Network Working Group
Internet Draft
<draft-ietf-dkim-ssp-03>
Intended status: Standards Track
Expires: August 2008

E. Allman
Sendmail, Inc.
J. Fenton
Cisco Systems, Inc.
M. Delany
Yahoo! Inc.
J. Levine
Taughannock Networks
February 23, 2008

DKIM Author Signing Practices (ASP)

draft-ietf-dkim-ssp-03

Status of this Memo

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 for signing their outgoing mail, and how other hosts can access those records.

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 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 desirable for such domains to be able to advertise that fact to other hosts. This is the topic of Author Signing Practices (ASP).

Hosts implementing this specification can inquire what Author Signing Practices a domain advertises. This inquiry is called an Author Signing Practices check.

The detailed requirements for Author Signing Practices are given in [RFC5016]. 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) in the From: header field described in [RFC2822]. Briefly,

- A "Signer" is the agent that signs a message, as defined in section 2.1 of [RFC4871].
- A "Selector" specifies which of the keys published by a signing domain is to be queried, as defined in section 3.1 of [RFC4871].
- A "Local-part" is the part of an address preceding the @ sign, as defined in [RFC2822] and used in [RFC4871].

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 Author

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

2.6 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.

2.7 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. When the identity of the user or agent includes a Local-part, the identities match if the Local-parts match and the domains match. Otherwise, the identities match if the domains match.

For example, if a message has a Valid Signature, with the DKIM-Signature field containing `i=a@domain.example`, then domain.example is asserting that it takes responsibility for the message. If the message's From: field contains the address `b@domain.example` and an ASP query produces a `dkim=all` or `dkim=discardable` result, that would mean that the message does not have a valid Author Signature. Even though the message is signed by the same domain, its failure to satisfy ASP could be problematic.

3. Operation Overview

Domain owners can publish Author Signing Practices via a query mechanism such as the Domain Name System; specific details are given in Section 4.1.

Hosts can look up the Author Signing Practices of the domain(s) specified by the Author Address(es) as described in Section 4.2.2. If a message has multiple Author Addresses the ASP lookups SHOULD be performed independently on each address. This standard does not address the process a host might use to combine the lookup results.

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 each 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 for an Author Address 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 in the DNS 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 delimiters between the strings.

The ASP record for a domain is 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 the domain of an Alleged Author. In order to ensure that ASP applies to any hosts within that domain (e.g., www.example.com, ftp.example.com.) the ASP lookup algorithm looks up one level in the domain tree. For example, mail signed by www.example.com could be covered by the ASP record for example.com. This avoids the need to include an ASP record for every name within a given domain.

Normally, a domain expressing Author Signing Practices will want to do so for both itself and all of its "descendants" (child domains at all lower levels). Domains wishing to do so MUST publish ASP records for the domain itself and any subdomains.

Wildcards within a domain publishing ASP records pose a particular problem. This is discussed in more detail in Section 6.3.

4.2.1 Record Syntax

ASP records use the "tag=value" syntax described in section 3.2 of [RFC4871].

Tags used in ASP records are described below. Unrecognized tags MUST be ignored. In the ABNF below, the WSP token is imported from [RFC2822]. The ALPHA and DIGIT tokens are imported from [RFC5234].

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 = %x64.6b.69.6d *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:

```
asp-t-tag    = %x74 *WSP "=" *WSP { asp-t-tag-flag
      0*( *WSP ":" *WSP 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.

4.2.2 Author Signing Practices Lookup Procedure

Hosts 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 matches the ABNF for a `tag-list` and includes a defined `dkim=` tag.

1. *Fetch Named ASP Record.* The host MUST query DNS for a TXT record corresponding to the Author Domain prefixed by `_asp._domainkey.` (note the trailing dot). If the result of this query is a `NOERROR` response with an answer which is a valid ASP record, use that record; otherwise, continue to the next step.
2. *Verify Domain Exists.* The host 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 algorithm MUST terminate with an appropriate error.

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 host MUST query DNS for a TXT record for the immediate parent domain, prefixed with `_asp._domainkey.` If the result of this query is anything other than a `NOERROR` response with a valid ASP record, the algorithm terminates with a result indicating that no ASP record was present. If the ASP "t" tag exists in the response and any of the flags is "s" (indicating it does not apply to a subdomain), the algorithm also terminates without finding an ASP record. Otherwise, use that record.

If any of the queries involved in the Author Signing Practices Check result in a `SERVFAIL` error response, the algorithm terminates without returning a result; possible actions include queuing the message or returning an SMTP error indicating a temporary failure.

5. IANA Considerations

ASP introduces some new namespaces that have been registered with IANA. In all cases, new values are assigned only for values that have been documented in a published RFC that has IETF Consensus [RFC2434].

INFORMATIVE NOTE [to be removed before publication]: RFC 4871 defines a selector as a sub-domain, importing the term from RFC 2822. A sub-domain starts with a letter or digit, hence names such as _asp that start with an underscore cannot collide with valid selectors.

5.1 ASP Specification Tag Registry

An ASP record provides for a list of specification tags. IANA has established the ASP Specification Tag Registry for specification tags that can be used in ASP fields.

The initial entries in the registry comprise:

