           Recommended Usage of the Authenticated Received Chain (ARC)
                     draft-ietf-dmarc-arc-usage-07

Abstract

   The Authentication Received Chain (ARC) provides an authenticated
   "chain of custody" for a message, allowing each entity that handles
   the message to see what entities handled it before, and to see what
   the message's authentication assessment was at each step in the
   handling. But the specification does not indicate how the entities
   handling these messages should interpret or utilize ARC results in
   making decisions about message disposition. This document will
   provide guidance in these areas.

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 https://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 October 25, 2019.

Table of Contents

1. Introduction

[ARC] is intended to be used by Internet Mail Handlers who forward or
resend messages, with or without alterations, such that they will no
longer pass the SPF [RFC7208], DKIM [RFC6376], and/or DMARC [RFC7489]
mechanisms when evaluated by subsequent message handlers or the final
recipient. In such cases ARC may provide useful information about
the message before the forwarding and/or alterations took place, and
recipients may choose to use this information to influence delivery
decisions.

2. Overview

2.1. How does ARC work?

Consider a message sent to a mailing list. Assume that the message
author's domain publishes an SPF record, signs messages with a DKIM
signature that includes the RFC5322.Subject header and the message
body, and publishes a DMARC policy of "p=reject". Finally, assume
that the final recipient(s) of the message implement SPF, DKIM and
DMARC authentication checks on incoming messages.

This message is received by the ADMD hosting the Mailing List Manager
(MLM) software. Upon receipt from the message author's ADMD, the
results from any DKIM, DMARC, and SPF checks would be recorded in an
Authentication-Results header. Then as part of normal list operation
the following changes are made to the message:

o An address controlled by the MLM is substituted in the
   RFC5321.MailFrom address field, allowing it to receive
   undeliverable messages

o A prefix is added to the message's RFC5322.Subject header

o Some text is appended to the message body

After these alterations have been made, the message is sent to list
members.

A list member's ADMD receiving the message will typically strip out
any existing Authentication-Results headers. It will then perform an
SPF check using the domain in the RFC5321.MailFrom address field, and
would find that the sending host is in the list of authorized senders
for the MLM's domain. However under DMARC, since this domain does
not match the domain in the RFC5322.From address field, the DMARC SPF
result is "fail."

The DKIM signature from the domain in the RFC5322.From address field
- the message author's domain - will fail to verify, because the
RFC5322.Subject header and the message body were altered by the MLM.
Therefore the DMARC DKIM result is also "fail," even if there is a
valid DKIM signature attached by the MLM's ADMD using its domain.

Since neither SPF or DKIM yield a "pass" under DMARC's alignment
rules, the DMARC result for this message is "fail." Therefore under
the DMARC policy published by the message author's domain, the list
member's ADMD should reject the message.

If the MLM implemented ARC, it would record the results of its email
authentication checks when receiving the message from the author's
ADMD in the Authentication-Results header, then perform the
alterations described above. It would then "seal" the message under
ARC, which includes the following steps.

It would record the contents of the Authentication-Results header(s)
in a newly created ARC-Authentication-Results header. It would
create an ARC-Message-Signature header, which includes a
cryptographic signature of the message itself very similar to a DKIM
signature, but excluding any ARC headers. Then it would create an
ARC-Seal header, which includes a cryptographic signature of all ARC
headers present in the message. The MLM's ADMD would then send the
ARC "sealed" message to the list members.

When the message reaches a list member's ADMD, the SPF and DKIM
results will still not pass the DMARC check. However if the
receiving ADMD implements ARC, it can check for and validate the ARC

chain in the message, and verify that the contents of the ARC-
Authentication-Results header were conveyed intact from the MLM's
ADMD. At that point the final recipient's ADMD might choose to use
those authentication results in the decision whether or not to
deliver the message, even though it failed to pass conventional SPF,
DKIM, and DMARC checks.

2.2. What new headers are introduced by ARC?

The following new headers are defined in [ARC] Section 4.1, "ARC
Header Fields":

o ARC-Seal

o ARC-Message-Signature

o ARC-Athentication-Results

Each time a message passes through an ARC Intermediary, an ARC Set
consisting of these three headers will be attached to the message.
More information about ARC Sets can be found in [ARC] Section 4.2,
"ARC Set." The entire collection of ARC Sets in a message is
commonly referred to as the ARC Chain.

