DMARC Working Group
Internet-Draft
Intended status: Informational
Expires: September 21, 2015

F. Martin, Ed.
LinkedIn
E. Lear, Ed.
Cisco Systems GmbH
T. Draegen, Ed.
Eudaemon
E. Zwicky, Ed.
Yahoo

March 20, 2015

Interoperability Issues Between DMARC and Indirect Email Flows
draft-ietf-dmarc-interoperability-01

Abstract

DMARC introduces a mechanism for expressing domain-level policies and preferences for email message validation, disposition, and reporting. The DMARC mechanism can encounter interoperability issues when messages originate from third party sources, are modified in transit, or are forwarded enroute to their final destination. Collectively these email flows are referred to as indirect email flows. This document describes interoperability issues between DMARC and indirect email flows. Possible methods for addressing interoperability issues are presented.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 21, 2015.

Copyright Notice

Table of Contents

1. Introduction

DMARC [RFC7489] introduces a mechanism for expressing domain-level policies and preferences for message validation, disposition, and reporting. DMARC is used to combat exact-domain phishing, to gain visibility into email infrastructure, and to provide email egress controls. Due to wide adoption, the impact of DMARC-based email rejection policies on both direct and indirect email flows can be significant.

The DMARC mechanism can encounter several different types of interoperability issues due to third-party message sourcing, message transformation or rerouting. These cases in which mail does not go directly from the author's administrative domain to the recipients are known collectively as indirect email flows.

The next section describes interoperability issues between DMARC and indirect email flows. These issues are first described in the context of configuration behavior that DMARC requires from underlying authentication technology, and then described as they appear in context of the Internet Mail Architecture [RFC5598].

Lastly, possible methods for addressing interoperability issues are presented. There are often multiple ways to address any given interoperability issue. While this document strives to be comprehensive in its review, it should not be treated as complete.

1.1. Document Conventions

Notation regarding structured fields is taken from [RFC5598].

Organizational Domain and Authenticated Identifiers are specified in DMARC [RFC7489].

2. Causes of Interoperability Issues

What do we mean by "interoperability issues"? We say that DMARC introduces interoperability issues or problems, when conformance to the DMARC specification leads an implementation to reject a message that is both compliant with the architecture as specified in [RFC5598] and would have been viewed as legitimate in the eyes of the

intended recipient. Therefore, we can already conclude that DMARC poses no interoperability problems when legitimate messages properly validate through its specified processes. The rest of this section delves into how legitimate messages may get rejected.

2.1. Identifier Alignment

A fundamental aspect of message source validation is understanding what defines the source that is validated. Each of the underlying mechanisms that DMARC uses (DKIM [RFC6376] and SPF [RFC7208]) takes a different approach. Therefore, the DMARC [RFC7489] mechanism attempts to predictably specify the domain of the originator that will be used for its purposes (reporting/message disposition). This step is referred to as Identifier Alignment.

DKIM provides a cryptographic means for a domain to be associated with a particular message. DKIM does not make any constraints on what domains may or must present this association. However, for a DKIM identifier to align in DMARC, the signing domain must be part of the same Organizational Domain as the domain in the RFC5322.From header field [RFC5322], and the signature must be valid.

In addition, DKIM allows for the possibility of multiple valid signatures. The DMARC mechanism will process Authenticated Identifiers that are based on DKIM signatures until an aligned Authenticated Identifier is found (if any). However, operational experience has shown that some implementations have difficulty processing multiple signatures. The impact on DMARC processing is clear: if an implementation cannot process multiple DKIM signatures it may lead to perfectly valid messages being flagged as not authentic.

SPF provides two Authenticated Identifiers the first one is RFC7208.HELO [RFC7208] based on RFC5321.HELO/EHLO and the second one is RFC7208.MAILFROM [RFC7208] based on the RFC5321.MailFrom [RFC5321] domain or, if the RFC5321.MailFrom address is absent (as in the case of "bounces"), on the domain found in the HELO/EHLO SMTP command. Local policies, as well as DMARC often only use the RFC7208.MAILFROM identifier. Again, for an SPF identifier to align in DMARC, the validated domain must be part of the same Organizational Domain as the domain in the RFC5322.From header field. Even when an SPF record exists for the domain in RFC5322.From, SPF will not authenticate it unless it is also the domain SPF checks. While aligning RFC5322.From and RFC5321.MailFrom is usually possible, it can be difficult to change the domain in the HELO/EHLO used for bounces to the domain in the RFC5322.From header field, especially when several mail streams share the same sending IP address.

