DKIM Working Group	D. Otis	
Internet-Draft	Trend Micro	
Intended status: Standards Track	D. Black	
Expires: April 24, 2010	October 21, 2009	

TOC

DKIM Third-Party Authorization Label
draft-otis-dkim-tpa-label-03

Status of this Memo

Copyright Notice

Abstract

A third party authorization label (TPA-Label) is a DNS-based prefix for DKIM ADSP records that acts as a scheme for domains to authorize acceptable third-party signatures for messages containing their domain within the From header. This scheme allows Author Domains to autonomously authorize a range of third-party domains using scalable, individual DNS transactions. This authorization extends the scope of

DKIM signing practice assertions as a means to supplant more difficult to administer schemes. Alternatives for facilitating third-party authorizations currently necessitate the coordination between two or more domains to synchronously set up selector/key DNS records, DNS zone delegations, and/or the regular exchange of public/private keys. Checking TPA-Label Resource Records for signing practices may occur when an Author Domain Signature is missing or is invalid and a Third Party Signature exists. When a third-party signature is found, TPA-Label Resource Record transactions offer an efficient means for Author Domains to authorize specific third-party signing domains and for recipients to determine whether an authorization exists. The TPA-Label Resource Record scheme reduces reliance upon email source reputation that is often based upon an IP address rather than the domain.

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

Table of Contents

---

1. Introduction

TOC

Normally a DKIM authorization effort will likely involve sharing a number of details between the domain owner, and one or more email and DNS providers. Since there are many ways in which such authorizations can be accomplished, it is unlikely there will be consistent or standardized formats developed to exchange necessary, and at times, sensitive information. In addition, when there is a security breach, the wrong party might be held accountable for content they may have never seen nor logged. The TPA-Label Resource Record scheme permits the DKIM signature header to clarify who signed the message and on whose behalf, while also permitting greater control of specific header field authorizations made by the Author Domain.

This document describes how any Author Domain publishing DKIM ADSP records defined in [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.), can also autonomously authorize DKIM signatures [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures,” May 2007.) (updated by [RFC5672] (Crocker, D., “RFC 4871 DomainKeys Identified Mail (DKIM) Signatures -- Update,” August 2009.))

by specific third-party domains. TPA-Label listed domains offer secondary signing practices for compliance options when no Author Domain Signature is present within the message. Recommended or suggested actions for DKIM receivers are not included, and are considered "out-of-scope" for this document. The receiver is considered best able to determine the impacts of email handling based on TPA-Label Resource Records. The intended purpose of TPA-Label Resource Records are to improve acceptance rates of genuine messages and to lessen administrative costs associated with email.
TPA-Label Resource Records authorize third-party signing domains as a means to extend DKIM compliance options for signing practices defined by [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.). TPA-Label listed domains are to be considered equivalent to the authorizing Author Domain when assessing compliance with DKIM signing practices. The TXT resource records associated with TPA-Label start with the 'dkim' tag as defined by [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.) for signing practices, and may contain tags specifically defined for TPA-Label Resource Records.

2. Language and Terminology

TOC

2.1. Terms Imported from other DKIM Specifications:

TOC

> A "Valid Signature" is any signature on a message that 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.).
>
> "Author Address" is defined in Section 2.3 of [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.).
>
> "Author Domain" is defined in section 2.4 of [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.).

> "Alleged Author" is defined in Section 2.5 of [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)," August 2009.).
>
> "Author Domain Signature" is defined in Section 2.7 of [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)," August 2009.)

2.2. Terms Defined by this Specification: TOC

2.2.1. Third Party Domain TOC

A "Third Party Domain" is an originating domain within a message that is not at or below the Author Domain.

2.2.2. Third Party Signature TOC

A "Third Party Signature" is a Valid Signature that does not qualify as a Author Domain Signature.

> Editor's Note: While this term is defined in Section 6 of [I-D.ietf-dkim-deployment] (Hansen, T., Siegel, E., Hallam-Baker, P., and D. Crocker, "DomainKeys Identified Mail (DKIM) Development, Deployment and Operations," January 2010.) and in Section 2 of [RFC5016] (Thomas, M., "Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices Protocol," October 2007.), this definition is in terms of the Author Domain Signature and avoids statements about any header field dependencies.

2.2.3. Third Party Signer TOC

A "Third Party Signer" is a signer that adds a valid DKIM signature that references a Third Party Domain with the 'd=' tag in the DKIM-Signature header field.

2.2.4. TPA-Label Listed Domain

TOC

TPA-Label Listed Domain, TPA-LLD, is a domain TXT resource record that can be referenced with a TPA-Label within an Author Domain. When a "tpa" tag exists within the TXT resource record located at the TPA-Label, the referenced domain must be within a listed domain. When this tag does not exist, the referenced domain is presumed listed. The "scope" tag provides the TPA-LLD authorization, limited to the scoped message elements, to act on behalf of Author Domain publishing the TPA-Label Resource Record.

2.2.5. Author's Domain Acceptable Third-Party Signature

TOC

An "Author's Domain Acceptable Third-Party Signature" is a Valid Signature in which the domain name of the DKIM signing entity, i.e., the 'd=' tag in the DKIM-Signature header field, is the domain name referenced in the TPA-Label Resource Record published by the Author Domain with a scope of 'F', or 'L' when the List-ID is within the TPA-LLD. Following [RFC5321] (Klensin, J., “Simple Mail Transfer Protocol,” October 2008.), domain name comparisons as well as TPA-Labels are case insensitive.

