records by an SSP Checker under the direction of an Evaluator.

3.1. Publication of SSP Records

3.1.1. DNS Representation

Sender Signing Practices Records are published using the DNS "TXT" resource record type.

[[DRAFT DISCUSSION, TO BE DELETED BEFORE PUBLICATION: There has been considerable discussion on the DKIM WG mailing list regarding the relative advantages of TXT and a new resource record (RR)

type. Many DNS server and resolver implementations are incapable of quickly and easily supporting new resource record types. For this reason, support of TXT records is required whether a new RR type is defined or not. 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. SSP records follow the tag-list syntax described in section 3.2 of [RFC4871], including the restriction on duplicate tags, the use of white space, and case sensitivity. Records not in overall compliance with that syntax MUST be ignored (considered equivalent to a "NODATA" result), although they MAY cause the logging of warning messages via an appropriate system logging mechanism. All syntactically valid tags MUST be made available to the Evaluator.

3.1.2. Location of SSP Records

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 that is published at "_ssp._domainkey.example.com".

Sender Signing Practices are intended to apply to all mail sent from the domain of an Alleged Author. In order to ensure that SSP applies to any hosts within that domain (e.g., www.example.com, ftp.example.com, etc.) the SSP lookup algorithm looks up one level in the domain tree. For example, mail signed by www.example.com may optionally be covered by the SSP record for example.com. This prevents administrators from having to include an SSP record for every name within a given domain.

Normally, a domain expressing Sender Signing Practices will want to

do so for both itself and all of its "descendents" (child domains at

all lower levels). Domains wishing to do so MUST publish SSP records for the domain itself and any subdomains.

Wildcards within a domain publishing SSP records pose a particular problem. This is discussed in more detail in Section 5.2.

3.2. Lookup of SSP Records

NON-NORMATIVE NOTE: While the operation of the Evaluator is outside the scope of this specification, it is generally not worthwhile for an Evaluator to request an SSP check when the results of that check will not affect the disposition of the message. Since the information provided by SSP is only relevant in the absence of valid Author Signature(s), there is little to be gained by performing an SSP check on domains corresponding to valid Author Signatures. SSP checks may also be unnecessary when the Evaluator has some other basis for deciding to process the message "normally", including, but not limited to, the presence of a DKIM signature that the Evaluator has some basis to trust sufficiently for this purpose.

3.2.1. SSP Checker Results

A Sender Signing Practices check produces one of four possible results for use by the Evaluator:

1. The domain does not exist in DNS.

2. The domain does exist, but no SSP Record is present.

3. The SSP Record exists, and that value is also returned.

4. The DNS information could not be determined due to a transient error such as "SERVFAIL".

3.2.2. SSP Lookup Algorithm

SSP Checkers doing an SSP lookup MUST produce a result that is semantically equivalent to applying the following steps in the order listed below. In practice, several of these steps can be performed in parallel in order to improve performance. However, implementations SHOULD avoid doing unnecessary DNS lookups. For the purposes of this section a "valid SSP record" is one that is both syntactically and semantically correct; in particular, it must match the ABNF for a "tag-list" and must include a defined "dkim=" tag.

1. _Fetch Named SSP Record._ The SSP Checker MUST query DNS for a TXT record corresponding to the Author Domain prefixed by

""_ssp._domainkey."" (note the trailing dot). If the result of this query is a "NOERROR" response with one or more answers which are valid SSP records, return that record for interpretation by the Evaluator; otherwise, continue to the next step.

2. _Verify Domain Exists._ The SSP Checker MUST perform a DNS query for a record corresponding to the Author Domain (with no prefix). The type of the query can be of any type, since this step is only to determine if the domain itself exists in DNS. This query MAY be done in parallel with the query made in step 2. If the result of this query is an "NXDOMAIN" error, the SSP Checker MUST return an appropriate error to the Evaluator and terminate the algorithm.

   NON-NORMATIVE DISCUSSION: Any resource record type could be used for this query since the existence of a resource record of any type will prevent an "NXDOMAIN" error. "MX" is a reasonable choice for this purpose is because this record type is thought to be the most common for likely domains, and will therefore result in a result which can be more readily cached than a negative result.