2.2. Message Forwarding

Message forwarding is a generic concept encapsulating a variety of behaviors. Section 3 describes forwarding behavior as it relates to the components of the Internet Mail Architecture.

All of these behaviors involve mail being retransmitted by a new SMTP server. As discussed above, for SPF to cause a DMARC pass, the domain of the RFC5321.MailFrom or RFC5321.HELO/EHLO must be aligned with that of the RFC5322.From header field. If the forwarder keeps the RFC5321.MailFrom, the SPF validation will fail altogether unless the forwarder is an authorized part of the originator's mail sending infrastructure. If the forwarder uses its own domain in the RFC5321.MailFrom and/or RFC5321.HELO/EHLO, SPF passes but the alignment with the RFC5322.From header field fails. In either case, SPF cannot produce a DMARC pass, and DKIM will be required to get DMARC to pass.

2.3. Message Modification

Modification of email content invalidates most DKIM signatures. For instance while DKIM provides a length flag so that content can be appended (See Section 8.2 of RFC6376 [RFC6376] for additional security considerations), in practice, particularly with MIME-encoded [RFC2045] messages, a mailing list processor will do more than append (See Section 5.3 of [RFC5598] for details). Even forwarding systems make content modifications. Furthermore, the use of the length flag is by no means universal.

DKIM has two canonicalizations: simple and relaxed. The latter allows some modest in transit modifications that do not change the interpretation of the content of the email. The relaxed canonicalization used to be computing intensive and may not have been preferred in the early deployment of DKIM.

3. Internet Mail Architecture, DMARC, and Indirect Email Flows

This section describes components within the Internet Mail Architecture [RFC5598] where interoperability issues between DMARC and indirect email flows can be found.

3.1. Message Handling System

Section 4 of [RFC5598] describes six basic components that make up the Message Handling System (MHS):

- Message

- Message User Agent (MUA)
- Message Submission Agent (MSA)
- Message Transfer Agent (MTA)
- Message Delivery Agent (MDA)
- Message Store (MS)

Of these components MSA, MTA, and MDA are discussed in relation to interoperability with DMARC.

A Mediator is a special class of MUA that is given special consideration in this section due to the unique issues Mediators face when attempting to interoperate with DMARC.

3.1.1. Message Submission Agents

An MSA accepts messages submitted by a Message User Agent (MUA) and enforces the policies of the hosting ADministrative Management Domain (ADMD) and the requirements of Internet standards.

MSAs are split into two sub-components:

- Author-focused MSA functions (aMSA)
- MHS-focused MSA functions (hMSA)

MSA interoperability issues with DMARC begin when an aMSA accepts a message where the RFC5322.From header field contains a domain that is outside of the ADMD of the MSA. The ADMD will almost certainly not be capable of sending email that yields Authenticated Identifiers aligned with the domain found in the RFC5322.From header field. Examples of this issue include "forward-to-friend" functionality commonly found on news/article websites or "send-as" functionality present on some MUAs.

When an hMSA takes responsibility for transit of a message containing a domain in the RFC5322.From header field that is outside of the hMSA's ADMD, the hMSA faces DMARC interoperability issues if the domain publishes a DMARC policy of "quarantine" or "reject". These issues are marked by an inherent difficulty in modifying the domain present in a message's RFC5322.From header field. Examples of this issue include:

- Pseudo-open relays - a residential ISP that allows its customers to relay any domains through its infrastructure.

- Embedded devices - cable/dsl modems, firewalls, wireless access points that send email using hardcoded domains.

- Email service providers - ESPs that service customers that are using domains that publish a DMARC "reject" policy.

- Calendaring software - an invited member of an event modifies the event causing calendaring software to emit an update that appears to come from the creator of the event.

3.1.2. Message Transfer Agents

MTAs relay a message until the message reaches a destination MDA.

3.1.2.1. Message Encoding

An MTA may change the message encoding, for instance by converting 8-bit mail sections to quoted-printable 7-bit sections. This is outside the scope of DKIM canonicalization and will invalidate DKIM signatures that include message content.

3.1.2.2. Header Standardization

An MTA may standardize headers, usually in order to make non-RFC compliant headers properly compliant. For instance, some common MTAs will correct comprehensible but non-compliant date formats to compliant ones. Again, this is outside the scope of DKIM canonicalization and will invalidate DKIM signatures.

