DMARC Working Group
Internet-Draft
Intended status: Informational
Expires: December 11, 2015

F. Martin, Ed.
LinkedIn
E. Lear, Ed.
Cisco Systems GmbH
T. Draegen, Ed.
Eudaemonic Development LLC
E. Zwicky, Ed.
Yahoo

June 9, 2015

Interoperability Issues Between DMARC and Indirect Email Flows
draft-ietf-dmarc-interoperability-04

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 do not flow directly from the author's administrative domain to the final recipients. 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 December 11, 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. The DMARC mechanism can encounter several different types of interoperability issues due to third-party message sourcing, message transformation or rerouting.

DMARC is, as this writing, an Informational RFC, however it has a significant deployment within the email community.

Cases in which email does not flow directly from the author's administrative domain to the recipients are collectively referred to in this document as indirect email flows. Due to existing and increasing adoption of DMARC, the impact of DMARC-based email rejection policies on both direct and indirect email flows can be significant.

Several known causes of interoperability issues are presented, followed by a description of components within the Internet Mail Architecture [RFC5598] where interoperability issues can arise.

Lastly, known and 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

Interoperability issues between DMARC and indirect email flows arise when conformance to the DMARC specification leads an implementation to apply DMARC based policy to messages that are both compliant with the architecture as specified in [RFC5598] and viewed as legitimate

by the intended recipient. To be clear, this document does not address emails considered legitimate by the intended recipient but which are not conformant to other email specifications. The rest of this section describes several conceptual causes of interoperability issues.

2.1. Originator vs Receiver Perspective

Some Receivers are concerned that wanted email messages are received, regardless if such email messages are not strictly in conformance to any standard or protocol.

Some Originators, particularly for high value transactional messages, want the message discarded if it passes through an intermediary and is modified in any way resulting in a failure to validate. Examples of such messages include those related to financial organizations and medical establishments.

2.2. Identifier Alignment

DMARC relies on DKIM [RFC6376] and SPF [RFC7208] to perform message source validation. The DMARC [RFC7489] mechanism refers to source domains that are validated by DKIM or SPF as Authenticated Identifiers. DMARC requires an Authenticated Identifier to be relevant to the domain found in the message's RFC5322.From header field [RFC5322]. This relevancy is referred to as Identifier Alignment.

Identifier Alignment can be strict, where the domains exactly match each others, or relaxed where the domains are part of the same Organizational Domain. There are, in general, the same interoperability issues between strict and relaxed alignment, however in strict mode the possible solutions are more constrained when possible. This Document mainly implies relaxed 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 of a valid signature must be part of the same Organizational Domain as the domain in the RFC5322.From header field [RFC5322].

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: implementations that cannot process multiple DKIM signatures may erroneously apply DMARC based policy to otherwise legitimate messages.

SPF can provide two Authenticated Identifiers based on two different SPF identities: RFC7208.HELO [RFC7208] and RFC7208.MAILFROM [RFC7208]. DMARC uses only the RFC7208.MAILFROM identifier for alignment. The SPF validated domain in RFC7208.MAILFROM must be part of the same Organizational Domain as the domain in the RFC5322.From header field to be aligned. It is important to note that even when an SPF record exists for the domain in RFC5322.From, SPF will not authenticate it unless it is also the domain in RFC7208.MAILFROM, furthermore, RFC7208.MAILFROM definition is different from RFC5321.MailFrom [RFC5321] definition.

2.3. 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 email being retransmitted by a new SMTP server. As discussed above, for SPF to cause a DMARC pass, the domain of the RFC7208.MAILFROM, must be aligned with that of the RFC5322.From header field:

- If the RFC5321.MailFrom is not empty and if the forwarder keeps the RFC5321.MailFrom, the SPF validation will fail altogether unless the forwarder is an authorized part of the originator's email sending infrastructure. On another hand, if the forwarder uses its own domain in the RFC5321.MailFrom, SPF passes but the alignment with the RFC5322.From header field fails.

