independent
Internet-Draft
Intended status: Informational
Expires: August 11, 2016

. OAR-DEV Group
OAR-DEV Group
K. Andersen
LinkedIn
J. Rae-Grant, Ed.
B. Long, Ed.
Google
T. Adams, Ed.
Paypal
S. Jones, Ed.
TDP
February 08, 2016

Authenticated Received Chain (ARC)
draft-andersen-arc-02

Abstract

Authenticated Received Chain (ARC) permits an organization which is creating or handling email to indicate their involvement with the handling process by adding a cryptographically signed header (or headers) in a manner analagous to that of DomainKeys Identified Mail (DKIM). Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. Changes in the message which may break DKIM, may be tracked through the ARC set of headers.

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 August 11, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

Table of Contents

1. Introduction 3
2. Requirements 4
  2.1. Primary Design Criteria 4
  2.2. Out of Scope 4
  2.3. Utility 4
3. Terminology 4
4. Overview 5
5. Definition 5
  5.1. Description of the new headers 6
    5.1.1. ARC-Seal 6
    5.1.2. ARC-Message-Signature 8
    5.1.3. ARC-Authentication-Results 10
  5.2. Constructing the ARC-Seal Header Set 10
    5.2.1. Handling Violations in the ARC Header Set 11
  5.3. Key Management and Binding 11
    5.3.1. Namespace 12
6. Usage 12
  6.1. Participation 12
  6.2. Relationship between DKIM Signatures and ARC Headers . . 12
  6.3. Relationship of ARC-Message-Signatures and ARC-Seals . . 12
  6.4. Validating the ARC set of headers 13
  6.5. Assessing violations of ARC set validity 13
  6.6. Reporting violations of ARC set validity 13
  6.7. Recording results of ARC evaluation 13
    6.7.1. RFC6651 Failure Reporting for ARC 14
    6.7.2. Reporting ARC Effects for DMARC Local Policy 14
7. Privacy Considerations 14
8. IANA Considerations 14

8.1. Update to RFC7601 header method list 14
8.2. Definitions of the ARC headers 14
9. Security Considerations 15
9.1. Preventing Repurposing of ARC Headers 15
9.2. Messages Which Transit the Same ADMD More Than Once . . . 16
10. References 16
10.1. Normative References 16
10.2. Informative References 17
Appendix A. Appendix A - Example Usage 18
A.1. Example 1: Simple mailing list 18
A.1.1. Here's the message as it exits the Origin: 18
A.1.2. Message is then received at example.org 19
A.1.3. Example 1: Message received by Recipient 21
A.2. Example 2: Mailing list to forwarded mailbox 22
A.2.1. Here's the message as it exits the Origin: 22
A.2.2. Message is then received at example.org 23
A.2.3. Example 2: Message received by Recipient 27
A.3. Example 3: Mailing list to forwarded mailbox with source 29
A.3.1. Here's the message as it exits the Origin: 29
A.3.2. Message is then received at example.org 30
A.3.3. Example 3: Message received by Recipient 35
Appendix B. Acknowledgements 37
Appendix C. Comments and Feedback 38
Appendix D. Historical Note 38
Authors' Addresses 38

1. Introduction

The development of strong domain authentication through SPF and DKIM has led to the implementation of the DMARC framework [RFC7489]. Implicit within the DMARC framework is a requirement that any intermediaries between the source system and ultimate receiver system must preserve the validity of the DKIM signature; however, there are common email practices which break the DKIM validation ([DMARC-INTEROP]). This proposal is intended to define an Authenticated Received Chain (ARC) to address the problems with the untrustworthiness of the standard Received header sequence so that receivers can develop a more nuanced interpretation to guide any local policies related to messages which arrive with broken domain authentication.

Forgery of the Received headers is a common tactic for bad actors. One of the goals of this proposal is to define a comparable set of trace headers which can be relied upon by receivers in so far as all ADMD (ADministrative Management Domain) handlers of a message participate in the ARC chain.

The Authentication-Results (A-R) mechanism [RFC7601] permits the output of an email authentication evaluation process to be transmitted from the evaluating host to a consuming host that uses the information. On its own, A-R operates within a trust domain. ARC provides a protection mechanism for the data, permiting the communication to cross trust domain boundaries.