3. _Try Parent Domain._ The SSP Checker MUST query DNS for a TXT record for the immediate parent domain, prefixed with ""_ssp._domainkey."" If the result of this query is anything other than a "NOERROR" response with a valid SSP record, the algorithm terminates returning a result indicating that no SSP record was present. If the SSP "t" tag exists in the response and any of the flags is "s" (indicating it should not apply to a subdomain), the SSP Checker MUST also return a "No SSP Record" result. Otherwise, return that record for interpretation by the Evaluator.

If any of the queries involved in the Sender Signing Practices Check result in a "SERVFAIL" error response, the SSP Checker MUST return that information to the Evaluator; possible actions include queuing the message or returning an SMTP error indicating a temporary failure.

3.3. SSP Record Syntax

SSP Records MUST match the "tag-list" syntax defined in [RFC4871]. The specific tags used in SSP records are described below. Unrecognized tags MUST be ignored.

dkim= Outbound signing practices for the domain (plain-text; REQUIRED). Possible values are as follows:

unknown The domain may sign none, some, or all email.

all All mail from the domain is signed with an Author Signature.

discardable All mail from the domain is signed with an Author Signature. Furthermore, if a message arrives without a valid Author Signature due to modification in transit, submission via a path without access to a signing key, or other reason, the domain encourages the recipient(s) to discard it.

NON-NORMATIVE DISCUSSION: Sender signing practices of "discardable" would be usually inappropriate for domains of end users, because of the potential for mailing lists and similar agents to modify messages in such a way as to render the signature invalid. Domains sending mail that is expected to pass with no significant modification to the recipient, such as domains sending only transactional messages, are appropriate places to consider the publication of a "discardable" practice. See [RFC5016] section 5.3 and Appendix A for further discussion.

ABNF:

```
ssp-dkim-tag   = "dkim" *WSP "=" *WSP ("unknown" /
                    "all" / "discardable")
```

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

s The signing practices apply only to the named domain, and not to subdomains.

ABNF:

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


Unrecognized flags MUST be included in the result that is provided to the Evaluator.

4. 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.

<<< Needs to be updated to be more complete; see 4871 for examples >>>

5. 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 authors, often in an attempt to defraud either the recipient or an Alleged Author.

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

<<<THIS SECTION IS NOT COMPLETE.>>>

5.1. 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 not sign all of its messages. It is therefore important that the SSP Checker distinguish a DNS failure such as SERVFAIL from other DNS errors so that appropriate actions can be taken.

5.2. DNS Wildcards

Wildcards within a domain publishing SSP records, 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.

> NON-NORMATIVE NOTE: Complete SSP coverage of domains containing (or where any parent contains) wildcards generally cannot be guaranteed.

6. References

6.1. 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.

6.2. Informative References

[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.

[RFC5016] Thomas, M., "Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices Protocol", RFC 5016, October 2007.

Appendix A. Usage Examples (INFORMATIVE)

These examples are intended to illustrate typical uses of SSP. They are not intended to be exhaustive, nor to apply to every domain or mail system's individual situation.

A.1. Single Location Domains

A common mail system configuration handles all of a domain's users' incoming and outgoing mail through a single MTA or cluster of MTAs. In that case, the MTA(s) can be configured to sign outgoing mail with an Author Signature.

In this situation it might be appropriate to publish an SSP record for the domain containing "all", depending on whether the users also send mail through other MTAs that do not apply an Author Signature. Such MTAs could include MTAs at hotels or hotspot networks used by travelling users, or web sites that provide "mail an article"

features.

Domain managers are advised to consider the ways that mail processing can modify messages in ways that will invalidate an existing DKIM signature, such as mailing lists, courtesy forwarders, and other paths that could add or modify headers, or modify the message body. In that case, if the modifications invalidate the DKIM signature, recipient MTAs will consider the mail not to have an Author Signature, even though the signature was present when the mail was originally sent.

A.2. Bulk Mailing Domains

Another common configuration uses a domain solely for bulk or broadcast mail, with no individual human users, again typically sending all the mail through a single MTA or cluster of MTAs that can apply an Author Signature. In this case, the domain's management can be confident that all of its outgoing mail will be sent through the signing MTA. Lacking individual users, the domain is unlikely to participate in mailing lists, but could still send mail through other paths that might invalidate signatures.