- If the RFC5321.MailFrom is empty, the RFC5321.Helo of the forwarder will likely be in different organizational domain of the RFC5322.From. SPF may pass 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.

2.4. Message Modification

Modification of email content invalidates most DKIM signatures, and many message forwarding systems modify email content. Mailing list processors are the most common example of such systems, but other forwarding systems also make modifications. Although DKIM provides a length flag so that content can be appended (See Section 8.2 of

[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). Furthermore, the use of the length flag is seldom found in emails in part because of its security challenges.

DKIM has two canonicalizations to use for headers and body separately: 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 is more computing intensive and may not have been preferred in the early deployment of DKIM as this may have been more significant than today.

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 establishing alignment with 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 modify the message encoding, for instance by converting 8-bit MIME sections to quoted-printable 7-bit sections. This modification 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. This correction is outside the scope of DKIM canonicalization and will invalidate DKIM signatures. This correction is also outside the scope of this document in providing solutions for non RFC compliant emails.

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 only 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(s) 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 or S/MIME 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.

These changes are common for many mailing lists and receivers are used to them. Furthermore MUA expects certain mailing list behavior in presenting emails to the end users

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 company's domains by rewriting messages to use the domain of the acquiring company. Since the RFC5322.To header field 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.

Issues may arise if SPF and DKIM is evaluated after the filter modifications.

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 Mitigations of 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 of 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 DMARC 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. Mitigations in Current Use

At many places where DMARC is already deployed, mitigations are in use. These mitigations vary in their effectiveness and side effects, but have the advantage that they are currently available.

4.1.1. Mitigations for Senders

4.1.1.1. Identifier Alignment

- 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 RFC5321.HELO/EHLO to RFC5322.From, particularly when sending bounce messages. Adjusting dynamically the RFC5321.HELO based on the RFC5322.From may not be possible for some MTA software.

- MTAs may choose to DKIM sign bounces with an aligned domain 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. Handling DKIM keys with a third party has its security challenges.

- Senders who are sending on behalf of users in other Administrative Domains may choose to use an RFC5322.From under the sender's control. The new From can be either a forwarding address in a domain controlled by the Sender, or a placeholder address, with the original user's address in a RFC5322.Reply-to header field. However this may affect what the recipient expects in its MUA.

- Senders can use different domains with different DMARC policies for email sent directly and email known to use indirect mail flow. However for known brands, all active domains are likely to be targeted equally by abusers.

4.1.1.2. Message Modification

- 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.

- In order to minimize the chances of transport conversions, Senders can convert the message to a suitable MIME content-transfer encoding such as quoted-printable or base64 before signing ([RFC6376] Section 5.3).

4.1.2. Mitigations for Receivers

4.1.2.1. Identifier Alignment

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

4.1.2.2. Policy Override

- Receivers can amalgamate data from their user base to identify forwarders and use such list for a DMARC local policy override. This process may be easier for large receivers, where there is data and resources to create such lists, than for small receivers.

4.1.3. Mitigations for ReSenders

4.1.3.1. Changes to the RFC5322.From

Many ReSender issues can be avoided by using an RFC5322.From header field under the ReSender's control, instead of the initial RFC5322.From. This will correct identifier alignment issues and allow arbitrary message modification, for instance. When ReSenders change the RFC5322.From, it is desirable to preserve the information about the original initiator of the message.

A first option is to use the Original-From [RFC5703] (or X-Original-From) header field for this purpose in various contexts (X- header fields name are discouraged by [RFC6648]). However, handling of Original-From (or X-Original-From) is not defined anywhere. It is not currently used consistently or displayed to the user, but in any situation where it is used, it is a new unauthenticated identifier available for exploitation.

Another option for ReSenders is to rewrite the RFC5322.From header field address to a valid forwarding address to the original sender, in a domain that the ReSender controls.