3. TPA-Label Resource Record Authorization Considerations

TOC

When an Author Domain is not within the DKIM signing domain, the TPA-LLD scheme can safely extend ADSP signing practice compliance. The TPA-LLD scheme with an 'F' or 'L' scope permits a contained Third Party Signature to be treated as a Author Domain Signature. This avoids a need for Author Domains to always be within the public key reference for compliance with restrictive ADSP signing practices. The TPA-LLD scheme for offering valid signatures only requires that DNS publications be made by Author Domains, even when signing domains and the Author Domain differ. This approach also avoids any need to exchange DKIM key information as well.

While offering only valid signatures will not ensure all possible spoofing is prevented, messages signed in this manner should not receive annotations that indicate the message contains authenticated identities either. The TPA-LLD scheme plays the role of only providing acceptable signatures which might be suitable for non-critical messages, where the goal would be to improve delivery acceptance, such

as those from specific mailing-lists. Before TPA-LLD authorization is deployed, the Author Domain should be assured by the domains being authorized that appropriate measures are in place to authenticate those submitting messages.

3.1. Evaluating the Third-party Signing Domain

TOC

An Author Domain deploying a TPA-Label Resource Record for a Third Party Signer does so on a trust basis. Reasons for deploying TPA-Label Resource Records might be to allow selective deployment of more stringent ADSP records, such as "dkim=all". TPA-Label Resource Records can help reduce the receiver's reliance upon reputation services when evaluating any signing practice compliance exception. In addition, most reputation services use IP addresses, rather than domains, as their basis for evaluation. An IP address basis reduces the benefits that might be obtained by using DKIM signatures. TPA-Label Resource Record authorization by-name scheme can influence whether a message is accepted or rejected, and might even impact the reputation of the Author Domain itself.
This act of trust can be abused by Bad Actors when an authorized Third Party Signer does not employ necessary authentication control to ensure messages are from an Author Address before applying their signature. A lack of authentication control may result in Bad Actors successfully spoofing an email as being from an Author Address by exploiting the authorization granted by a TPA-Label Resource Record.

3.1.1. Third Party Authentication

TOC

The Author Domain SHOULD ensure the Authorization Scope of the TPA-Label Resource Record is authenticated. There are a number of ways email can be authenticated, and different authentication mechanism validate different parts of the email. The following are examples of how authentication might work:

3.1.1.1. Third Party Authentication - Web Email Provider with Subscriber Pingbacks

TOC

The Author Domain "example.com" wants to deploy a TPA-Label Resource Record to permit their traveling agents the use of "webmail.example.net" services. This email provider has a closed user

policy and adds DKIM signatures to messages on behalf of the "webmail.example.net" domain.
The closed user policy of "webmail.example.net" permits subscribers to post messages with Author Domains that are not "webmail.example.net" in the From header fields only when control of the Author Addresses has been validated by a response to an encoded "pingback" email. The "webmail.example.net" service also establishes accounts to authenticate all users sending messages through their service. Therefore, the referenced TPA-Label Resource Record can include an 'F' scope value to authorize Author Domain messages to be signed by this Third-Party Signer.

3.1.1.2. Third Party Authentication - Closed Mailing List Example

TOC

The Author Domain wants to deploy a TPA-Label Resource Record for a mailing list with a closed posting policy that redistributes email in a way that breaks Author Domain Signatures, but that adds a DKIM signature on behalf of their domain and includes an Authentication-Results header field for posted messages. The closed posting policy is enforced by requiring subscribers to validate their control of their Author Address by responding to encoded "pingback" email sent to this address.
Because the list management always verifies control of the Author Address, is configured to include Authentication-Results headers, the referenced TPA-Label Resource Record can include an 'L' scope value to permit Author Domain messages containing an authorized List-ID domain to be signed by this Third-Party Signer.

3.1.1.3. Third Party Authentication - Open Mailing List Example

TOC

The Author Domain wants to deploy a TPA-Label Resource Record for a mailing list with an open posting policy that redistributes email in a way that breaks Author Domain Signatures, but that adds a DKIM signature on behalf of their domain and includes an Authentication-Results header field for posted messages. The open posting policy will refuse messages lacking Author Domain Signatures for domains that have deployed an ADSP signing practice of "dkim=all" or "dkim=discardable".
Because the list management always refuses the posting of an Author Address lacking a Author Domain Signature when the domain has deployed an ADSP record with an "dkim=all" or "dkim=discardable", and is configured to include Authentication-Results headers, the referenced TPA-Label Resource Record can include an 'L' scope value to permit

Author Domain messages containing an authorized List-ID domain to be signed by this Third-Party Signer.

3.1.1.4. Third Party Authentication Example - Sender Header Field

TOC

Author Domain "example.com" wishes to temporarily employ the service agency "temp.example.org" to handle overflow secretarial support. The agency "temp.example.org" sends email on behalf of the executive staff of "example.com" and adds the Sender header field of "secretary@example.org" in the email. Since "temp.example.org" only allows its own staff to email through its server that adds "temp.example.org" DKIM signatures, a TPA-LLD can include the "temp.example.org" domain with 'O' and 'F' scope to specifically authorize the use of the Sender header field to help ensure these messages are not detected as a phishing attempt.