2.3. Does ARC support Internationalized Email (EAI)?

Changes to support EAI are inherited from DKIM [RFC6376] as updated
by [draft-levine-eaiauth], and Authentication-Results as updated in
[I-D-7601bis]. For more details, please refer to [ARC]
Section 4.1.4, "Internationalized Email (EAI)."

2.4. Does ARC support multiple digital signature algorithms?

Originally ARC only supported a single signing algorithm, but the
DCRUP working group https://datatracker.ietf.org/wg/dcrup/about [1]
is expanding the set of supported algorithms available to DKIM
[RFC6376] and derived protocols. [ARC-MULTI] is adapting this work
to extend [ARC] to support multiple algorithms.

3. Guidance for Receivers/Validators

3.1. What is the significance of an intact ARC chain?

An intact ARC chain conveys authentication results like SPF and DKIM
as observed by the first ARC participant. In cases where the message
no longer produces passing results for DKIM, SPF, or DMARC but an
intact ARC chain is present, the message receiver may choose to use

   the contents of the first ARC-Authentication-Results header field in
   determining how to handle the message.

3.2. What exactly is an "intact" ARC chain?

   Note that not all ADMDs will implement ARC, and receivers will see
   messages where one or more non-participating ADMDs handled a message
   before, after, or in between participating ADMDs.

   An intact ARC chain is one where the ARC headers that are present can
   be validated, and in particular the ARC-Message-Signature header from
   the last ARC participant can still be validated. This shows that the
   portions of the message covered by that signature were not altered.
   If any non-participating ADMDs handled the message since the last ARC
   intermediary but did not alter the message in a way that invalidated
   the most recent ARC-Message-Signature present, the chain would still
   be considered intact by the next ARC-enabled ADMD.

   Message receivers may make local policy decisions about whether to
   use the contents of the ARC-Authentication-Results header field in
   cases where a message no longer passes DKIM, DMARC, and/or SPF
   checks. Whether an ARC chain is intact can be used to inform that
   local policy decision.

   So for example one message receiver may decide that, for messages
   with an intact ARC chain where a DMARC evaluation does not pass, but
   the ARC-Authentication-Results header field from the first ARC
   participant indicates a DKIM pass was reported that matches the
   domain in the RFC5322.From header field, it may override a DMARC
   "p=reject" policy. Another message receiver may decide to do so only
   for a limited number of ARC-enabled ADMDs. A third message receiver
   may choose not to take ARC information into account at all.

3.3. What is the significance of an invalid ("broken") ARC chain?

   An ARC chain is broken if the signatures in the ARC-Seal header
   fields cannot be verified, or if the most recent AMS can not be
   verified. For example if a non-ARC-enabled ADMD delivers a message
   with ARC header sets to the validating ADMD, but modified the message
   such that those ARC and DKIM signatures already in the message were
   invalidated.

   In case of a broken ARC chain, the message should be treated the same
   as if there was no ARC chain at all. For example, a message that
   fails under DMARC and has an invalid ARC chain would be subject to
   that DMARC policy, which may cause it to be quarantined or rejected.

Email transit can produce broken signatures for a wide variety of
benign reasons. This includes possibly breaking one or more ARC
signatures. Therefore, receivers need to be wary of ascribing motive
to such breakage, although patterns of common behaviour may provide
some basis for adjusting local policy decisions.

**3.4. What error code(s) should be returned if an invalid ARC chain is
       detected during an SMTP transaction?**

According to [ARC] Section 5.2.2, a Validator MAY signal the breakage
during the SMTP transaction by returning the extended SMTP response
code 5.7.29 "ARC validation failure" and corresponding SMTP basic
response code. Since ARC failures are likely the be detected due to
other, underlying authentication failures, Validators may also choose
to return the more general 5.7.26 "Multiple authentication checks
failed instead of the ARC-specific code.

