Network Working Group	E. Allman	
Internet-Draft	Sendmail, Inc.	
Intended status: Standards Track	J. Fenton	
Expires: November 12, 2009	Cisco Systems, Inc.	
	M. Delany	
	Yahoo! Inc.	
	J. Levine	
	Taughannock Networks	
	May 11, 2009	

TOC

DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)
draft-ietf-dkim-ssp-10

Status of this Memo

Copyright Notice

Abstract

DomainKeys Identified Mail (DKIM) defines a domain-level authentication framework for email to permit verification of the source and contents of messages. This document specifies an adjunct mechanism to aid in assessing messages that do not contain a DKIM signature for the domain used in the author's address. It defines a record that can advertise whether a domain signs its outgoing mail, and how other hosts can access that record.

Table of Contents

---

1. Introduction

TOC

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 names. It might be desirable for such domains to be able to advertise that fact to other hosts. This is the topic of Author Domain Signing Practices (ADSP).
Hosts implementing this specification can inquire what Author Domain Signing Practices a domain advertises. This inquiry is called an Author Domain Signing Practices check.
The basic requirements for ADSP are given in [RFC5016] (Thomas, M., "Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices

Protocol," October 2007.). This document refers extensively to [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.) 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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.)

---

2. Language and Terminology

TOC

2.1. Terms Imported from DKIM Signatures Specification

TOC

Some terminology used herein is derived directly from [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.). 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 [RFC5322] (Resnick, P., Ed., "Internet Message Format," October 2008.). Briefly,

- A "Signer" is the agent that signs a message, as defined in section 2.1 of [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.).

- A "Local-part" is the part of an address preceding the @ character, as defined in [RFC5322] (Resnick, P., Ed., "Internet Message Format," October 2008.) and used in [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.).

2.2. Valid Signature

TOC

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

(Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures,” May 2007.).

2.3. Author Address

TOC

An "Author Address" is an email address in the From header field of a message [RFC5322] (Resnick, P., Ed., “Internet Message Format,” October 2008.). If the From header field contains multiple addresses, the message has multiple Author Addresses.

2.4. Author Domain

TOC

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

2.5. Alleged Author

TOC

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

2.6. Author Domain Signing Practices

TOC

"Author Domain 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 Domain Signature

TOC

An "Author Domain Signature" is a Valid Signature in which the domain name of the DKIM signing entity, the d= tag in the DKIM-Signature header field, is the same as the domain name in the Author Address. Following [RFC5321] (Klensin, J., “Simple Mail Transfer Protocol,” October 2008.), domain name comparisons are case insensitive.
For example, if the From: line address is bob@domain.example, and the message has a Valid Signature, with the DKIM-Signature header field

containing d=domain.example, then the message has an Author Domain Signature.

---

3. Operation Overview

TOC

Domain owners publish ADSP information via a query mechanism such as the Domain Name System; specific details are given in Section 4.1 (DNS Representation).
Hosts can look up the ADSP information of the domain(s) specified by the Author Address(es) as described in Section 4.3 (ADSP Lookup Procedure). If a message has multiple Author Addresses the ADSP lookups SHOULD be performed independently on each address. This document does not address the process a host might use to combine the lookup results.

3.1. ADSP Applicability

TOC

ADSP as defined in this document is bound to DNS. For this reason, ADSP is applicable only to Author Domains with appropriate DNS records (see Note below). The handling of other Author Domains is outside the scope of this document. However, attackers may use such domain names in a deliberate attempt to sidestep an organization's ADSP policy statements. It is up to the ADSP checker implementation to return an appropriate error result for Author Domains outside the scope of ADSP. ADSP applies to specific domains, not domain subtrees. If, for example, an Author Address were user@domain.example, the Author Domain would be domain.example, and the applicable ADSP record would be at _adsp._domainkey.domain.example. An Author Address in a subdomain such as user@sub.domain.example would have a different ADSP record at _adsp._domainkey.sub.domain.example. ADSP makes no connection between a domain and its parent or child domains.