3.1.1.5. Third Party Authentication Example - SMTP Host

TOC

Author Domain "example.com" makes use of Virtual Private Servers to handle their enterprise services. This VPS service provides a shared outbound SMTP server with the host name given by the EHLO command as "vps.example.net". The Author Domain can authorize the domain "vps.example.net" with the scope of 'H' to improve acceptance of DKIM signed messages that are on behalf of "example.com" from this outbound server.

---

4. Abuse and DSN Reporting

TOC

The ancillary scopes available within the TPA-LLD records allow the Author Domain to be associated with SMTP Clients publicly transmitting messages and/or the Mail return path when these domains differ. Appropriate DSN or abuse reporting is better assured as a result. The correspondence between SMTP Client hosts and Mail return path can be affirmed by the TPA-LLD scheme with a scope of 'H' or 'M' that might be used to better categorize feedback data or DSN destinations. In addition, a correspondence with SMTP Client hosts may help in determining which outbound SMTP Clients are to be monitored for consistent IP address use. Relationships established between email related domains and stable hosts by the TPA-LLD scheme may provide both improved message acceptance and reporting criteria.

5. DNS Representation

TOC

The receiver obtains domain authorizations with a DNS query for an IN class TXT TPA-Label resource record located below the ADSP record location specified in [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.) section 4.3. The TPA-Label is normally generated by processing the domain referenced within the DKIM signature's "d=" parameter. A TPA-Label Resource Record is then published below the [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.) conventional ADSP record, for example below "._adsp.domainkey.<Author-Domain>". The Author Domain provides authorization for other domains with the existence of a TPA-Label TXT resource record that when a "tpa" tag value exists, it includes the referenced domain. Authorization to act on behalf of the Author Domain is limited by the "scope" tag value to specific message elements. Character-strings contained within the TXT resource record are concatenated into forming a single string. A character-string is a single length octet followed by that number of characters treated as binary information. As an example, a TPA-Label Resource Record may be located at these domains:

> <tpa-label>._adsp._domainkey.<Author-Domain>.

6. TPA-Label and Tag Syntax Definitions

TOC

> "base32" function is defined in [RFC4648] (Josefsson, S., “The Base16, Base32, and Base64 Data Encodings,” October 2006.).
>
> "sha1" function is defined in [FIPS.180-2.2002] (National Institute of Standards and Technology, “Secure Hash Standard,” August 2002.).
>
> "lcase" converts upper-case ALPHA characters to lower-case.
>
> "signing-domain" is the "d=" tag value defined in Section 3.5 of [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures,”

May 2007.).

Augmented BNF for Syntax Specifications:

```
asterisk = %x2A ; "*"
dash = %x2D ; "-"
dot = %x2E ; "."
underscore = %x5F ; "_"
ANY = asterisk dot ; "*."
dns-char = ALPHA / DIGIT / dash
id-prefix = ALPHA / DIGIT
label = id-prefix [*61dns-char id-prefix]
sldn = label dot label
base-char = (dns-char / underscore)
domain = *(label dot) sldn
tpa-label = underscore base32( sha-1( lcase(signing-domain)))
```

---

7. TPA-Label Generation

TOC

The TPA-Label is created from the hash value returned by the "sha1" function of the signing-domain expressed in lower case ASCII. The hash is then converted to a base32 character set, with the resulting label prefixed with an underscore. Any terminating period is not included with the signing-domain, as indicated by the ABNF definition.

> Note: No newline character, 0x0A, is to be appended to the end of the domain name, as might occur with the command line generation of SHA1 values. Command line appended newlines can be avoided by using the 'echo -n" option, for example.

---

8. TPA-Label TXT Resource Record Structure

TOC

Every TPA-Label TXT resource record MUST start with an outbound signing-practices tag, so the first four characters of the record are lowercase "dkim", followed by optional whitespace and "=". In addition to the tags defined by [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.), TPA-Label syntax descriptions for additional tags follow the tag-value syntax described in section 4.2.1 of [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine,

"DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)," August 2009.) and 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.). Unrecognized tags and tags with illegal values MUST be ignored. In the ABNF below, the WSP token is inherited from [RFC5322] (Resnick, P., Ed., "Internet Message Format," October 2008.). The ALPHA and DIGIT tokens are imported from [RFC5234] (Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.). The tags used in TPA-Label resource records are as follows:

Tag	Function
scope=	Authorization Scope List (as-list)
tpa=	Authorized Domains List (ad-list)

TPA-Label Extended Tags

Scope Values	Field or Parameter
F	From (Author) Header
L	List-ID
O	Other than From (Author) Headers
M	MailFrom
H	SMTP Host

TPA-Label Scope Values

8.1. TPA-Label Resource Record Scope Syntax

TOC

scope= Authorization Scope List (Optional). This tag defines a list of scoping assertions for various email-address locations within the message. Only recognized scope values offer any form of DKIM authorization.

```
scope = "F" / "L" / "O" / "M" / "H"
```

```
as-list = "scope" [WSP] "=" [WSP] scope 0*([WSP] ":" [WSP] scope)
```

8.1.1. TPA-Label Listed Domain Authorization

TOC

8.1.1.1. From (Author) Header Field

TOC

The "F" scope asserts that messages carrying the Author Domain within the From header field are authorized to be signed by the TPA-LLD. When the Third Party Signing Domain is within the TPA-LLD, then the signing practice, the value of the "dkim" tag, can supersede the signing practice generally asserted by the conventional ADSP record.