3.5. What does the absence of an ARC chain in a message mean?

The absence of an ARC chain means nothing. ARC is intended to allow
a participating message handler to preserve certain authentication
results when a message is being forwarded and/or modified such that
the final recipient can evaluate this information. If they are
absent, there is nothing extra that ARC requires the final recipient
to do.

**3.6. What reasonable conclusions can you draw based upon seeing lots of
       mail with ARC chains?**

With sufficient history, ARC can be used to augment DMARC
authentication policy (i.e. a message could fail DMARC, but validated
ARC information and therefore could be considered as validly
authenticated as reported by the first ARC participant).

If the validator does content analysis and reputation tracking, the
ARC participants in a message can be credited or discredited for good
or bad content. By analyzing different ARC chains involved in "bad"
messages, a validator might identify malicious participating
intermediaries.

With a valid chain and good reputations for all ARC participants,
receivers may choose to apply a "local policy override" to the DMARC
policy assertion for the domain authentication evaluation, depending
on the ARC-Authentication-Results header field value. Normal content
analysis should never be skipped.

3.7. **What if none of the intermediaries have been seen previously?**

   This has no impact on the operation of ARC, as ARC is not a
   reputation system. ARC conveys the results of other authentication
   mechanisms such that the participating message handlers can be
   positively identified. Final message recipients may or may not
   choose to examine these results when messages fail other
   authentication checks. They are more likely to override, say, a
   failing DMARC result in the presence of an intact ARC chain where the
   participating ARC message handlers have been observed to not convey
   "bad" content in the past, and the initial ARC participant indicates
   the message they received had passed authentication checks.

3.8. **What about ARC chains where some intermediaries are known and
         others are not?**

   Validators may choose to build reputation models for ARC message
   handlers they have observed. Generally speaking it is more feasible
   to accrue positive reputation to intermediaries when they
   consistently send messages that are evaluated positively in terms of
   content and ARC chains. When messages are received with ARC chains
   that are not intact, it is very difficult identify which
   intermediaries may have manipulated the message or injected bad
   content.

3.9. **What should message handlers do when they detect malicious content
         in messages where ARC is present?**

   Message handlers should do what they normally do when they detect
   malicious content in a message - hopefully that means quarantining or
   discarding the message. ARC information should never make malicious
   content acceptable.

   In such cases it is difficult to determine where the malicious
   content may have been injected. What ARC can do in such cases is
   verify that a given intermediary or message handler did in fact
   handle the message as indicated in the header fields. In such cases
   a message recipient who maintains a reputation system about email
   senders may wish to incorporate this information as an additional
   factor in the score for the intermediaries and sender in question.
   However reputation systems are very complex, and usually unique to
   those organizations operating them, and therefore beyond the scope of
   this document.

3.10. **What feedback does a sender or domain owner get about ARC when it is applied to their messages?**

   ARC itself does not include any mechanism for feedback or reporting.
   It does however recommend that message receiving systems that use ARC
   to augment their delivery decisions, who use DMARC and decide to
   deliver a message because of ARC information, should include a
   notation to that effect in their normal DMARC reports. These
   notations would be easily identifiable by report processors, so that
   senders and domain owners can see where ARC is being used to augment
   the deliverability of their messages.

3.11. **What prevents a malicious actor from removing the ARC header fields, altering the content, and creating a new ARC chain?**

   ARC does not prevent a malicious actor from doing this. Nor does it
   prevent a malicious actor from removing all but the first ADMD's ARC
   header fields and altering the message, eliminating intervening
   participants from the ARC chain. Or similar variations.

   A valid ARC chain does not provide any automatic benefit. With an
   intact ARC chain, the final message recipient may choose to use the
   contents of the ARC-Authentication-Results header field in
   determining how to handle the message. The decision to use the ARC-
   Authentication-Results header field is dependent on evaluation of
   those ARC intermediaries.

   In the first case, the bad actor has succeeded in manipulating the
   message but they have attached a verifiable signature identifying
   themselves. While not an ideal situation, it is something they are
   already able to do without ARC involved, but now a signature linked
   to the domain responsible for the manipulation is present.

   Additionally in the second case it is possible some negative
   reputational impact might accrue to the first ARC participant left in
   place until more messages reveal the pattern of activity by the bad
   actor. But again, a bad actor can similarly manipulate a sequence of
   RFC5322.Received header fields today without ARC, but with ARC that
   bad actor has verifiably identified themselves.