> **Note:** If an organization wants to publish Author Domain Signing Practices for all the subdomains it uses, such as host names of servers within the domain, it does so by creating ADSP records for every _adsp._domainkey.<sub>.domain.example. Wildcards cannot be used (see Section 6.3 (DNS Wildcards).); however, suitable DNS management tools could automate creation of the ADSP records.
>
> **Note:** The results from DNS queries that are intended to validate a domain name unavoidably approximate the set of Author Domains that can appear in legitimate email. For example, a DNS A record could belong to a device that does not even have an email implementation. It is up to the checker to decide what degree of approximation is acceptable.

3.2. ADSP Usage

TOC

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

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

3.3. ADSP Results

TOC

An ADSP lookup for an Author Address produces one of four possible results:

- Messages from this domain might or might not have an author domain signature. This is the default if the domain exists in the DNS but no ADSP record is found.
- All messages from this domain are signed with an Author Domain Signature.
- All messages from this domain are signed with an Author Domain Signature and discardable, i.e., if a message arrives without a valid Author Domain Signature, the domain encourages the recipient(s) to discard it.
- This domain is out of scope, i.e., the domain does not exist in the DNS.

An ADSP lookup could terminate without producing any result if a DNS lookup results in a temporary failure.

TOC

4. Detailed Description

4.1. DNS Representation

TOC

ADSP records are published using the DNS TXT resource record type. The RDATA for ADSP resource records is textual in format, with specific syntax and semantics relating to their role in describing ADSP. The "Tag=Value List" syntax described in section 3.2 of [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.) is used, modified to use WSP rather than FWS. 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 ADSP, 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.

> **Note:** ADSP changes the "Tag=Value List" syntax from [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.) to use WSP rather than FWS in its DNS records.
>
> **Note:** Domains MUST NOT publish ADSP records with wildcard names. Wildcards within a domain publishing ADSP records pose a particular problem, as discussed in more detail in Section 6.3 (DNS Wildcards).

4.2. Publication of ADSP Records

TOC

ADSP is intended to apply to all mail sent using the domain name string of an Alleged Author.

4.2.1. Record Syntax

TOC

ADSP records use the "tag=value" syntax described in section 3.2 of [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.), modified to use WSP rather than FWS. Every ADSP record MUST start with an outbound signing practices tag, so the first four

characters of the record are lower case "dkim", followed by optional whitespace and "=".
Tags used in ADSP records are described below. Unrecognized tags MUST be ignored. In the ABNF below, the WSP token, and the ALPHA and DIGIT tokens are imported from [RFC5234] (Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.).

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 Domain Signature.

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

Any other values are treated as "unknown".

ABNF:

```
adsp-dkim-tag = %x64.6b.69.6d *WSP "=" *WSP
                ("unknown" / "all" / "discardable")
```

4.3. ADSP Lookup Procedure

TOC

Hosts doing an ADSP lookup MUST produce a result that is semantically equivalent to applying the following steps in the order listed below. In practice, 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 ADSP record" is one that is both syntactically and semantically correct; in particular, it matches the ABNF for a tag-list and starts with a valid dkim tag.

Check Domain Scope: An ADSP checker implementation MUST determine whether a given Author Domain is within scope for ADSP. Given the background in Section 3.1 (ADSP Applicability) the checker MUST decide which degree of approximation is acceptable. The checker

MUST return an appropriate error result for Author Domains that are outside the scope of ADSP.

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 to fetch the named ADSP Record. If the result of this query is that the Author domain does not exist in the DNS (often called an NXDOMAIN error, rcode=3 in [RFC1035] (Mockapetris, P., "Domain names - implementation and specification," November 1987.)), the algorithm MUST terminate with an error indicating that the domain is out of scope. Note that a result with rcode=0 but no records (often called NODATA) is not the same as NXDOMAIN.

> 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 because this record type is thought to be the most common for domains used in e-mail, and will therefore produce a result which can be more readily cached than a negative result.