8.1.2. List-ID Header Field

TOC

The "L" scope asserts that a List-ID identifier of the List-ID header field [RFC2919] (Chandhok, R. and G. Wenger, “List-Id: A Structured Field and Namespace for the Identification of Mailing Lists,” March 2001.) that is within the TPA-LLD are also authorized. When the LIST-ID is within the TPA-LLD, then the signing practice, the value of the "dkim" tag, can supersede the signing practice generally asserted by the conventional ADSP record. When 'L' is used in absence of the 'F' scope, then an 'F' scope is assumed only when List-ID is authorized. Asserting a signing practice of "unknown" for an TPA-LLD might be used to aid acceptance of messages from mailing lists that have not yet adopted use of DKIM.

8.1.3. Ancillary Use of Domain Authorizations

TOC

Ancillary Authorizations will not alter TPA-LLD results.

TOC

8.1.3.1. Other Originating Header Fields

The "O" scope asserts that messages with Sender, Resent-From, or Resent-Sender header fields with email-address domains within the TPA-LLD are also authorized.

8.1.3.2. MailFrom Parameter

TOC

This "M" scope asserts that an email-address domain that is within a TPA-LLD used in the [RFC5321] (Klensin, J., "Simple Mail Transfer Protocol," October 2008.) MAIL command is also authorized.

8.1.3.3. SMTP Host domains

TOC

The "H" scope asserts that host names given in [RFC5321] (Klensin, J., "Simple Mail Transfer Protocol," October 2008.) EHLO or HELO commands within TPA-LLD are also authorized. This scope might be used to better ensure DKIM signatures within messages from these hosts are validated.

---

9. Authorized Signing Domain

TOC

tpa= Authorized Signing Domain list. (optional) This tag when present, MUST repeat all or portions of the domain encoded within the TPA-Label Resource Record. This option ensures the proper handling of possible hash collisions. When a domain is prefixed with the "*." ANY label, then all subdomains of this domain are to be considered included within the list. When the 'tpa' tag is not present or has no value, it should be assumed to compare with the domain used to generate the TPA-Label.

```
ad = [ANY] domain

ad-list = "tpa" [WSP] "=" [WSP] ad 0*([WSP] ":" [WSP] ad)
```

---

10. TPA-Label Resource Record Query Transactions

TOC

The discovery of TPA-Label resource records need not be subsequent to the discovery of the ADSP record specified by [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.). However, when no ADSP record is discovered, the verifier MAY assume that no TPA-Label Resource Records have been published below this location. Otherwise, when there is a Third Party Signature without any Author Domain Signature, then the discovery of TPA-Label Resource Records should be attempted. The discovery of a TPA-Label Resource Record may be attempted for LIST-ID domains as well.

---

11. TPA-Label Resource Record Compliance Assessment

TOC

Signing practice compliance assessment of Third Party Signatures is a discretionary operation performed by the verifier. Where a verifier decides to assess compliance with signing practices asserted by the Author Domain for Third Party Signatures, all of the following conditions MUST be met for the result to be considered a pass.

- The Third Party Signature MUST validate according to [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures,” May 2007.).

- The TPA-Label TXT Resource Record MUST exist in DNS.

- The TPA-Label TXT Resource Record Structure MUST be valid.

- Where a scope of "F" is specified, then the Author Domain MUST have an Author Domain Signature or an Author's Domain Acceptable Third-Party Signature.

- Where a scope of "L" is specified, then when a List-ID identifier in the List-ID header field is within the TPA-LLD, then the Author Domain MUST have an Author Domain Signature or an Author's Domain Acceptable Third-Party Signature.

When the TPA-Label TXT Resource Record can not be retrieved due to some error that is likely transient in nature, as specified in [RFC5617] (Allman, E., Fenton, J., Delany, M., and J. Levine, “DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP),” August 2009.) Section 4.3. such as "SERVFAIL" for example, the result of the TPA-Label Resource Record compliance assessment is "temperror".

When the TPA-Label TXT Resource Record can not be retrieved with a DNS "NOERROR" with zero or more than one TXT records, the result of the TPA-Label Resource Record compliance assessment is "permerror".
When the TPA-Label TXT Resource Record can not be retrieved with a DNS "NXDOMAIN",the result of the TPA-Label Resource Record compliance assessment is "nxdomain".
When one or more valid Third-Party Signatures are present in the message, then:

*When a TPA-Label Resource Record referenced from the Author Domain has a scope tag of "F", and the TPA-LLD represents the domain of the DKIM signing entity, then the message is considered signed with an Author Domain Acceptable Third-Party Signature.

*When a TPA-Label Resource Record referenced from the Author Domain has a scope tag of "L", and the List-ID given by [RFC2919] (Chandhok, R. and G. Wenger, “List-Id: A Structured Field and Namespace for the Identification of Mailing Lists,” March 2001.) in the List-ID header is within the TPA-LLD, and the TPA-LLD represents the domain of the DKIM signing entity, then the message is considered signed with an Author Domain Acceptable Third-Party Signature.

