pre-MASS
Internet-Draft
Expires: January 10, 2006

E. Allman
Sendmail, Inc.

July 9, 2005

# DKIM Sender Signing Policy
# draft-allman-dkim-ssp-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 [ID-DK-BASE]. This document describes the policy 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)

Security Considerations needs further work.

Need to add new and check existing ABNF.

DKP RR needs to be defined.

Text structure of document needs to be examined; this is a quick slash-and-burn approach. Stop signs indicate sections that haven't even been approached yet.

CONVERSION DISCLAIMER

This initial version that is being submitted as an IETF Internet-Draft has been converted over to RFC format by Dave Crocker. Besides the many rough edges to the resulting format of the document, he suspects there also might be some more serious errors, such as sub-sections being at the wrong level. These errors will be repaired as soon as they are reported.

Table of Contents

## 1. Introduction

DomainKeys Identified Mail (DKIM) [ID-DK-BASE] defines a method whereby email senders ("signers") may sign their outgoing messages with a secret key that can be checked by a receiver ("verifier") to determine whether the signer was authorized to use the sending domain name. The method used is based on well-known public-key cryptography methods.

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 senders may choose to sign all of their outgoing mail, for example, to protect their brand name. Such signers must be able to advertise to verifiers that messages claiming to be from them that are not signed are forgeries. This is the topic for sender signing policy.

In the absence of a valid DKIM signature on behalf of the "From" address [RFC2822], the verifier of a message MUST determine whether messages from a particular sender are expected to be signed, and what signatures are acceptable. In particular, whether a domain is participating in DKIM, whether they are testing, and whether it signs all outbound email must be communicated 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 Policy Check.

Sender Signing Policies MAY be expressed on behalf of an entity which may be a domain or an individual address. Expression of signing policy on behalf of individual addresses will, of course, entail additional key server transaction load.

Conceivably, such policy 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 of the need for outside auditing they fall under the purview of reputation and accreditation.

## 2. Language and Terminology

### 2.1 Originator Address

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 email address in the "Sender" header field.

- An "Alleged Signer" is the identify of the signer claimed in the DKIM-Signature header field in a message received by a verifier; it is "alleged" because it has not yet been verified.

- An "Alleged Sender" is the Originator Address of a message received by a verifier; it is "alleged" because it has not yet been verified.

- A "Sender Signing Policy" (or just "policy") is a machine-readable record published by the Alleged Sender which includes information about whether that sender signs all, some, or none of their email. It must be considered together with the "key" records, which advertise the public keys associated with the Alleged Sender.

### 2.2 Suspicious

Messages that fail an initial signature verification step (either by an incorrect signature or a lack of signature) and also a further

Sender Signing Policy check 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 layer; a verifier may decide the message should be accepted on the basis of other information beyond the scope of this document. Conversely, messages deemed non-Suspicious may be rejected for other reasons.

Some terminology used herein is derived directly from [ID-DK-BASE]. Briefly,

- A "signer" is the agent that signs a message. In normal cases it will probably correspond closely with the original author of the message or an agent working on the author's behalf. However, third parties are often legitimately involved with mail sending, and hence it is reasonable for what may seem at first glance to be an unaffiliated third party might reasonably send mail on behalf of another domain. Hence, "signer" refers only to the administrative authority that has the secret key necessary to sign the message. In particular, that secret key may have been transferred to them or otherwise delegated to them by the alleged sender.

- 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 Policy published by the alleged sender if the





message is not correctly signed by the Alleged Sender.

- A "selector" specifies which of the keys published by an Alleged Signer or Sender should be queried. It is essentially a way of subdividing the address space to allow a single sending domain to publish multiple keys.

## 3. Overview of DKIM

This section is informative only and MUST NOT be treated as normative. The actual specification is described in [ID-DK-BASE] and must be consulted.

Briefly, when a verifier receives a message, they examine the header

field of that message to see if it includes one or more DKIM-Signature header fields. If it does, the authenticity of that message may be validated using conventional cryptographic techniques. However, if the verifier receives a message containing no valid DKIM-Signature header fields, it must proceed with the algorithms defined in this document.

## 4. Operation

Sender Signing Policy Checks MUST be based on the Originator Address. If the message contains a valid signature on behalf of the Originator Address no Sender Signing Policy Check need be performed: the verifier SHOULD NOT look up the Sender Signing Policy and the message SHOULD be considered non-Suspicious.

Verifiers checking messages that do not have at least one valid signature MUST perform a Sender Signing Policy Check by doing a DNS query to the domain specified by the Originator Address. The query MUST be for the search key "_policy._domainkey.<domain>", where <domain> is the domain of the Originator Address. The query may return either a DKSSP record or a TXT record; the DKSSP record MUST override the TXT record.