```
+------+-----------------+
| TYPE | REFERENCE       |
+------+-----------------+
| dkim | (this document) |
| t    | (this document) |
+------+-----------------+
```

ASP Specification Tag Registry Initial Values

5.2 ASP Outbound Signing Practices Registry

The `dkim=` tag spec, defined in Section 4.2.1, provides for a value specifying Outbound Signing Practices. IANA has established the ASP Outbound Signing Practices Registry for Outbound Signing Practices.

The initial entries in the registry comprise:

```
+-------------+-----------------+
| TYPE        | REFERENCE       |
+-------------+-----------------+
| unknown     | (this document) |
| all         | (this document) |
| discardable | (this document) |
+-------------+-----------------+
```

ASP Outbound Signing Practices Registry Initial Values

5.3 ASP Flags Registry

The `t=` tag spec, defined in Section 4.2.1, provides for a value specifying Flags. IANA has established the ASP Flags Registry for ASP Flags.

The initial entries in the registry comprise:

TYPE	REFERENCE
s	(this document)

ASP Flags Registry Initial Values

6. Security Considerations

Security considerations in the Author Signing Practices are mostly related to attempts on the part of malicious senders to represent themselves as authors for whom they are not authorized to send mail, often in an attempt to defraud either the recipient or an Alleged Author.

Additional security considerations regarding Author Signing Practices are found in the DKIM threat analysis [RFC4686].

6.1 ASP Threat Model

Email recipients often have a core set of content authors that they already trust. Common examples include financial institutions with which they have an existing relationship and Internet web transaction sites with which they conduct business.

Email abuse often seeks to exploit the name-recognition that recipients will have, for a legitimate email author, by using its domain name in the From: header field. Especially since many popular MUAs do not display the author's email address, there is no empirical evidence of the extent that this particular unauthorized use of a domain name contributes to recipient deception or that eliminating it will have significant effect.

However, closing this exploit could facilitate some types of optimized processing by receive-side message filtering engines, since it could permit them to maintain higher-confidence assertions about From: header field uses of a domain, when the occurrence is authorized.

Unauthorized uses of domain names occur elsewhere in messages, as do unauthorized uses of organizations' names. These attacks are outside the scope of this specification.

ASP does not provide any benefit--nor, indeed, have any effect at all--unless an external system acts upon the verdict, either by treating the message differently during the delivery process or by showing some indicator to the end recipient. Such a system is out of scope for this specification.

ASP Checkers perform up to three DNS lookups per Alleged Author Domain. Since these lookups are driven by domain names in email message headers of possibly fraudulent email, legitimate ASP Checkers can become participants in traffic multiplication attacks.

6.2 DNS Attacks

An attacker might attack the DNS infrastructure in an attempt to impersonate ASP records, in an attempt to influence a receiver's decision on how it will handle mail. 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. These DNS security issues are addressed by DNSSEC [RFC4033].

Because ASP operates within the framework of the legacy e-mail system, the default result in the absence of an ASP record is that the domain does not sign all of its messages. It is therefore important that the ASP clients distinguish a DNS failure such as `SERVFAIL` from other DNS errors so that appropriate actions can be taken.

6.3 DNS Wildcards

Wildcards within a domain publishing ASP records, 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: Complete ASP coverage of domains containing (or where any parent contains) wildcards generally cannot be provided by standard DNS servers.

7. References

7.1 References - Normative

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H.T. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[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.

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

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

7.2 References - Informative

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

Authors' Addresses

Eric Allman
Sendmail, Inc.
6475 Christie Ave, Suite 350
Emeryville, CA 94608
Phone: +1 510 594 5501
EMail: eric+dkim@sendmail.org

Jim Fenton
Cisco Systems, Inc.
MS SJ-9/2
170 W. Tasman Drive
San Jose, CA 95134-1706
Phone: +1 408 526 5914
EMail: fenton@cisco.com

Mark Delany
Yahoo! Inc.
701 First Avenue
Sunnyvale, CA 94089
Phone: +1 408 349 6831
EMail: markd+dkim@yahoo-inc.com

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886
Phone: +1 831 480 2300
EMail: standards@taugh.com
URI: http://www.taugh.com

A. 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's or mail system's individual situation.

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 hosts will consider the mail not to have an Author Signature, even though the signature was present when the mail was originally sent.

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 group 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 paths that do not apply an Author Signature. Such paths could include MTAs at hotels or hotspot networks used by travelling users, or web sites that provide "mail an article" features.

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 group 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 prefer 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 might 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.

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.

B. Acknowledgements

This document greatly benefited from comments by Steve Atkins, Jon Callas, Dave Crocker, JD Falk, Arvel Hathcock, Ellen Siegel, Michael Thomas, and Wietse Venema.

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-02

- Merge in more text from ASP draft.
- Phrase actions as host's rather than checker.
- Explanatory description of i= matching.
- Lookup procedure consistently refers to one ASP record per lookup.
- Update security section w/ language from W. Venema
- Simplify imports of terms from other RFCs, add Local-part, 4234 -> 5234.
- Add usage example appendix.
- Add IANA considerations.
- Update authors list

C.2 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.3 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.4 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 to be published, and effect of wildcard records within the domain, on SSP.

C.5 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.6 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.

Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org [1].

[1] mailto:ietf-ipr@ietf.org