*When a TPA-Label Resource Record referenced from the Author Domain returns a TXT resource record that has a scope tag of "O", and the email-address domain within the Sender, Resent-From, or Resent-Sender headers are within the TPA-LLD, use of these headers by this domain is authorized by the Author Domain.

*When a TPA-Label Resource Record referenced from the Author Domain returns a TXT resource record that has a scope tag of "M", and the email-address domain within the [RFC5321] (Klensin, J., “Simple Mail Transfer Protocol,” October 2008.) MAIL command is within the TPA-LLD, use of this command by this domain is authorized by the Author Domain.

*When a TPA-Label Resource Record referenced from the Author Domain returns a TXT resource record that has a scope tag of "H", and a host domain given by [RFC5321] (Klensin, J., “Simple Mail Transfer Protocol,” October 2008.) EHLO or HELO command is within the TPA-LLD, the SMTP client is authorized by the Author Domain.

12. IANA Considerations

TOC

12.1. Email Authentication Method Registry

TOC

To accommodate the method derived from TPA-Label Resource Record processing, The IANA Registry "Email Authentication Method" defined by Section 6.2 of [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.) needs the following elements to be added:
Note to RFC EDITOR: This is currently located at: http://www.iana.org/assignments/email-auth/email-auth.xhtml#email-auth-methods

Method	Defined	ptype	property	value
tpa-lld	[THIS DOCUMENT]	header	d	value of signature "d" tag. The dkim method results from [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.) should also be included in a Authenticated Results header field
			scope	value of scope (Third Party Authorizations Scope Registry) tag. (When 'scope' contains 'H', the iprev (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.) [RFC5451] (Section 3) method results should also be included in the Authenticated-Results header field)
			ca-scope	The scopes (Third Party Authorizations Scope Registry) with a compliance assessment as pass
			tpa	Value of tpa (Authorized Signing Domain) tag at time of compliance assessment

TPA-Label Resource Record validation Method

12.2. Email Authentication Result Names Registry

TOC

To accommodate the results derived from TPA-Label Resource Record processing, The IANA Registry "Email Authentication Method" defined by Section 6.3 of [RFC5451] (Kucherawy, M., “Message Header Field for Indicating Message Authentication Status,” April 2009.) needs the following elements added:
Note to RFC EDITOR: This is currently located at: http://www.iana.org/assignments/email-auth/email-auth.xhtml#email-auth-result-names

code	method	meaning
none	tpa-lld	No TPA-Label was published
pass	tpa-lld	section Section 11 (TPA-Label Resource Record Compliance Assessment)
tempfail	tpa-lld	section Section 11 (TPA-Label Resource Record Compliance Assessment)
permfail	tpa-lld	section Section 11 (TPA-Label Resource Record Compliance Assessment)
unknown	tpa-lld	The TPA-Label Resource Record had a tag/value of "dkim=unknown" and the Third Party Signature failed its compliance assessment.
discard	tpa-lld	The TPA-Label Resource Record had a tag/value of dkim=discard and the Third Party Signature failed its compliance assessment.
fail	tpa-lld	The TPA-Label Resource Record had a tag/value of dkim=all and the Third Party Signature failed to its compliance assessment.
nxdomain	tpa-lld	When obtaining the TPA-Label Resource Record, DNS indicated this domain does not exist.
Other value defined in the IANA ADSP Outbound Signing Practices Registry	tpa-lld	The TPA-Label Resource Record had a tag/value of dkim={other value} and the Third Party Signature failed to its compliance assessment.

TPA-Label Resource Record complaince assessment Results

12.3. Third Party Authorizations Labels Registry

TOC

Names of tags that are valid in TPA-Label Resource Records with the exception of experimental tags Section 8 (TPA-Label TXT Resource Record Structure) MUST be registered in this created IANA registry.
New entries are assigned only for values that have been documented in a published RFC that has had IETF Review, per IANA CONSIDERATIONS (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.) [RFC5226].
Each tag registered must correspond to a definition.
The initial set of values for this registry is:

tag	defined	definition
dkim	Section 8 (TPA-Label TXT Resource Record Structure)	As per IANA Registry ADSP Outbound Signing Practices
scope	Section 8.1 (TPA-Label Resource Record Scope Syntax)	Section 12.4 (Third Party Authorizations Scope Registry)
tpa	Section 9 (Authorized Signing Domain)	List of authorized domains

TPA-Label Resource Record compliance assessment Results

12.4. Third Party Authorizations Scope Registry

TOC

Values that correspond to Section 8.1 (TPA-Label Resource Record Scope Syntax) MUST be registered in this created registry:
New entries are assigned only for values that have been documented in a published RFC that has had IETF Review, per IANA CONSIDERATIONS (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.) [RFC5226].
Each value registered must correspond to a definition.
The initial set of values for this registry is:

value	defined
F	Section 8.1.1 (TPA-Label Listed Domain Authorization)
L	Section 8.1.2 (List-ID Header Field)
O	Section 8.1.3.1 (Other Originating Header Fields)

M	Section 8.1.3.2 (MailFrom Parameter)
H	Section 8.1.3.3 (SMTP Host domains)

TPA-Label Resource Record compliance assessment Results

---

13. Security Considerations

TOC

This draft extends signing practices related to [RFC4871] (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007.) where most generic DKIM Signature related security matters are discussed there. Security considerations for the TPA-Label Resource Record scheme are mostly related to attempts on the part of malicious senders to represent themselves as other senders, often in an attempt to defraud either the recipient or the alleged originator. Additional security considerations regarding DKIM signing practices may be found in the DKIM threat analysis [RFC4686] (Fenton, J., "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)," September 2006.).