3.1.2.3. Email Address Internationalization

A DMARC interoperability issue arises in the context of Email Address Internationalization [RFC6530]. [RFC6854] allows group syntax in the RFC5322.From header field during the transition period to SMTPUTF8. If an EAI/SMTPUTF8-aware MTA needs to transmit a message to a non-aware MTA, the EAI/SMTPUTF8-aware system may transform the RFC5322.From header field of the message to include group syntax to allow the non-aware MTA to receive the email.

This transformation will modify the original content of the message and may invalidate any DKIM signatures if the transformation is not done by the MSA or MUA. In addition, group syntax will remove the ability for the DMARC mechanism to find an Organizational Domain that aligns with any authenticated domain identifier from SPF or DKIM.

In addition, the group syntax will result in an invalid domain in the RFC5322.From header field. If the receiving MTA pays attention to

the validity and reputation of domains, this may present its own set of delivery problems.

3.1.3. Message Delivery Agents

The MDA transfers a message from the MHS to a mailbox. Like the MSA, the MDA consists of two sub-components:

- MHS-focused MDA functions (hMDA)
- Recipient-focused MDA functions (rMDA)

Both the hMDA and the rMDA can redirect a message to an alternative address. DMARC interoperability issues related to redirecting of messages are described in Section 3.2.

SIEVE [RFC5228] functionality often lives in the rMDA sub-component and can cause DMARC interoperability issues. The SIEVE 'addheader' and 'deleteheader' filtering actions can modify messages and invalidate DKIM signatures, removing DKIM-supplied Authenticated Identifiers as inputs to the DMARC mechanism. There are also SIEVE extensions that modify the body. SIEVE may become an issue when the email is reintroduced in the transport infrastructure.

3.2. Mediators

See [RFC5598] for a complete definition of Mediators.

Mediators forward messages through a re-posting process. Mediators share some functionality with basic MTA relaying, but have greater flexibility in both addressing and content modifications.

DMARC interoperability issues are prevalent within the context of Mediators, which are often used precisely for their ability to modify messages.

3.2.1. Alias

An Alias is a simple re-addressing facility that provides one or more new Internet Mail addresses, rather than a single, internal one. A message continues through the transfer service for delivery to one or more alternative addresses.

Aliases can be implemented by mailbox-level forwarding (e.g. through "dot-forwarding") or SIEVE-level forwarding (through the SIEVE 'redirect' action) or other methods. When an Alias preserves message content and does not make significant header changes, DKIM signatures

may remain valid. However, Aliases often extend the delivery path beyond SPF's ability to grant authorization.

Examples of Aliasing include:

- Forwarding email between freemail providers to try different interfaces while maintaining an original email address.
- Consolidating many email addresses into a single acccount to centralize processing.
- Services that provides "activity based", "role based" , "vanity" or "temporary" email addresses such as universities and professional associations. For instance professional or alumni institutions may offer to their members an alias for the duration of their membership but may not want to deal with the long term storage of emails.

In most cases, the aMSA providing Alias services has no administrative relationship to the ADMD of the final recipient, so solutions to Alias-related DMARC failure should not assume such a relationship.

3.2.2. ReSenders

ReSenders "splice" a message's addressing information to connect the Author of the original message with the Recipient of the new message. The new Recipient sees the message as being from the original Author, even if the Mediator adds commentary.

ReSenders introduce DMARC interoperability issues as content modification invalidates DKIM signatures. SPF's ability to grant authorization via alignment is removed as the new Recipient receives the message from the Mediator.

Without an ability to produce Authenticated Identifiers relevant to the Author's RFC5322.From header field domain using either DKIM or SPF, the new Recipient has almost no chance of successfully applying the DMARC mechanism.

Examples of ReSenders include MUA-level forwarding by resending a message to a new recipient or by forwarding a message "inline" to a new recipient (this does not include forwarding a message "as an attachment"). An additional example comes in the form of calendaring software that allows a meeting attendee (not the meeting organizer) to modify the content of an invite causing the invitations to appear to be reissued from the meeting organizer.

3.2.3. Mailing Lists

A Mailing List receives messages as an explicit addressee and then re-posts them to a list of subscribed members. The Mailing List performs a task that can be viewed as an elaboration of the ReSender.