4.1.3.2. Avoiding Message Modification

- Forwarders can choose to add email header fields instead of modifying existing headers or bodies, for instance to indicate a message may be spam.

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

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

4.1.3.3. Mailing Lists

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

- One mitigation policy, which is now present on several Mailing List software, 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 modifications may to some extent defeat the purpose of DMARC itself. It may make it difficult to ensure that users of all email clients can easily reply to the author, the list, or all using the email client features provided for that purpose. Use of RFC5322.Reply-To header field can alleviate this problem depending on whether the mailing list is configured to reply-to-list, reply-to-author or reply-to-fixed-address, however it is important to note that this header field can take multiple email addresses. When altering the RFC5322.From there are two possibilities, to change it to put the mailing list email address, or to change it to add a suffix like ".invalid" to the domain of the email address present there. The later modification may create issues because it is an invalid domain name, and some MTAs may take particular attention to the validity of email addresses in RFC5322.From and the reputation of the domains present there.

- Another mitigation policy is to configure the MLM to "wrap" the message in a MIME message/rfc822 part and to send as the Mailing List email address. Many email clients (as of August 2014) have difficulty reading such messages.

- Another mitigation policy, is to configure the MLM to not modify the message so that the DKIM signature remains valid. Some Mailing Lists are mainly setup this way and require little modifications to ensure the DKIM signature is preserved. However

moving to this policy a list that do extensive modification to the email, may be too much of a change for the members of such list.

- Another mitigation policy, is to reject posts from domains with a DMARC policy other than p=none. However members of such Mailing Lists may complain of unfair exclusion.

- 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. [RFC3463] specifies Enhanced Mail System Status Codes which help differentiate between various bounces. Correctly interpreting Extended SMTP error messages is useful in this case in particular codes defined in [RFC7372] and in DMARC.

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.

4.2. Proposed and In-Progress Mitigations

The following mitigations are based on Internet Drafts which have not yet received broad consensus. They are described here to offer exploratory path for solutions. These solutions should not be used in a production environment.

- 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.

- DKIM with constrained transformations, [I-D.kucherawy-dkim-list-canon] is proposed to allow message modification.

- DKIM with recorded transformations, [I-D.kucherawy-dkim-transform] is proposed to indicate what limited transformations were done to the message so that a receiver could reverse them and confirm the validity of the orignal DKIM signature.

- [I-D.kucherawy-original-authres] is intended as a way to pass along Original Authentication Results to "downstream" receivers. It is not widely implemented and relies on a trust relationship between the forwarder and the other receivers.

- [I-D.levine-dkim-conditional] could be used to have the sender add a limited DKIM signature, that signs only a very limited set of header fields and not the body of the message. This DKIM

signature would come with the condition that a subsequent known domain fully DKIM sign the message. For instance a Mailing List could transform the message, add its DKIM signature and there would be a valid DKIM signature aligned with the RFC5322.From that would satisfy DMARC while limiting the possibilities of replay attack.

4.2.1. Getting More Radical: Requiring New Communication Paths Between MUAs

In practice a number of operators are using strict alignment mode in DMARC in order to avoid receiving new and innovative forms of unwanted and unauthentic email 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 some form of transitive trust.

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 Draegen and Franck Martin contributed to the IETF DMARC Working Group's wiki page listing all known interoperability issues with DMARC and indirect email flows.

Tim Draegen created the first draft of this document from these contributions and by hamfistedly 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.

[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.

[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-dkim-transform]
Kucherawy, M., "Recognized Transformations of Messages Bearing DomainKeys Identified Mail (DKIM) Signatures", draft-kucherawy-dkim-transform-00 (work in progress), April 2015.

[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)
Eudaemonic Development LLC
PO Box 19443
Asheville, NC 28815
USA

Email: tim@eudev.net

Elizabeth Zwicky (editor)
Yahoo
Sunnyvale, CA
USA

Email: zwicky@yahoo-inc.com