13.1. Benefits to Recipients

TOC

The verifier, after finding an Author's Domain Acceptable Third-Party Signature in a message, has a significantly greater confidence in the Third-Party authorization than when the no TPA-Label Resource Record could be retrieved. This enhanced confidence may, at the recipients' discretion, cause a message to be delivered to recipient without further domain compliance assessment.

13.2. Risks to Recipients

TOC

The decisions that a recipient makes with regard to message filtering based on TPA-Label Resource Records is likely to depend on the system integrity of the Third Party with respect to Authentication (see Section 3.1.1 (Third Party Authentication)) and the provided scope labels. When the scope is not authenticated by the Third Party, there is a risk of accepting a potentially spoofed message.
With this specification, third party signatures now have some verifiable value. When implementing the compliance assessment of third

party signatures and TPA-Label Resource Records, implementers need to consider the possibility that a Bad Actor will send the recipient a message with a large number of valid DKIM Signatures. Verifying all of these may consume a large amount of processing resources and it may be worth checking the existence of a TPA-Label Resource Record first. Section 10 (TPA-Label Resource Record Query Transactions) describes a quick check to see if TPA-Label Resource Records may exist.
Additionally validating DKIM signatures and obtaining related resource records might be limited to known trustworthy domains.

13.3. Benefits to Author Domains

TOC

TPA-Label resource records can replace domain delegations, selector/key record mirroring, or key exchanges. Significant amounts of detail is associated with selector/key records. These details include user limitations, suitable services, key resource record's Time-To-Live, revocation and update procedures, and how the DKIM Signature header field's 'i=' semantics are to be applied. In addition, to better secure services that might depend upon DKIM keys, rather than delegating DKIM keys, the TPA-LLD scheme allows Author Domains an ability to limit the scope of their authorizations, without being mistaken for having authenticated the entity submitting the message, or for running ancillary services that may make use of DKIM public keys.
TPA-Label Resource Records convey which third-party domains are authoritative. However, third-party domains are unable to utilize DKIM signature's 'i=' semantics to directly assert which identifiers on whose behalf a signature was added. As such, no third-party domain should be authorized unless it is trusted to ensure the Alleged Author of an email undergoes some form authentication that offers acceptable protections for the Author Domain. Such authentication might be to ensure submitting entities have demonstrated receipt of "pingback" messages sent to the Author Address contained within the messages being signed, for example.
Author Domains benefit by deploying TPA-Label Resource Records in that a recipient who assesses signing practice compliance using the TPA-LLD scheme is less likely to drop messages from their domain. In addition, the authorized third party domains are less likely to need reputations for the recipient to validate the signature and assess the message for compliance with signing practices.
Scope labels provide a fine grained control that allows the Author Domain to limit message attributes even from the authorized third parties.
Signing domains having good reputations referenced by a TPA-LLD might therefore provide a means to safely extend limited compliance assessment resources to otherwise unknown Author Domains or SMTP Clients.

13.4. Risks to Author Domains

TOC

As indicated in Section 3.1 (Evaluating the Third-party Signing Domain), there is ultimately a trust of the third party domain to do the right thing and not generate or allow others to generate messages that appear to be from the Author Domain. The compliance assessment mechanisms deployed need to carefully match the scope of the TPA records.
By authorizing some mailing lists with TPA-Label Resource Records there could be a loss of confidentiality in respect to mailing list domain participation by the Author Domain. This might then help Bad Actors deduce which subscription email the Author Domain might receive.
Because of the hashing function in generating the TPA-label, anyone wishing to find out the authorized domains has to probe each TPA-label based on the exact signing domain.

13.5. Benefits to Third Party Signers

TOC

Third Party Signers benefit by having the autonomy to deploy and change DKIM signing without consultation with Author Domains. This is particularly useful for mailing lists.

13.6. Risks caused by Third Party Signers

TOC

Third Party Signers as mentioned before need to authenticate in some way messages from Author Domains. This authentication provides a safety mechanism for the Author Domain and the recipient. The Third Party may not be aware of the value of the authentication and change this without understanding the negative impact this may have on the author and recipient domains. The Third Party also may stop DKIM signing messages also causing a detriment to both author and recipient.

13.7. SHA-1 Collisions

TOC

The use of the SHA-1 hash algorithm does not represent a security concern. The hash simply ensures a deterministic domain-name size is achieved. Unexpected collisions can be detected and handled by using the extended TPA-Label Resource Record "tpa=" option. The use of TPA-

Label Resource Records without the TPA-Label "tpa=" options does present an opportunity for an adversary to attempt to find a hash collision. Message spoofing outside the realm of DKIM protection is still likely to be easier to achieve than finding hash collisions.

