Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 3, 2008

S. Atkins
Word to the Wise
J. Falk
Return Path
J. Levine, Ed.
Taughannock Networks
W. Venema
IBM T. J. Watson Research
January 31, 2008

DKIM Author Signing Practices (ASP)
draft-levine-asp-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 authors can use to advertise their practices for signing their outgoing mail, and how other hosts can access those records.

Table of Contents

1. Introduction

Much of this document is adapted from [I-D.ietf-dkim-ssp-01] by Allman et al. The features described here are approximately a subset of the ones described in that document.

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 is very likely that most messages will remain unsigned. However, some domains might decide 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 other hosts. This is the topic of Author Signing Practices (ASP).

In the absence of a valid DKIM signature, hosts implementing this specification can inquire what Author Signing Practices that domain advertises. This inquiry is called an Author Signing Practices check.

The detailed requirements for Author Signing Practices are given in [I-D.ietf-dkim-ssp-requirements]. This document refers extensively to [RFC4871] and assumes the reader is familiar with it.

Requirements Notation: 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]

2. Language and Terminology

2.1. Terms Imported from DKIM Signatures Specification

Some terminology used herein is derived directly from [RFC4871]. In several cases, references in that document to Sender have been changed to Author here, to emphasize the relationship to the Author address(es) on the From: header line described in [RFC2822]. 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 "Selector" specifies which of the keys published by a signing domain is to 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. Author Address

An "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.

2.4. Author Domain

An "Author Domain" is everything to the right of the "@" in an Author 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; it is "alleged" because it has not yet been verified.

2.6. Alleged Authors

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

2.7. Author Signing Practices

"Author Signing Practices" (or just "practices") consist of a machine-readable record published by the domain of an Alleged Author which includes statements about the domain's practices with respect to mail it sends with its domain in the From: line.

2.8. Author Signature

An "Author Signature" is any Valid Signature where the signing domain (listed in the "i=" tag if present, otherwise its default value, consisting of the value of the "d=" tag) matches the domain of an

Author Address.

3. Operation Overview

A host typically looks up Author Signing Practices based on the Author Address(es).

Hosts can look up the Author Signing Practices of the domain(s) specified by the Author Address(es) as described in Section 4.4.

3.1. ASP Usage

Depending on the Author Domain(s) and the signatures in a message, a recipient gets varying amounts of useful information from an ASP lookup.

- If a message has no Valid Signature, the ASP result is directly relevant to the message.
- If a message has a Valid Signature from an Author Domain, ASP provides no benefit relative to that domain since the message is already known to be compliant with any possible ASP for that domain.
- If a message has a Valid Signature from a domain other than an Author Domain, the receiver can use both the Signature and the ASP result in its evaluation of the message.

3.2. ASP Results

An Author Signing Practices lookup produces one of four possible results:

- Messages from this domain might or might not have an author signature. This is the default if the domain exists but no record is found.
- All messages from this domain are signed.
- All messages from this domain are signed and discardable.
- The domain does not exist.

4. Detailed Description

4.1. DNS Representation

Author Signing Practices records are published using the DNS TXT resource record type.

NON-NORMATIVE DISCUSSION [to be removed 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. Read the archive for details.

The RDATA for ASP resource records is textual in format, with specific syntax and semantics relating to their role in describing Author 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 ASP, although they MAY cause the logging of warning messages via an appropriate system logging mechanism. If the RDATA contains multiple character strings, the strings are logically concatenated with no delimeters between the strings.

ASP records for a domain are published at a location in the domain's DNS hierarchy prefixed by _asp._domainkey.; e.g., the ASP record for example.com would be a TXT record that is published at _asp._domainkey.example.com. A domain MUST NOT publish more than one ASP record; the semantics of an ASP lookup that returns multiple ASP records for a single domain are undefined. (Note that example.com and mail.example.com are different domains.)

4.2. Publication of ASP Records

Author Signing Practices are intended to apply to all mail sent from a 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 might or might not be used for email
- Host names which might or might 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

A domain publishing Author Signing Practices may want to do so for both itself and all of its "descendants" (child domains and hosts, at all lower levels). Domains wishing to do so publish ASP records as follows:

- Publish an ASP record for the domain itself.

- Publish an ASP 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 ASP records for every single-level label within the domain. This has been done to relieve domain administrators of the burden of publishing an ASP record for every other record in the domain, which would be otherwise needed.

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 ASP 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, ASP coverage for subdomains of domains containing a wildcard record is incomplete.

NON-NORMATIVE NOTE [to be removed before publication]: Complete ASP coverage of domains containing (or where any parent contains) wildcards generally cannot be guaranteed.

4.3. Record Syntax

ASP records follow the "tag=value" syntax described in section 3.2 of [RFC4871]. The ASP 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 ASP records are as follows. Unrecognized tags MUST be ignored. In the ABNF below, 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 might sign 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.

ABNF:

```
asp-dkim-tag = "dkim=" ("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:

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

Unrecognized flags MUST be ignored.

4.4. Author Signing Practices Lookup Procedure

To look up the Author Signing Practices of a domain, ASP Checkers doing an ASP 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 ASP 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. The host makes a DNS query for a TXT record corresponding to the domain prefixed by "_asp._domainkey.". If the result of this

query is a NOERROR response with an answer which contains a syntactically-valid ASP record, the Author Signing Practices are described by the contents of the record and the algorithm terminates.

2. The host MUST query DNS for an MX record corresponding to the 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 1. If the result of this query is an NXDOMAIN error, the domain does not exist and the algorithm terminates.

   NON-NORMATIVE DISCUSSION [to be removed before publication]: 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.

3. The host MUST query DNS for a TXT record for the immediate parent domain, prefixed with "_asp._domainkey." If the result of this query is a NOERROR response with one or more answers that are syntactically-valid ASP responses, and the responses do not contain a "s" flag, the Author Signing Practices are described by the contents of the record(s).

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

5. Usage Examples

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

5.1. 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 ASP 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.

5.2. 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.

5.3. 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 ASP 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" ASP record, since any mail with an author address in the domain is a forgery.

5.4. 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.

6. References

6.1. References - Normative

[I-D.ietf-dkim-ssp-requirements]
Thomas, M., "Requirements for a DKIM Signing Practices Protocol", April 2007.

[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. References - Informative

[I-D.ietf-dkim-ssp-01]
Allman, E., Delany, M., and J. Fenton, "DKIM Sender Signing Practices", September 2007.

Appendix A. Acknowledgements

This document adapted large sections from a previous draft by Eric Allman, Jim Fenton, et al. It greatly benefited from comments by Jon Callas, Dave Crocker, Arvel Hathcock, Ellen Siegel, and Michael

Thomas.

Authors' Addresses

Steve Atkins
Word to the Wise
PO Box 7086
San Carlos, CA 94070-7086
US

Phone: +1 650 678 3453
Email: steve-asp@wordtothewise.com
URI: http://wordtothewise.com/

J. D. Falk
Return Path
100 Superior Plaza Way
Superior, CO 80027

Phone: +1 303 642 4100
Email: ietf@cybernothing.org

John Levine (editor)
Taughannock Networks
PO Box 727
Trumansburg, NY 14886

Phone: +1 831 480 2300
Email: standards@taugh.com
URI: http://www.taugh.com

Wietse Venema
IBM T. J. Watson Research
19 Skyline Drive
Hawthorne, NY 10532

Email: wietse@watson.ibm.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).