4. **Guidance for Intermediaries**

4.1. **What is an Intermediary under ARC?**

   In the context of ARC, an Intermediary is typically an Administrative
   Management Domain [RFC5598] that is receiving a message, potentially
   manipulating or altering it, and then passing it on to another ADMD
   for delivery. Common examples of Intermediaries are mailing lists,

   alumni or professional email address providers that forward messages
   such as universities or professional organizations, et cetera.

4.2. What are the minimum requirements for an ARC Intermediary?

   A participating ARC intermediary must validate the ARC chain on a
   message it receives, if one is present. It then attaches its own ARC
   seal and signature, including an indication if the chain failed to
   validate upon receipt.

**4.2.1. More specifically a participating ARC intermediary must do the
          following:**

   1. Validate that the ARC chain, if one is already present in the
       message, is intact and well-formed. ([ARC] Section 5.2,
       "Validator Actions")

   2. Record the ARC status in an Authentication-Results header
       ([RFC7601])

   3. Generate a new ARC set and add it to the message. ([ARC]
       Section 5.1, "Sealer Actions")

4.3. Should every MTA be an ARC participant?

   Generally speaking, ARC is designed to operate at the ADMD level.
   When a message is first received by an ADMD, the traditional
   authentication results should be captured and preserved - this could
   be the common case of creating an Authentication-Results header
   field. But when it is determined that the message is being sent on
   outside of that ADMD, that is when the ADMD should add itself to the
   ARC chain - before sending the message outside of the ADMD.

   Some organizations may operate multiple ADMDs, with more or less
   independence between them. While they should make a determination
   based on their specific circumstances, it may be useful and
   appropriate to have multiple ADMDs be ARC participants.

**4.4. What should an intermediary do in the case of an invalid or
        "broken" ARC chain?**

   In general terms, a participating ARC intermediary will note that an
   ARC chain was present and invalid, or broken, when it attaches its
   own ARC seal and signature. However the fact that the ARC chain was
   invalid should have no impact on whether and how the message is
   delivered.

4.5. What should I do in the case where there is no ARC chain present
      in a message?

   A participating ARC intermediary receiving a message with no ARC
   chain, and which will be delivered outside its ADMD, should start an
   ARC chain according to the ARC specification. This will include
   capturing the normal email authentication results for the
   intermediary (SPF, DKIM, DMARC, etc), which will be conveyed as part
   of the ARC chain.

4.6. How could ARC affect my reputation as an intermediary?

   Message receivers often operate reputation systems, which build a
   behavioral profile of various message handlers and intermediaries.
   The presence or absence of ARC is yet another data point that may be
   used as an input to such reputation systems. Messages deemed to have
   good content may provide a positive signal for the intermediaries
   that handled it, while messages with bad content may provide a
   negative signal for the those intermediaries. Intact and valid ARC
   elements may amplify or attenuate such signals, depending on the
   circumstances.

   Reputation systems are complex and usually specific to a given
   message receiver, and a meaningful discussion of such a broad topic
   is beyond the scope of this document.

4.7. What can I do to influence my reputation as an intermediary?

   Today it is extremely simple for a malicious actor to construct a
   message that includes your identity as an intermediary, even though
   you never handled the message. It is possible that an intermediary
   implementing ARC on all traffic it handles might receive some
   reputational benefit by making it easier to detect when their
   involvement in conveying bad traffic has been "forged."

   As mentioned previously reputation systems are very complex and
   usually specific to a given message receiver, and a meaningful
   discussion of such a broad topic is beyond the scope of this
   document.

5. Guidance for Originators

5.1. Where can I find out more information?

   Please visit the http://arc-spec.org [2] web site, or join the arc-
   discuss mailing list at http://lists.dmarc.org/mailman/listinfo/arc-
   discuss [3].

To discuss the [ARC] specification itself, please join the DMARC
working group at https://datatracker.ietf.org/wg/dmarc [4].