The result of a Sender Signing Policy Check is one of four possible policies:

(1) Some messages from this entity are not signed; the message SHOULD be presumed to be legitimate in the absence of a valid signature. This is the default policy.z

(2) All messages from this entity are signed; all messages from this entity SHOULD have a valid signature, either directly on behalf of the originator or on behalf of a third party (e.g., a





mailing list or an outsourcing house) handling the message.

(3) All valid messages from this entity are signed, and SHOULD have a valid signature from this entity. Third-party signatures SHOULD not be accepted.

(4) Signing policy for this domain is expressed at the individual address level. A second Sender Signing Policy Check should be

performed specifying the individual address.

(5) This Alleged Sender never sends mail at all.

If a message is encountered by a verifier without a valid signature from the Originator Address, the policy results MUST be interpreted as follows:

If the result of the check is policy (1) described above, the message MUST be considered non-Suspicious.

If the result of the check is policy (2), and any verifiable signature is present from some signer other than the Originator Address in the message, the message SHOULD be considered non-Suspicious.

If the result of the check is policy (3), the message MUST be considered suspicious.

If the result of the check is policy (4), a second Sender Signing Policy Check SHOULD be performed based on the entire Originator Address and interpreted using the above steps. If the result of that check is policy (4), the signing policy for the originator is misconfigured, and the message SHOULD be considered non-Suspicious.

If the Sender Signing Policy record does not exist, verifier systems MUST assume that some messages from this entity are not signed and the message SHOULD NOT be considered to be Suspicious.

## 5. Query and record format

Signing policy records for a domain are published in key servers as the "_policy" selector. Signing policy records for individual addresses are published as the "user._policy" selector.

NON-NORMATIVE RATIONALE: Use of a synthetic selector allows non-DNS based access for signer policies.





To avoid a Denial-of-Service attack, signer policy searches for

signing policy checks of very deeply nested domains MUST strip off all but the last five components of a domain name. If a policy record is not found, the verifier MUST repeat the request to successively higher levels of the domain hierarchy until the root is reached. This allows subdomains to inherit the signing policy of their parent domains without allowing attackers to specify extremely deep subdomains such as "a.b.c.d.e.f.g.h.i.j.k.l.m.n.o.p.q.r.s.t.u.v.w.x.y.z.example.com". If presented with such a signing domain in a DKIM-Signature header field, the search for a policy record would start at "x.y.z.example.com" and proceed upwards. Verifiers MUST stop searching at the first policy record they encounter.

NON-NORMATIVE DISCUSSION: It seems like this limitation should be part of the DNS binding rather than a general restriction.

Signing policy records follow the tag-value syntax described in [ID-DK-BASE]. Tags used in signing policy records are as follows:

o= Outbound signing policy for the entity (plain-text; OPTIONAL, default is "~"). Possible values are as follows:

~ The entity signs some but not all email.

- All mail from the entity is signed; unsigned email MUST NOT be accepted, but email signed by a third party SHOULD be accepted.

! All mail from the entity is signed; third-party signatures SHOULD NOT be accepted

. This entity never sends email. The "." policy can be used to "short circuit" searches from subdomains; for example, the "ad.jp" domain might use this. If an initial policy search receives this policy then the email SHOULD NOT be accepted; if found while searching parent domains then the search should terminate as though no policy record was found.

^ Repeat query at user level. This value MUST NOT be used in user-level policy records.

t= A vertical-bar separated list of flags (plain-text; OPTIONAL, default is that no flags are set). Flag values are:

y -- The entity is testing signing policy, and the verifier SHOULD NOT consider a message suspicious based on the record.

n= Human readable notes regarding the record (quoted-printable with semicolon encoded in addition to the standard characters; OPTIONAL, default is no notes).

r= Email address for reports and inquiries regarding the signing policy for this entity (plain-text; OPTIONAL, default is no contact address available).

u= Reserved for future reference to a URI to provide more detailed policy information.

When represented in DNS, signing policy checks MUST search for a DKSSP (DomainKey Sender Signing Policy) RR type first. If no DKSSP RR is found, signing policy checks MUST search for a TXT RR type.

## 6. IANA Considerations

Use of the _domainkey prefix in DNS records will require registration by IANA.

Use of the _policy prefix in DNS records will require registration by IANA.

The DKSSP RR type must be registered by IANA.

## 7. Normative References

[ID-DK-BASE] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM)", draft-allman-dkim-base-00 (work in progress), July 2005.

[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.

Author's Address

Eric Allman
Sendmail, Inc.
6425 Christie Ave, Suite 400
Emeryville, CA 94608
USA

Phone: +1 510 594 5501
Email: eric+dkim@sendmail.org
URI:

## Intellectual Property Statement



## Disclaimer of Validity

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.