If the domain does exist, the checker MAY make more extensive checks to verify the existence of the domain, such as the ones described in Section 5 of [RFC5321] (Klensin, J., "Simple Mail Transfer Protocol," October 2008.). If those checks indicate that the Author domain does not exist for mail, e.g., the domain has no MX, A, or AAAA record, the checker SHOULD terminate with an error indicating that the domain is out of scope.

Fetch Named ADSP Record: The host MUST query DNS for a TXT record corresponding to the Author Domain prefixed by _adsp._domainkey. (note the trailing dot).

If the result of this query is a NOERROR response (rcode=0 in [RFC1035] (Mockapetris, P., "Domain names - implementation and specification," November 1987.)) with an answer which is a single record that is a valid ADSP record, use that record, and the algorithm terminates.

If the result of the query is NXDOMAIN or NOERROR with zero records, there is no ADSP record. If the result of the query contains more than one record, or a record that is not a valid ADSP record, the ADSP result is undefined.

If a query results in a SERVFAIL error response (rcode=2 in [RFC1035] (Mockapetris, P., "Domain names - implementation and specification," November 1987.)), the algorithm terminates

> without returning a result; possible actions include queuing the message or returning an SMTP error indicating a temporary failure.

See Appendix A (Lookup Examples) for examples of ADSP Lookup.

---

5. IANA Considerations

TOC

ADSP adds the following namespaces to the IANA registry. In all cases, new values are assigned only for values that have been documented in a published RFC after IETF Review as specified in [RFC5226] (Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," May 2008.).

5.1. ADSP Specification Tag Registry

TOC

An ADSP record provides for a list of specification tags. IANA has established the ADSP Specification Tag Registry for specification tags that can be used in ADSP fields.
The initial entry in the registry is:

TYPE	REFERENCE
dkim	(this document)

ADSP Specification Tag Registry Initial Values

5.2. ADSP Outbound Signing Practices Registry

TOC

The dkim= tag spec, defined in Section 4.2.1 (Record Syntax), provides for a value specifying Outbound Signing Practices. IANA has established the ADSP 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)

ADSP Outbound Signing Practices Registry Initial Values

5.3. Authentication-Results Method Registry Update

TOC

IANA is requested to add the following to the Email Authentication Method Name Registry:

> **Method:** dkim-adsp
>
> **Defined In:** this memo
>
> **ptype:** header
>
> **property:** from
>
> **value:** Contents of the [RFC5322] (Resnick, P., Ed., "Internet Message Format," October 2008.) From: header field, with comments removed

---

5.4. Authentication-Results Result Registry Update

TOC

IANA is requested to add or update the following in the Email Authentication Result Name Registry:

> **Code:** none
>
> **Existing/New Code:** existing
>
> **Defined In:** [RFC5451] (Kucherawy, M., "Message Header Field for Indicating Message Authentication Status," April 2009.)
>
> **Auth Method:** dkim-adsp (added)
>
> **Meaning:** No DKIM author domain signing practises (ADSP) record was published.

Code:
pass

Existing/New Code: existing

Defined In: [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.)

Auth Method: dkim-adsp (added)

Meaning: This message had an Author Domain Domain Signature that was validated. (An ADSP check is not strictly required to be performed for this result, since a valid Author Domain Signature satisfies all possible ADSP policies.)

Code: unknown

Existing/New Code: new

Defined In: this memo

Auth Method: dkim-adsp

Meaning: No valid Author Domain Signature was found on the message and the published ADSP was "unknown".

Code: fail

Existing/New Code: existing

Defined In: [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.)

Auth Method: dkim-adsp (added)

Meaning: No valid Author Domain Signature was found on the message and the published ADSP was "all".

Code: discard

Existing/New Code: new

Defined In: this memo

Auth Method: dkim-adsp

Meaning: No valid Author Domain Signature was found on the message and the published ADSP was "discardable".

Code: nxdomain

Existing/New Code:
new

Defined In: this memo

Auth Method: dkim-adsp

Meaning: Evaluating the ADSP for the Author's DNS domain indicated that the Author's DNS domain does not exist.