5.2. How/where can I test interoperabililty for my implementation?

There have been numerous interoperability tests during the
development of the [ARC] specification. These tests are usually
announced on both the arc-discuss mailing list at
http://lists.dmarc.org/mailman/listinfo/arc-discuss [5], and the
DMARC working group at https://datatracker/ietf.org/wg/dmarc [6].
Join whichever body is most appropriate for you and/or your
organization to receive future announcements.

5.3. How can ARC impact my email?

Prior to ARC, certain DMARC policies on a domain would cause messages
using those domains in the RFC5322.From field, and which pass through
certain kinds of intermediaries (mailing lists, forwarding services),
to fail authentication checks at the message receiver. As a result
these messages might not be delivered to the intended recipient.

ARC seeks to provide these so-called "indirect mailflows" with a
means to preserve email authentication results as recorded by
participating intermediaries. Message receivers may accept validated
ARC information to supplement the information that DMARC provides,
potentially deciding to deliver the message even though a DMARC check
did not pass.

The net result for domain owners and senders is that ARC may allow
messages routed through participating ARC intermediaries to be
delivered, even though those messages would not have been delivered
in the absence of ARC.

5.4. How can ARC impact my reputation as a message sender?

Message receivers often operate reputation systems, which build a
behavioral profile of various message senders (and perhaps
intermediaries). The presence or absence of ARC is yet another data
point that may be used as an input to such reputation systems.
Messages deemed to have good content may provide a positive signal
for the sending domain and the intermediaries that handled it, while
messages with bad content may provide a negative signal for the
sending domain and the intermediaries that handled it. Intact and
valid ARC elements may amplify or attenuate such signals, depending
on the circumstances.

Reputation systems are complex and usually specific to a given
message receiver, and a meaningful discussion of such a broad topic
is beyond the scope of this document.

5.5. Can I tell intermediaries not to use ARC?

At present there is no way for a message sender to request that
intermediaries not employ ARC.

6. Considerations

6.1. IANA Considerations

This document has no actions for IANA.

6.2. Security Considerations

This document does not have security considerations aside from those
raised in the main content.

7. References

7.1. Normative References

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,
           DOI 10.17487/RFC5321, October 2008,
           <https://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322,
           DOI 10.17487/RFC5322, October 2008,
           <https://www.rfc-editor.org/info/rfc5322>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598,
           DOI 10.17487/RFC5598, July 2009,
           <https://www.rfc-editor.org/info/rfc5598>.

[RFC6377] Kucherawy, M., "DomainKeys Identified Mail (DKIM) and
           Mailing Lists", BCP 167, RFC 6377, DOI 10.17487/RFC6377,
           September 2011, <https://www.rfc-editor.org/info/rfc6377>.

[RFC7601] Kucherawy, M., "Message Header Field for Indicating
           Message Authentication Status", RFC 7601,
           DOI 10.17487/RFC7601, August 2015,
           <https://www.rfc-editor.org/info/rfc7601>.

7.2. Informative References

   [ARC]   Andersen, K., Long, B., Blank, S., and M. Kucherawy,
               "Authenticated Received Chain (ARC) Protocol", December
               2018, <https://tools.ietf.org/html/
               draft-ietf-dmarc-arc-protocol-23>.

   [ARC-MULTI]
               Andersen, K., Blank, S., and J. Levine, "Using Multiple
               Signing Algorithms with ARC", June 2018,
               <https://tools.ietf.org/html/
               draft-ietf-dmarc-arc-multi-02>.

   [draft-levine-eaiauth]
               Levine, J., "E-mail Authentication for Internationalized
               Mail", August 2018, <https://tools.ietf.org/html/
               draft-levine-appsarea-eaiauth-03>.

   [ENHANCED-STATUS]
               "IANA SMTP Enhanced Status Codes", n.d.,
               <http://www.iana.org/assignments/smtp-enhanced-status-
               codes/smtp-enhanced-status-codes.xhtml>.

   [I-D-7601bis]
               Kucherawy, M., "Message Header Field for Indicating
               Message Authentication Status", February 2018,
               <https://datatracker.ietf.org/doc/
               draft-ietf-dmarc-rfc7601bis/>.

   [OAR]   Chew, M. and M. Kucherawy, "Original-Authentication-
               Results Header Field", February 2012,
               <https://tools.ietf.org/html/
               draft-kucherawy-original-authres-00>.