13.8. DNS Limits

TOC

Use of the TPA-Label Resource Records, rather than simply listing the authorized domain, ensures the DNS record size is independent of the Third Party Domain. The typical domain name size has been steadily increasing. This increase has been caused by domain names that encode international character sets, and perhaps soon an increase will be spurred by an expanse of TLDs having larger labels.
Using TPA-Label Resource Records in the DNS, as described by this scheme, leaves a residual size of 430 for the length of the author domain and the resource record content. DNS servers that add additional resource records, for nameservers as an example, will further limit this size. Author Domains exceeding this length will need to rely on the recipients using TCP for DNS retrieval or extended DNS lengths [RFC2671] (Vixie, P., “Extension Mechanisms for DNS (EDNS0),” August 1999.). Normally, DNS messages should not exceed 512 bytes as per Section 2.3.4 of [RFC1035] (Mockapetris, P., “Domain names - implementation and specification,” November 1987.).

14. Acknowledgements

TOC

Frank Ellermann, and Wietse Venema.

15. References

TOC

15.1. Normative References

TOC

[FIPS. 180-2.2002]	National Institute of Standards and Technology, “Secure Hash Standard,” FIPS PUB 180-2, August 2002.

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2919]	Chandhok, R. and G. Wenger, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists," RFC 2919, March 2001 (TXT).
[RFC4648]	Josefsson, S., "The Base16, Base32, and Base64 Data Encodings," RFC 4648, October 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).
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," STD 68, RFC 5234, January 2008 (TXT).
[RFC5321]	Klensin, J., "Simple Mail Transfer Protocol," RFC 5321, October 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).
[RFC5617]	Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)," RFC 5617, August 2009 (TXT).

15.2. Informative References

TOC

[I-D.ietf-dkim-deployment]	Hansen, T., Siegel, E., Hallam-Baker, P., and D. Crocker, "DomainKeys Identified Mail (DKIM) Development, Deployment and Operations," draft-ietf-dkim-deployment-11 (work in progress), January 2010 (TXT).
[RFC1035]	Mockapetris, P., "Domain names - implementation and specification," STD 13, RFC 1035, November 1987 (TXT).
[RFC2671]	Vixie, P., "Extension Mechanisms for DNS (EDNS0)," RFC 2671, August 1999 (TXT).
[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).
[RFC5226]	

	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 5226, May 2008 (TXT).
[RFC5672]	Crocker, D., “RFC 4871 DomainKeys Identified Mail (DKIM) Signatures -- Update,” RFC 5672, August 2009 (TXT).

Appendix A. DNS Example of TPA-Label Resource Record placement

TOC

```
####
# Practices for Example.com email domain using example.com, isp.com,
# and example.com.isp.com as signing domains.
####

#### 5322.From authorization for 3P domains ####

## "isp.com" TPA-Label Resource Record ##
_HTIE4SWL3L7G4TKAFAUA7UYJSS2BTEOV._adsp._domainkey.example.com. IN TXT
   "dkim=all; tpa=isp.com; scope=F;"

#### 5322.From/Originator/MailFrom authorization for 3P domains ####

## "example.com.isp.com" TPA-Label Resource Record ##
_6MEHLQLKWAL5HQREXWDN2TBXAJ6VZ44B._adsp._domainkey.example.com.  IN TXT
   "dkim=all; tpa=*.isp.com; scope=F:O:M;"
```