Mailing Lists share the same DMARC interoperability issues as ReSenders (Section 3.2.2), and very commonly modify headers or message content in ways that will cause DKIM to fail, including:

- prepending the RFC5322.Subject header field with a tag, to allow the receiver to identify visually the mailing list.
- adding a footer to the email body to contain administrative instructions.
- removing some MIME-parts from the email or converting the message to text only.
- PGP-encrypting the body to the receiver's key.
- enforcing community standards by rewriting banned words.
- allowing moderators to add arbitrary commentary to messages.

Any such modifications would invalidate a DKIM signature.

Mailing Lists may also have the following DMARC interoperability issues:

- Subscribed members may not receive email from members that post using domains that publish a DMARC "p=reject" policy.
- Mailing Lists may interpret DMARC-related email rejection as an inability to deliver email to the recipients that are checking and enforcing DMARC policy. This processing may cause subscribed members to be suspended or removed from the Mailing List. [RFC3463] specifies Enhanced Mail System Status Codes which help differentiate between various bounces. DMARC even defines specific codes to be used.

3.2.4. Gateways

A Gateway performs the basic routing and transfer work of message relaying, but it also is permitted to modify content, structure, address, or attributes as needed to send the message into a messaging environment that operates under different standards or potentially incompatible policies.

Gateways share the same DMARC interoperability issues as ReSenders (Section 3.2.2).

Gateways may share also the same DMARC interoperability issues as MTAs (Section 3.1.2).

Gateway-level forwarding can introduce DMARC interoperability issues if the Gateway is configured to rewrite the message to map between recipient domains. For example, an acquisition may lead the acquiring company to decide to decommission the acquired companies domains by rewriting messages to use the domain of the acquiring company. Since the To: header is usually DKIM-signed, this kind of rewriting will also cause DKIM signatures to fail.

3.2.5. Boundary Filters

To enforce security boundaries, organizations can subject messages to analysis for conformance with their safety policies. A filter might alter the content to render it safe, such as by removing content deemed unacceptable.

Boundary Filters share the same DMARC interoperability issues as ReSenders.

Examples of Boundary Filters include:

- Anti-spam: To keep its reputation, an MTA that transfers a message may remove harmful content from messages that are likely to be unwanted by the next MTA and/or add text in the body to indicate the message has been scanned. Any such modifications would invalidate a DKIM signature.

- Any service that reformulates the RFC5322.body for any other reason, for instance adding an organizational disclaimer.

- Secondary MX services. In this case, however, it is inappropriate for a primary MX server to perform an SPF check against its own secondaries. Rather, the secondary MX should perform this function.

3.3. Combinations

The causes of indirect email flows can be combined. For example, a university student may subscribe to a mailing list (using his university email address) while this university email address is configured to forward all emails to a freemail provider where a more permanent email address for this student exists.

Within an organization the message may pass through various MTAs (Section 3.1.2), each of which performs a different function (authentication, filtering, distribution, etc.)

4. Possible Solutions to Interoperability Issues

Solutions to interoperability issues between DMARC and indirect email flows vary widely in their scope and implications. They range from improvements to underlying processors, such as proper handling multiple DKIM signatures, to more radical approaches to the messaging architecture. This section describes possible ways to address interoperability issues.

Mail systems are diverse and widely deployed and are expected to continue to work with old systems. For instance, Qmail is still used and the base code has not been updated since 1998. Ezmlm, a once popular mailing list manager, is still deployed and has not been updated since 1997, although a new version, Ezmlm-idx exists. In this constrained environment, some solutions may be time-consuming and/or disruptive to implement.

DMARC provides for receivers to make decisions about identity alignment acceptability based on information outside the DMARC headers and communicate those decisions as "overrides" to the sender. This facility can be used to ease some interoperability issues, although care is needed to ensure that this does not create loopholes that abusers can use arbitrarily.

4.1. Identifier Alignment

Currently used work-arounds and fixes to identifier alignment issues:

- MTAs handling multiple domains may choose to change RFC5321.MailFrom to align with RFC5322.From to improve SPF usability for DMARC.

- MTAs handling multiple domains may also choose to align HELO/EHLO to RFC5322.From, particularly when sending bounce messages.

- MTAs may choose to DKIM sign bounces to allow DKIM-based DMARC pass.

- MTAs handling multiple domains may require DMARC-using senders to provide DKIM keys and use DKIM to avoid SPF alignment issues.

- ReSenders may choose to change RFC5322.From to one under the ReSender's control, avoiding alignment issues with the original.

- Receivers should update DKIM handling libraries to ensure that they process all valid DKIM signatures and check them for alignment.