   [RFC6376]   Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed.,
               "DomainKeys Identified Mail (DKIM) Signatures", STD 76,
               RFC 6376, DOI 10.17487/RFC6376, September 2011,
               <https://www.rfc-editor.org/info/rfc6376>.

   [RFC7208]   Kitterman, S., "Sender Policy Framework (SPF) for
               Authorizing Use of Domains in Email, Version 1", RFC 7208,
               DOI 10.17487/RFC7208, April 2014,
               <https://www.rfc-editor.org/info/rfc7208>.

   [RFC7489]   Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based
               Message Authentication, Reporting, and Conformance
               (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015,
               <https://www.rfc-editor.org/info/rfc7489>.

   [RFC7960] Martin, F., Ed., Lear, E., Ed., Draegen. Ed., T., Zwicky,
              E., Ed., and K. Andersen, Ed., "Interoperability Issues
              between Domain-based Message Authentication, Reporting,
              and Conformance (DMARC) and Indirect Email Flows",
              RFC 7960, DOI 10.17487/RFC7960, September 2016,
              <https://www.rfc-editor.org/info/rfc7960>.

7.3. URIs

   [1] https://datatracker.ietf.org/wg/dcrup/about

   [2] http://arc-spec.org

   [3] http://lists.dmarc.org/mailman/listinfo/arc-discuss

   [4] https://datatracker.ietf.org/wg/dmarc

   [5] http://lists.dmarc.org/mailman/listinfo/arc-discuss

   [6] https://datatracker/ietf.org/wg/dmarc

   [7] mailto:arc-discuss@dmarc.org

   [8] https://datatracker.ietf.org/wg/dmarc

   [9] https://arc-spec.org

   [10] mailto:arc-discuss@dmarc.org

   [11] http://lists.dmarc.org/mailman/listinfo/arc-discuss

Appendix A. Glossary

   ADMD Administrative Management Domain as used in [RFC5598] and
      similar references refers to a single entity operating one or more
      computers within one or more domain names under said entity's
      control. One example might be a small company with a single
      server, handling email for that company's domain. Another example
      might be a large university, operating many servers that fulfill
      different roles, all handling email for several different domains
      representing parts of the university.

   ARC ARC is an acronym: Authentication Results Chain - see also [ARC]

   ARC-Seal An [RFC5322] message header field formed in compliance with
      the ARC specification. It includes certain content from all prior
      ARC participants, if there are any.

ARC-Message-Signature (also abbreviated as "AMS") An [RFC5322]
   message header field formed in compliance with the [ARC]
   specification. It includes certain content about the message as
   it was received and manipulated by the intermediary who inserted
   it.

ARC-Authentication-Results (also abbreviated as "AAR") An [RFC5322]
   message header field formed in compliance with the [ARC]
   specification. It includes certain content about the message as
   it was received by the intermediary.

Authentication Results Chain (ARC) A system that allows a Message
   Receiver to identify Intermediaries or Message Handlers who have
   conveyed a particular message. For more information see the
   Abstract of this document, or refer to [ARC].

Domain Naming System Block List (DNSBL) This is a system widely used
   in email filtering services whereby information about the past
   activity of a set of hosts or domains indicates that messages
   should not be accepted from them, or at least should be subject to
   greater scrutiny before being accepted. Common examples would be
   SpamCop, Spamhaus.org, SORBS, etc.

Email Service Provider (ESP) An Email Service Provider is typically
   a vendor or partner firm that sends mail on behalf of another
   company. They may use email addresses in Internet domains
   belonging to the client or partner firm in various [RFC5321]
   fields or [RFC5322] message header fields of the messages they
   send on their behalf.

Intermediary In the context of [ARC], an Intermediary is typically
   an Administrative Management Domain (per [RFC5598]) that is
   receiving a message, potentially manipulating or altering it, and
   then passing it on to another ADMD for delivery. Also see
   [RFC7960] for more information and discussion. Common examples of
   Intermediaries are mailing lists, alumni or professional email
   address providers like universities or professional organizations,
   et cetera.