Code: temperror

Existing/New Code: existing

Defined In: [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.)

Auth Method: dkim-adsp (added)

Meaning: An ADSP record could not be retrieved due to some error that is likely transient in nature, such as a temporary DNS error. A later attempt may produce a final result.

Code: permerror

Existing/New Code: existing

Defined In: [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.)

Auth Method: dkim-adsp (added)

Meaning: An ADSP record could not be retrieved due to some error that is likely not transient in nature, such as a permanent DNS error. A later attempt is unlikely to produce a final result.

---

6. Security Considerations

TOC

Security considerations in the ADSP 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 Domain Signing Practices are found in the DKIM threat analysis (Fenton, J., “Analysis of Threats Motivating DomainKeys Identified Mail (DKIM),” September 2006.) [RFC4686].

6.1. ADSP Threat Model

TOC

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 a legitimate email author's name-recognition among recipients, by using the author's 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.

ADSP 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.

ADSP checkers may perform multiple DNS lookups per Alleged Author Domain. Since these lookups are driven by domain names in email message headers of possibly fraudulent email, legitimate ADSP checkers can become participants in traffic multiplication attacks on domains that appear in fraudulent email.

6.2. DNS Considerations

TOC

An attacker might attack the DNS infrastructure in an attempt to impersonate ADSP records 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 (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.) [RFC4033].

Because ADSP operates within the framework of the legacy e-mail system, the default result in the absence of an ADSP record is that the domain does not sign all of its messages. It is therefore important that the

ADSP clients distinguish a DNS failure such as SERVFAIL from other DNS errors so that appropriate actions can be taken.

6.3. DNS Wildcards

TOC

DNS wildcards (described in [RFC4592] (Lewis, E., "The Role of Wildcards in the Domain Name System," July 2006.)) that exist in the DNS hierarchy at or above the domain being checked interfere with the ability to verify the scope of the ADSP check described in Section 4.3 (ADSP Lookup Procedure). For example, a wildcard record for *.domain.example makes all subdomains such as foo.domain.example exist in the DNS. Domains that intend to make active use of ADSP by publishing a practice other than Unknown are advised to avoid the use of wildcards in their hierarchy.

If a domain contains wildcards, then any name that matches the wildcard can appear to be a valid mail domain eligible for ADSP. But the _adsp._domainkey. prefix on ADSP records does not allow publication of wildcard records that cover ADSP records without also covering non-ADSP records, nor publication of wildcard records that cover non-ADSP records without also covering ADSP records. A domain that uses ADSP practices other than unknown SHOULD NOT publish wildcard records.

6.4. Inappropriate Application of Author Domain Signatures

TOC

In one model of DKIM usage, a domain signs messages that are in transit through their system. Since any signature whose domain matches the Author Domain is by definition an Author Domain Signature, it would be unwise to sign mail whose Author Domain is the signer's domain if the mail is not known to meet the domain's standards for an Author Domain Signature.

One such use case is where a domain might apply such a signature is following application of an Authentication-Results header field as described in Section 7.1 of [RFC5451] (Kucherawy, M., "Message Header Field for Indicating Message Authentication Status," April 2009.). This problem can be easily avoided either by not applying a signature that might be confused with an Author Domain Signature or by applying a signature from some other domain, such as a subdomain of the Author Domain.

TOC

7. References

7.1. References - Normative

TOC

[RFC1035]	Mockapetris, P., “Domain names - implementation and specification,” STD 13, RFC 1035, November 1987 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” RFC 4033, March 2005 (TXT).
[RFC4592]	Lewis, E., “The Role of Wildcards in the Domain Name System,” RFC 4592, July 2006 (TXT).
[RFC4871]	Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures,” RFC 4871, May 2007 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 5226, May 2008 (TXT).
[RFC5234]	Crocker, D. and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” STD 68, RFC 5234, January 2008 (TXT).
[RFC5322]	Resnick, P., Ed., “Internet Message Format,” RFC 5322, October 2008 (TXT, HTML, XML).
[RFC5451]	Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” RFC 5451, April 2009 (TXT).