Appendix B. C code for label generation

TOC

The following utility can be compiled as tpa-label.c using the following:
gcc -lcrypto tpa-label.c -o tpa-label

```
/*
 * TPA-Label generation utility
 * Copyright (C) 2009 The IETF Trust & and the persons identified as
 * the document authors.  All rights reserved.
 * Redistributions of source code must retain the above copyright
 * notice and the following disclaimer.
 *
 * This document is subject to the rights, licenses and restrictions
 * contained in BCP 78, and except as set forth therein, the authors
 * retain all their rights.
 * This document and the information contained herein are provided on an
 * "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS
 * OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND
 * THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS
 * OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF
 * THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED
 * WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
 */

#include <stdio.h>
#include <sys/types.h>
#include <stddef.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <ctype.h>
#include <unistd.h>
#include <fcntl.h>
#include <errno.h>
#include <openssl/sha.h>

#define TPA_LABEL_VERSION   102
#define MAX_DOMAIN_NAME     256
#define MAX_FILE_NAME       1024

static char base32[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZ234567";
static char sign_on[] =
{"%s v%d.%02d Copyright (C) (2009)  The IETF Trust & Douglas Otis\n"};
char err_cmd[] =\
 "ERR: Command error with [%s]\n";
char use_txt[]=\
 "Usage: tpa-label [-i domain_input_file] [-o label_output_file][-v]\n";
char help_txt[]=\
"The options are as follows:\n"\
"-i  domain name input. Defaults to stdin. Removes trailing '.'\n"\
"-o  TPA-Label output.  Defaults to stdout.\n"\
"-v  Specifies Verbose Mode.\n\n";
```

```
static void usage(void);
/*- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */

static void
usage(void)
{
    (void) fprintf(stderr, "\n%s%s", use_txt, help_txt);
    exit(1);
}
/*- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */

int
main (int argc, char * argv[])
{
    int  ret_val, in_mode, out_mode, verbose, done, i, j, k;
    char ch;
    unsigned int len;
    unsigned long long b_5;
    char in_fn[MAX_FILE_NAME], out_fn[MAX_FILE_NAME];
    unsigned char in_buf[MAX_DOMAIN_NAME + 2];
    unsigned char sha_res[20], tpa_label[33];
    FILE *in_file, *out_file;

    ret_val = in_mode = out_mode = verbose = done = 0;
    len = 0;

    while ((ch = getopt(argc, argv, "i:o:v")) != -1)
    {
        switch (ch)
        {
            case 'i':
                in_mode = 1;          /* input from file */
                (void) strncpy(in_fn, optarg, sizeof(in_fn));
                in_fn[sizeof(in_fn) - 1] = '\0';
                break;
            case 'o':
                 out_mode = 1;         /* out to file */
                 (void) strncpy(out_fn, optarg, sizeof(out_fn));
                 out_fn[sizeof(out_fn) - 1] = '\0';
                 break;
            case 'v':
                 verbose = 1;
                 break;
            case '?':
            default:
                (void) usage();
                break;
        }
    };
```

```
if (in_mode)
{
    if ((in_file = fopen(in_fn, "r")) == NULL)
    {
        (void) fprintf(stderr,
                       "ERR: Error opening [%s] input file.\n",
                       in_fn);
        exit(2);
    }
}
else
{
    in_file = stdin;
}

if (out_mode)
{
    if ((out_file = fopen(out_fn, "w")) == NULL)
    {
        (void) fprintf(stderr,
                       "ERR: Error opening [%s] output file.\n",
                       out_fn);
        exit(3);
    }
}
else
{
    out_file = stdout;
}

if (out_mode && verbose)
{
    (void) printf(sign_on, "tpa-label utility",
                  TPA_LABEL_VERSION / 100,
                  TPA_LABEL_VERSION % 100);
}

for (i = 0; i < MAX_DOMAIN_NAME && !done; i++)
{
    if ((ch = fgetc(in_file)) == EOF)
    {
        ch = 0;
    }
    else  if (ch == '\n' || ch == '\r')
    {
        ch = 0;
    }
```

```
    in_buf[i] = tolower(ch);

    if (ch == 0)
    {
        len = i;         /* string length */
        done = 1;
    }
}

if (!done)
{
    (void) fprintf(stderr, "ERR: Domain name too long.\n");
    exit (4);
}

if (len && in_buf[len - 1] == '.')    /* remove any trailing "." */
{
    len--;
    in_buf[len] = 0;     /* replace trailing "." with 0 */
}

in_buf[len] = 0;         /* terminate string */

if (len < 2)
{
    (void)
    fprintf(stderr,
            "ERR: Domain name [%s] too short with %d length.\n",
            in_buf,
            len);
    exit (5);
}

SHA1(in_buf, len, sha_res);

if (verbose)
{
    printf("Normalized Domain = [%s] %d, SHA-1 = ", in_buf, len);

    for (i = 0; i < 20; i++)
    {
        printf("%02x", sha_res[i]);
    }
    printf("\nTPA-Label: 5 bit intervals left to right.\n");
}

/* process sha-1 results 4 times by 40 bits (0 to 160) */

for (i = 0, j = 0; i < 4 ; i++)
{
```

```
    b_5 =  (unsigned long long) sha_res[(i * 5)] << 32;
    b_5 |= (unsigned long long) sha_res[(i * 5) + 1] << 24;
    b_5 |= (unsigned long long) sha_res[(i * 5) + 2] << 16;
    b_5 |= (unsigned long long) sha_res[(i * 5) + 3] << 8;
    b_5 |= (unsigned long long) sha_res[(i * 5) + 4];

    if (verbose)
    {
        printf(" {%010llX}->", b_5);
    }

    for (k = 35; k >= 0; k-= 5, j++)    /* convert 40 bits (5x8) */
    {
        tpa_label[j] = base32[(b_5 >> k) & 0x1F];

        if (verbose)
        {
             printf(" %02X:%c",
                    (unsigned int)(b_5 >> k) & 0x1F,
                    tpa_label[j]);
        }
    }
    if (verbose)
    {
        printf ("\n");
    }
}
if (verbose)
{
    printf("\n");
}

tpa_label[j] = 0;   /* terminate label string */
fprintf(out_file, "_%s", tpa_label);
printf("\n");

/* close */
if (out_mode)
{
    if (fclose (out_file) != 0)
    {
        (void) fprintf(stderr,
                       "ERR: Unable to close %s output file.\n",
                       out_fn);
        ret_val = 6;
    }
}
if (in_mode)
{
```

```
            if (fclose (in_file) != 0)
            {
                (void) fprintf(stderr,
                               "ERR: Unable to close %s input file.\n",
                               in_fn);
                 ret_val = 7;
            }
        }
        return (ret_val);
    }
```

Authors' Addresses

TOC

	Douglas Otis
	Trend Micro
	10101 N. De Anza Blvd
	Cupertino, CA 95014
	USA
Phone:	+1.408.257-1500
Email:	doug_otis@trendmicro.com
	Daniel Black
	Canberra ACT
	Australia
Email:	daniel.subs@internode.on.net