Proposed and in-progress work-arounds and fixes to identifier alignment issues:

- Third party authorization, [RFC6541], [I-D.otis-tpa-label] and [I-D.kucherawy-dkim-delegate] provide ways to extend identifier alignment under the control of the domain owner.

4.2. Message Modification

Message modification invalidates DKIM signatures and complicates a receiver's ability to generate Authenticated Identifiers from a message. Avoiding message modification wherever possible is therefore desirable.

Currently used work-arounds and fixes to message modification issues:

- Senders can maximize survivability of DKIM signatures by limiting the header fields they sign, using relaxed canonicalization and by using length to allow appended signatures.

- Senders can also maximize survivability by starting with RFC-compliant headers and common body formats.

- Forwarders can choose to add email headers instead of modifying existing headers or bodies.

- Forwarders can minimize the circumstances in which they choose to fix messages, preferring preserving non-compliant headers to creating DKIM failures.

- Forwarders can choose to reject messages with suspect or harmful content instead of modifying them.

- If message modification is required, the RFC5322.From may be changed.

Proposed and in-progress work-arounds and fixes to message modification issues:

- DKIM with constrained transformations, [I-D.kucherawy-dkim-list-canon]

4.3. Message Forwarding

Forwarding messages without modification is referred to as "transparent forwarding", and is a way to preserve the validity of DKIM signatures.

Currently used work-arounds and fixes to message forwarding issues:

- Senders should use DKIM signing to allow transparent forwarding to succeed.
- ReSenders may choose to change RFC5322.From to one under the ReSender's control, avoiding alignment issues with the original.

The Original-From [RFC5703] (or X-Original-From) header is used in various contexts (X- header fields name are discouraged by [RFC6648]).

Note that Original-From (or X-Original-From) is merely adding complexity to the 'who was the author of this message' assessment, very possibly creating yet-another security hole.

4.3.1. Original-Authentication-Results

[I-D.kucherawy-original-authres] has been mentioned in early DMARC drafts as a way to pass along Original Authentication Results to "downstream" receivers.

4.4. Message Handling Services

4.4.1. Message Transfer Agents

4.4.1.1. Encoding

There are few reasons to modify the encoding of the message, compatibility issues between international character sets are few nowadays. More mail systems supports 8bitMIME, therefore the need for transport encoding changes are rarer. By default no modification of the message should be done when simply forwarding the message.

4.4.1.2. Filters

Filters should not add to or modify the body of the message, but either should reject the message or add new email headers (not under DKIM) to indicate the result of the filter.

4.4.1.3. Email Address Internationalization

During the transition from email systems that do not allow EAI (SMTPUTF8) to email system that allows it, [RFC6854] allows using the group syntax for the RFC5322.From header field rather than rejecting the message (if RFC5322 is implemented strictly). Allowing the group syntax is at the appreciation of the postmaster, that will always choose the solution best for its user, but really to avoid DMARC not finding a single useable domain in the RFC5322.From header field, the real solution is to upgrade your MTAs, to support EAI (SMTPUTF8). In that case a sending SMTPUTF8 MTA does not need to require a downgrade of the message to ASCII identifiers. Encouraging, by rejection or reputation scoring, the presence of a domain in the RFC5322.From header field is easier.

4.5. Mediators

4.5.1. Mailing Lists

[RFC6377] provides some guidance on using DKIM with Mailing lists. Here are some other remediations techniques:

- One common mitigation policy is to configure the Mailing List Manager (MLM) to alter the RFC5322.From header field to use the domain of the MLM. Since most list subscribers prefer to know the identity of the author of the original message, typically this information may be provided in the display name part of the RFC5322.From header field. This display name needs to be carefully crafted as to not collide with the original display name of the author, nor contain something that looks like an email address or domain name. These modification may to some extent defeats the purpose of DMARC itself. It may make it difficult to ensure that users of all email clients can easily reply to author, list, or all using the email client features provided for that purpose. Use of "Reply-To" can alleviate this problem depending if the mailing list is configured to reply-to-list, reply-to-author or reply-to-fixed-address.

- Another common mitigation policy is to configure the MLM to "wrap" the message in a MIME message/rfc822 part. This completely bypasses the DMARC policy in clients that allow reading the part as a message. Many email clients (as of August 2014) have difficulty reading such messages.

- Finally a less common mitigation policy, is to configure the MLM to not modify the message so that the DKIM signature remains valid.

- To alleviate unsubscribes to the mailing list due to the messages bouncing because of DMARC, the MLM needs to not act on bounces due to Message Authentication issues. Correctly interpreting Extended SMTP error messages is useful in this case ([RFC7372]).