7.2. References - Informative

TOC

[RFC4686]	Fenton, J., “Analysis of Threats Motivating DomainKeys Identified Mail (DKIM),” RFC 4686, September 2006 (TXT).
[RFC5016]	Thomas, M., “Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices Protocol,” RFC 5016, October 2007 (TXT).
[RFC5321]	Klensin, J., “Simple Mail Transfer Protocol,” RFC 5321, October 2008 (TXT).

TOC

Appendix A. Lookup Examples

Assume the example domain publishes these DNS records: (In these examples, the numbers in parentheses are comments to help identify the records, not part of the records themselves.)

```
aaa.example                  A     192.0.2.1        (1)
_adsp._domainkey.aaa.example TXT   "dkim=all"       (2)

bbb.example                  MX 10 mail.bbb.example (3)
mail.bbb.example             A     192.0.2.2        (4)
```

A.1. Domain and ADSP exist

TOC

A mail message contains this From: header line:

```
From: bob@aaa.example (Bob the Author)
```

The ADSP Lookup first identifies the Author Address bob@aaa.example and the Author Domain aaa.example. It does an MX DNS query for aaa.example, and gets back a NOERROR result with no DNS records. (There's no MX record, but since record (1) exists, the name exists in the DNS.) Since that query didn't return an error, the Lookup proceeds to a TXT DNS query for _adsp._domainkey.aaa.example, which returns record (2). Since this is a valid DKIM record, the result is that all messages from this domain are signed.

A.2. Domain exists, ADSP does not exist

TOC

A mail message contains this From: header line:

```
From: alice@bbb.example (Old-fashioned Alice)
```

The ADSP Lookup first identifies the Author Address alice@bbb.example and the Author Domain bbb.example. It does an MX DNS query for bbb.example, and gets back record (3). Since that query didn't return an error, it then proceeds to a TXT DNS query for _adsp._domainkey.bbb.example, which returns NXDOMAIN. Since the domain exists but there is no ADSP record, ADSP returns the default unknown result: messages may or may not have an author domain signature.

TOC

A.3. Domain does not exist

A mail message contains this From: header line:

```
From: frank@ccc.example (Unreliable Frank)
```

The ADSP Lookup first identifies the Author Address frank@ccc.example and the Author Domain ccc.example. It does an MX DNS query for ccc.example, and gets back an NXDOMAIN result since there are no records at all for ccc.example. The lookup terminates with the result that the domain does not exist in the DNS and so is out of scope.

Appendix B. Usage Examples

TOC

These examples are intended to illustrate typical uses of ADSP. 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 Domain Signature, even though the signature was present when the mail was originally sent.

B.1. Single Location Domains

TOC

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 Domain Signature.
In this situation it might be appropriate to publish an ADSP record for the domain containing "all", depending on whether the users also send mail through other paths that do not apply an Author Domain Signature. Such paths could include MTAs at hotels or hotspot networks used by travelling users, web sites that provide "mail an article" features, user messages sent through mailing lists, or third party mail clients that support multiple user identities.

TOC

B.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 Domain 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 Domain 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.

Regardless of the DNS and key management strategy chosen, whoever maintains the DKIM records for the domain could also install an ADSP record containing "all".

B.3. Bulk Mailing Domains with Discardable Mail

TOC

In some cases, a domain might sign all of its outgoing mail with an Author Domain Signature, but prefer that recipient systems discard mail without a valid Author Domain Signature to avoid confusion from mail sent from sources that do not apply an Author Domain Signature. (In the case of domains with tightly controlled outgoing mail, this latter kind of mail is sometimes loosely called "forgeries".) In that case, it might be appropriate to publish an ADSP 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.

B.4. Third Party Senders

TOC

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 or author domain, using that domain in the RFC5322 From: or other headers. Due to the many and varied complexities of such agreements, third party signing is not addressed in this specification.