Mail/Message Transfer Agent (MTA) This refers to software that sends
   and receives email messsages across a network with other MTAs.
   Often run on dedicated servers, common examples are Exim,
   Microsoft Exchange, Postfix, and Sendmail.

Mailflow A group of messages that share features in common. Typical
   examples would be all messages sent by a given Message Sender to a
   Message Receiver, related to a particular announcement, a given
   mailing list, et cetera.

   Malicious Actor A Malicious Actor is a party, often an Intermediary,
      that will take actions that seek to exploit or defraud the
      ultimate recipient of the message, or subvert the network controls
      and infrastructure of the Message Receiver. Typical examples
      would be a spammer who forges content or attributes of a message
      in order to evade anti-spam measures, or an entity that adds an
      attachment containing a virus to a message.

   Message Handler A Message Handler is another name for an
      Intermediary.

   Message Receiver In the transmission of an email message from one
      ADMD to another, this is the organization receiving the message on
      behalf of the intended recipient or end user. The Message
      Receiver may do this because the intended recipient is an employee
      or member of the organization, or because the end user utilizes
      email services provided by the Message Receiver (Comcast, GMail,
      Yahoo, QQ, et cetera).

   Message Sender In the transmission of an email message from one ADMD
      to another, this is the organization sending the message on behalf
      of the Originator or end user.

   Originator This refers to the author of a given email message. In
      different contexts it may refer to the end-user writing the
      message, or the ADMD providing email services to that end-user.

   Reputation In the larger context of email hygiene - blocking spam
      and malicious messages - reputation generally refers to a wide
      variety of techniques and mechanisms whereby a message receiver
      uses the past actions of a sending host or domain to influence the
      handling of messages received from them in the future. One of the
      classic examples would be a Spamhaus-style DNSBL, where individual
      IP addresses will be blocked from sending messages because they've
      been identified as being bad actors. Very large message receivers
      may build and maintain their own reputation systems of this kind,
      whereas other organizations might choose to use commercial
      products or free services.

   Reputation Service Provider A Reputation Service Provider would be a
      source of reputation information about a message sender. In this
      context, the DNSBL services offered by Spamhaus would allow them
      to be referred to as an RPS. Many spam and virus filtering
      vendors incorporate similar functionality into their services.

   Request For Comment (RFC) RFCs are memoranda that "contain technical
      and organizational notes about the Internet." Created and managed
      by the Internet Engineering Task Force (IETF), they are de facto

standards for various methods of communicating or collaborating over the Internet.

RFC5321 - Simple Mail Transfer Protocol This document describes the protocol used to transfer email messages between Message Transfer Agents (MTA) over a network. Link: [RFC5321]

RFC5322 - Internet Message Format This document describes the format of Internet email messages, including both the header fields within the message and various types of content within the message body. Link: [RFC5322]

Validator A Message Receiver that attempts to validate the ARC chain in a message.

Appendix B. References

Appendix C. Acknowledgements

This draft is based on the work of OAR-Dev Group.

The authors thank the entire OAR-Dev group for the ongoing help, innumerable diagrams and discussions from all the participants, especially: Alex Brotman, Brandon Long, Dave Crocker, Elizabeth Zwicky, Franck Martin, Greg Colburn, J. Trent Adams, John Rae-Grant, Mike Hammer, Mike Jones, Steve Jones, Terry Zink, Tim Draegen.

This document was influenced by questions posed in the arc-discuss@dmarc.org [7] mailing list, and the authors thank all the list participants for their input.

Appendix D. Comments and Feedback

Please address all comments, discussions, and questions about this document, or about [ARC] itself, to the dmarc working group at https://datatracker.ietf.org/wg/dmarc [8].

Readers looking for general information about ARC may refer to the website https://arc-spec.org [9], or to the arc-discuss@dmarc.org [10] mailing list at http://lists.dmarc.org/mailman/listinfo/arc-discuss [11].

Authors' Addresses

Steven M Jones (editor)
DMARC.org
2419 McGee Avenue
Berkeley, California 94703
USA

Email: smj@crash.com

Kurt Andersen
LinkedIn
2029 Stierlin Ct.
Mountain View, California 94043
USA

Email: kurta@linkedin.com