DKIM Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 20, 2008

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

September 17, 2007

DKIM Sender Signing Practices
draft-ietf-dkim-ssp-01

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)

Need to consider handling of multiple responses to a DNS query for the SSP record.

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], message verifiers implementing this specification 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 made available 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.
>
> Even when there is only one address in the From header field, this address is chosen as the reference address for SSP lookups because it represents the author of the message and is more widely displayed by Mail User Agents as a result. The Sender header

> field frequently has other meanings.

2.4. Originator Domain

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

2.5. 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.

2.6. 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.

2.7. 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 domain signs all of their email, and whether signatures from third parties are sanctioned by the Alleged Originator.

2.8. 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 Originator Address. If the signing address does not include a local-part, then only the domains must match; otherwise, the two addresses must be identical.

2.9. 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 domain 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 not deemed Suspicious may be

rejected for other reasons.

2.10. Third-Party Signature

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

2.11. 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 MUST NOT be considered 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.

A Sender Signing Practices check produces one of four possible results:

1. Some messages from this domain are not signed; the message MUST NOT be considered Suspicious, even in the absence of a valid signature. This is the default.

2. All messages from this domain are signed. Messages containing a Verifier Acceptable Third-Party Signature MUST NOT be considered Suspicious.

   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; the domain of the

Alleged Originator requests that only messages with valid Originator Signatures be considered not Suspicious; Third-Party Signatures are irrelevant. 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. In the absence of a valid Originator Signature, the message MUST be considered Suspicious.

4. The domain does not exist; 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 domain are not signed and the message MUST NOT be considered 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. 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. 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 that is published at _ssp._domainkey.example.com.

4.2. Publication of SSP Records

Sender Signing Practices are intended to apply to all mail sent from the domain of an Alleged Originator, 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

Normally, a domain expressing Sender Signing Practices will want to do so for both itself and 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

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

domain, which would be otherwise required.

Wildcards within a domain, 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.

4.3. Record Syntax

SSP records follow the "tag=value" syntax described in section 3.2 of [RFC4871]. The SSP record syntax is a tag-list as defined in that section, including the restriction on duplicate tags, the use of white space, and case sensitivity.

Tags used in SSP records are as follows. Unrecognized tags 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 domain (plain-text; REQUIRED). Possible values are as follows:

unknown The domain may sign some or all email.

all All mail from the domain is signed; unsigned email MUST be considered Suspicious. The domain may send messages through agents that may modify and re-sign messages, so email signed with a Verifier Acceptable Third-Party Signature SHOULD NOT be

considered Suspicious.

strict All mail from the domain is signed; messages lacking a valid Originator Signature MUST be considered Suspicious. The domain 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")
```

handling= Non-compliant message handling request for the domain (plain-text; OPTIONAL). Possible values are as follows:

process Messages which are Suspicious from this domain SHOULD be processed by the verifier, although the SSP failure MAY be considered in subsequent evaluation of the message. This is the default value.

deny Messages which are Suspicious from this domain MAY be rejected, bounced, or otherwise not delivered at the option of the verifier.

NON-NORMATIVE EXPLANATION: The "deny" practice is intended for use by domains that value security over deliverability. For example, a domain used by a financial institution to send transactional email, which signs all of its messages, might consider their concern about phishing messages purporting to come from their domain to be higher than their concern about some some legitimate messages not being

delivered. The "handling=deny" practice allows them to express that concern in a way that can be acted upon by verifiers, if they so choose.

ABNF:

```
ssp-handling-tag = "handling" [FWS] "=" [FWS] ("process" /
                           "deny")
```

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 domain 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

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 not Suspicious, and the algorithm terminates.

2. The Verifier MUST query DNS for a TXT record corresponding to

the Originator Domain prefixed by "_ssp._domainkey.". If the result of this query is a NOERROR response with one or more answers which are syntactically-valid SSP responses, proceed to step 7.

3. The Verifier MUST query DNS for an MX record corresponding to the Originator Domain (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 Suspicious and the algorithm terminates.

   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. The choice of MX 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.

4. If the immediate parent of the Originator Domain is a top-level domain (a domain consisting of a single element such as "com", "us", or "jp"), then the message is not 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 not Suspicious result if the parent domain matches an entry on the list.

5. The Verifier MUST query DNS for a TXT record for the immediate parent domain, prefixed with "_ssp._domainkey." If the result of this query is a NOERROR response with one or more answers which are syntactically-valid SSP responses, proceed to step 6. Otherwise, the message is not Suspicious and the algorithm terminates.

6. 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 message is not Suspicious and the algorithm terminates.

7. If the SSP "t" tag exists in the response and any of the flags

is "y" (indicating testing), the message is not Suspicious and the algorithm terminates.

8. If the value of the SSP "dkim" tag is "unknown", the message is not Suspicious and the algorithm terminates.

9. If the value of the SSP "dkim" tag is "all", and one or more Verifier Acceptable Third-Party Signatures are present on the message, the message is not Suspicious and the algorithm terminates.

10. The message is Suspicious and the algorithm terminates.

If any of the queries involved in the Sender Signing Practices Check result in a SERVFAIL error response, the verifier MAY either queue the message or return an SMTP error indicating a temporary failure.

5. 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.

6. 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].

6.1. 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

6.2. 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 not sign 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.

7. References

7.1. 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.

7.2. Informative References

[I-D.ietf-dkim-ssp-requirements]
Thomas, M., "Requirements for a DKIM Signing Practices Protocol", draft-ietf-dkim-ssp-requirements-05 (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. Acknowledgements

The authors wish to thank many members of the ietf-dkim mailing list, in particular Arvel Hathcock and Eliot Lear, for valuable suggestions and constructive criticism of earlier versions of this draft.

Appendix B. Change Log

B.1. 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 Originator 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.

B.2. 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.

B.3. 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.

B.4. 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

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).