Domain owners often use specialist mailing providers to send their bulk mail. In that case, the mailing provider needs access to a suitable signing key in order to apply an Author Signature. One possible route would be for the domain owner to generate the key and give it to the mailing provider. Another would be for the domain to delegate a subdomain to the mailing provider, for example, bigbank.example might delegate email.bigbank.example to such a provider. In that case, the provider can generate the keys and DKIM

DNS records itself and use the subdomain in the Author Address in the mail.

A.3. Bulk Mailing Domains with Discardable Mail

In some cases, a domain might sign all its outgoing mail with an Author Signature, but prefers that recipient systems discard mail without a valid Author Signature to avoid confusion from mail sent from sources that do not apply an Author Signature. (This latter kind of mail is sometimes loosely called "forgeries".) In that case, it may be appropriate to publish an SSP record containing

"discardable". Note that a domain SHOULD NOT publish a "discardable" record if it wishes to maximize the likelihood that mail from the domain is delivered, since it could cause some fraction of the mail the domain sends to be discarded.

As a special case, if a domain sends no mail at all, it can safely publish a "discardable" SSP record, since any mail with an author address in the domain is a forgery.

A.4. Third Party Senders

Another common use case is for a third party to enter into an agreement whereby that third party will send bulk or other mail on behalf of a designated author domain, using that domain in the RFC2822 From: or other headers. Due to the many and varied complexities of such agreements, third party signing is not addressed in this specification. The authors anticipate that as mail systems gain experience with DKIM, it will become possible to codify best practices of this and other usages of DKIM.

Appendix B. Acknowledgements

The authors wish to thank many members of the ietf-dkim mailing list for valuable suggestions and constructive criticism of earlier versions of this draft.

This draft incorporates content from a parallel "DKIM Author Signing Policies" document edited by John Levine. The authors appreciate this contribution.

Appendix C. Change Log

NOTE TO RFC EDITOR: This section may be removed upon publication of this document as an RFC.

C.1. Changes since -ietf-dkim-ssp-01

- Reworded introduction for clarity.

- Various definition clarifications.
- Changed names of practices to unknown, all, and discardable.
- Removed normative language mandating use of SSP in particular situations (issue 1538).
- Clarified possible confusion over handling of syntax errors.
- Removed normative language from Introduction (issue 1538).
- Changed "Originator" to "Author" throughout (issue 1529).
- Removed all references to Third-Party Signatures (issues 1512, 1521).
- Removed all mention of "Suspicious" (issues 1528, 1530).
- Removed "t=y" (testing) flag (issue 1540).
- Removed "handling" tag (issue 1513).
- Broke up the "Sender Signing Practices Check Procedure" into two algorithms: fetching the SSP record and interpretation thereof (issues 1531, 1535; partially addresses issue 1520). Interpretation is now the responsibility of the Evaluator.
- Document restructuring for better flow and remove redundancies (some may address issue 1523, but I'm not sure I understand that issue completely; also issues 1532, 1537).
- Removed all mention of how this interacts with users, even though it makes parts of the document harder to understand (issue 1526).
- Introduced the concepts of "SSP Checker" and "Evaluator".
- Multiple author case now handled my separate invocations of SSP checker by Evaluator (issue 1525).
- Removed check to avoid querying top-level domains.
- Changed ABNF use of whitespace from [FWS] to *WSP (partially addresses issue 1543).

C.2. Changes since -ietf-dkim-ssp-00

- Clarified Operation Overview and eliminated use of Legitimate as the counterpart of Suspicious since the words have different meanings.
- Improved discussion (courtesy of Arvel Hathcock) of the use of TXT records in DNS vs. a new RR type.
- Clarified publication rules for multilevel names.
- Better description of overall record syntax, in particular that records with unknown tags are considered syntactically correct.
- Clarified Sender Signing Practices Check Procedure, primarily by use of new term Author Domain.
- Eliminated section "Third-Party Signatures and Mailing Lists" that is better included in the DKIM overview document.
- Added "handling" tag to express alleged sending domain's preference about handling of Suspicious messages.
- Clarified handling of SERVFAIL error in SSP check.
- Replaced "entity" with "domain", since with the removal of user-granularity SSP, the only entities having sender signing policies are domains.

C.3. 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.

C.4. 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.

C.5. 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.
6475 Christie Ave, Suite 350
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).