B.5. Domains with Independent Users and Liberal Use Policies

TOC

When a domain has independent users and its usage policy does not explicitly restrict them to sending mail only from designated mail servers (e.g. many ISP domains and even some corporate domains), then it is only appropriate to publish an ADSP record containing "unknown". Publishing either "all" or "discardable" will likely result in significant breakage because independent users are likely to send mail from the external paths enumerated in Appendix B.1 (Single Location Domains).

B.6. Non-email Domains

TOC

If a domain sends no mail at all, it can safely publish a "discardable" ADSP record, since any mail with an author address in the domain is a forgery.

Appendix C. Acknowledgements

TOC

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

Appendix D. Change Log

TOC

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

D.1. Changes since -ietf-dkim-09

TOC

*Change author signature to use d=.

*Change all "author signature" to "author domain signature".

*Add authentication results for IANA per Murray K.

*Minor editorial clarifications.

D.2. Changes since -ietf-dkim-08

TOC

*Simplify and clarify interpretation of d= and i=.

*Add note pointing out that i= usage conflicts with normal usage, and suggest workaround.

*Add note pointing out that you can mechanically add ADSP records for all the subdomains you use.

*in Section 3.2 (ADSP Usage) fix text to say that only an Author Signature counts.

D.3. Changes since -ietf-dkim-07

TOC

Clarify that ADSP records use WSP rather than FWS in 4.1 and 4.2.1.

D.4. Changes since -ietf-dkim-06

TOC

Minor editorial changes suggested by AD:

*expand DKIM in title

*clarify that there's no subdomain matching in Section 3.1 (ADSP Applicability)

*ADSP lookup can terminate without a result if the DNS lookup fails

*random dkim= values are treated as unknown

*in 4.2 note WSP not FWS

*in 4.3 note that NODATA is not NXDOMAIN

*add new Appendix A with lookup examples

Also address Tony's nits in http://mipassoc.org/pipermail/ietf-dkim/2008q3/010720.html. Make the examples consistently use the .example domain.

D.5. Changes since -ietf-dkim-05

TOC

Minor editorial nits: define NOERROR, SERVFAIL, NXDOMAIN as rfc1035 rcodes, change some punctuation, IANA section change IETF Consensus to the new IETF Review.

D.6. Changes since -ietf-dkim-04

TOC

- Require dkim at the front of each record.
- Disparage wildcard records.
- Changed ABNF use of whitespace from FWS back to WSP, dkim-base is wrong.
- RFC 2434 -> 5226, make ref to 4686 informational since it's not standards track.
- Improve examples with material from Ellen.

D.7. Changes since -ietf-dkim-03

TOC

- Name change for title and filename, to be ADSP
- String changes throughout, to author Domain signing practices and to aDsp.
- Added some keywords.
- Clarified comparison of local part and domain in Author Address.
- Streamlined the Abstract.
- Revised text of last bullet in Results list.
- Removed definitions not used in the document.

*Removed all specification details pertaining to sub-domains.

*Moved Lookup Procedure up one document level.

*Revised domain validity specification. Part in ADSP Usage in Operations section, and part as it as first step in Lookup.

*Fixed xml for figures, including labeling ABNF with new xml2rfc construct.

*Revised wildcard text.

*Removed 't' tag.

*Removed ADSP Flags Registry section.

*Changed ABNF use of whitespace from WSP back to FWS, for consistency with dkim-base.

D.8. Changes since -ietf-dkim-02

TOC

*Merge in more text from ADSP draft.

*Phrase actions as host's rather than checker.

*Explanatory description of i= matching.

*Lookup procedure consistently refers to one ADSP 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

TOC

D.9. 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).

D.10. Changes since -ietf-dkim-ssp-00

TOC

*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.

D.11. Changes since -allman-ssp-02

TOC

*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.

D.12. Changes since -allman-ssp-01

TOC

*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.

D.13. Changes since -allman-ssp-00

TOC

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

TOC

	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