All these techniques may provide some specific challenges in MUAs and different operational usages for end users (like rewriting filters to sort emails in folders). There will be some time before all implications are understood and alleviated.

4.6. Getting More Radical: Requiring New Communication Paths Between MUA and the Message Store

In practice a number of operators are using strict alignement mode in DMARC in order to avoid receiving new and innovative forms of unwanted and unauthentic mail through systems purporting to be mailing list handlers. The receiving ADMD has no knowledge of which lists the user has subscribed to and which they have not. One avenue of exploration would be for the user to authorize mailing lists as proxies for authentication, at which point the receiving ADMD would be vesting some trust in the mailing list service. The creators of DKIM foresaw precisely this possibility at the time by not tightly binding any semantics to the RFC5322.From header field. Some experimental work has taken place in this area, as mentioned above. Additional work might examine a new communication path to the user to authorize third party signatures.

5. IANA Considerations

This document contains no actions for IANA. [RFC Editor: Please delete this section prior to publication.]

6. Security Considerations

This document is an analysis of DMARC's impact on indirect email flows. It describes the possibility of accidental denial-of-service that can be created by rejections of messages by DMARC-aware Mail Receivers. However, it introduces no new security issues to Internet messaging.

7. Acknowledgments

Miles Fidelman, John Levine, David Crocker, Stephen J. Turnbull, Rolf E. Sonneveld, Tim Dragen and Franck Martin contributed to the IETF DMARC Working Group's wiki page listing all known interoperability issues with DMARC and indirect mail flows.

Tim Draegen created the first draft of this document from these contributions and by carefully mapping contributions into the language of [RFC5598].

8. References

8.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, January 2003.

[RFC5228] Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language", RFC 5228, January 2008.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

[RFC5703] Hansen, T. and C. Daboo, "Sieve Email Filtering: MIME Part Tests, Iteration, Extraction, Replacement, and Enclosure", RFC 5703, October 2009.

[RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, September 2011.

[RFC6377] Kucherawy, M., "DomainKeys Identified Mail (DKIM) and Mailing Lists", BCP 167, RFC 6377, September 2011.

[RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, February 2012.

[RFC6541] Kucherawy, M., "DomainKeys Identified Mail (DKIM) Authorized Third-Party Signatures", RFC 6541, February 2012.

[RFC6648] Saint-Andre, P., Crocker, D., and M. Nottingham, "Deprecating the "X-" Prefix and Similar Constructs in Application Protocols", BCP 178, RFC 6648, June 2012.

[RFC6854] Leiba, B., "Update to Internet Message Format to Allow Group Syntax in the "From:" and "Sender:" Header Fields", RFC 6854, March 2013.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, April 2014.

[RFC7372] Kucherawy, M., "Email Authentication Status Codes", RFC 7372, September 2014.

8.2. Informative References

[I-D.kucherawy-dkim-delegate]
Kucherawy, M. and D. Crocker, "Delegating DKIM Signing Authority", draft-kucherawy-dkim-delegate-01 (work in progress), June 2014.

[I-D.kucherawy-dkim-list-canon]
Kucherawy, M., "A List-safe Canonicalization for DomainKeys Identified Mail (DKIM)", draft-kucherawy-dkim-list-canon-00 (work in progress), June 2014.

[I-D.kucherawy-original-authres]
Chew, M. and M. Kucherawy, "Original-Authentication-Results Header Field", draft-kucherawy-original-authres-00 (work in progress), February 2012.

[I-D.levine-dkim-conditional]
Levine, J., "DKIM Conditional Signatures", draft-levine-dkim-conditional-00 (work in progress), June 2014.

[I-D.otis-tpa-label]
Otis, D. and D. Black, "Third-Party Authorization Label", draft-otis-tpa-label-00 (work in progress), May 2014.

[RFC7489] Kucherawy, M. and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, March 2015.

Authors' Addresses

Franck Martin (editor)
LinkedIn
Mountain View, CA
USA

Email: fmartin@linkedin.com

Eliot Lear (editor)
Cisco Systems GmbH
Richtistrasse 7
Wallisellen, ZH CH-8304
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com

Tim Draegen (editor)
Eudaemon
NC
USA

Email: tim@eudaemon.net

Elizabeth Zwicky (editor)
Yahoo
Sunnyvale, CA
USA

Email: zwicky@yahoo-inc.com