2. Requirements

The specification of the ARC framework is driven by the following high-level goals, security considerations, and practical operational requirements.

2.1. Primary Design Criteria

- o Provide a method by which a "chain of custody" can be documented for email messages
- o Not require changes for senders of email
- o Support the complete verification of the ARC header set by each hop in the handling chain
- o Work at internet scale
- o Provide a trustable mechanism for the communication of Authentication-Results across trust boundaries.

2.2. Out of Scope

ARC is not a trust framework. Users of the ARC headers are cautioned against making unsubstantiated conclusions when encountering a "broken" ARC sequence.

2.3. Utility

The ARC-related set of headers can be used (when validated) to determine the path that an email message has taken between the sending system and receiver. Subject to the cautions mentioned below under Section 9, this information can assist in determining any local policy overrides to for violations of sender domain authentication policies.

3. Terminology

This section defines terms used in the rest of the document.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Readers are encouraged to be familiar with the contents of [RFC5598], and in particular, the potential roles of intermediaries in the delivery of email.

Syntax descriptions use Augmented BNF (ABNF) [RFC5234].

4. Overview

When an email is received without a properly valildated domain author, the inability to believe the accuracy of a series of Received headers prevents receiving systems from having a way to infer anything about the handling of the message by looking at the ADMD's through which the message has traveled.

With the implementation of this proposal, participating ADMDs would be able to securely register their handling of an email message. If all intermediaries participate in the ARC process, then receivers will be able to rely upon the chain and make local policy decisions informed by that information.

The ARC set of headers provides a method by which participating intermediaries can indicate the hand-offs for email messages.

5. Definition

This proposal defines three new headers:

- Header field name: ARC-Seal (abbreviated below as AS)

- Header field name: ARC-Message-Signature (abbreviated below as AMS)

- Header field name: ARC-Authentication-Results (abbreviated below as AAR)

Collectively, these headers form a connected set of attribution information by which receivers can identify the handling path for a message. The collective group is referred to in this document as the "ARC headers" or "set of ARC headers".

Specific references to individual headers use the header field names to distinguish such references.

The ARC header sets SHOULD be added at the top of a message as it transits MTAs that do authentication checks, so some idea of how far away the checks were done can be inferred. They are therefore considered to be a trace field as defined in [RFC5321], and all of the related definitions in that document apply.

Relative ordering of different trace headers (the ARC sets, DKIM, Received, etc.) is unimportant for this specification. In general, trace headers, such as ARC, SHOULD be added at the top of the email headers, but receivers MUST be able to process the headers from wherever they are found in the message headers. Ordering amongst the individual ARC headers and header sets is specified below and MUST be followed for proper canonicalized signing and evaluation.

5.1. Description of the new headers

5.1.1. ARC-Seal

ARC-Seal is a Structured Header Field as defined in Internet Message Format ([RFC5322]). All of the related definitions in that document apply.

The ARC-Seal makes use of the "tag=value" construction as defined in [RFC6376], section 3.2.

The value of the header field consists of an authentication identifier, and a series of statements and supporting data. The statements are of the form "tag=value" and indicate relevant data about the signing of the ARC set of headers. The header field can appear more than once in a single message.

The ARC-Seal header only signs across the (earlier) ARC-Seal, (and all) ARC-Message-Signature, and ARC-Authentication-Results headers.

5.1.1.1. Tags in the ARC-Seal header

5.1.1.1.1. Mandatory

- o i = instance or sequence number; monotonically increasing at each "sealing" entity beginning with '1'

- o a = hash algorithm (SHA256 as example) (as per [RFC6376] "a" tag)

- o t = timestamp (seconds since Unix epoch) (as per [RFC6376] "t" tag)

- o s = Selector for key ("s=seal2015") (as per [RFC6376] "s" tag)

o d = domain for key ("d=example.com") (as per [RFC6376] "d" tag)

o b = signature of the header hash (as per [RFC6376] "b" tag)

o cv = chain validation status: values =

** 'V' = valid chain received; ** 'N' = no pre-existing chain; ** 'P' = permanent error, the chain as received does not validate; ** 'T' = temporary error, such as a DNS lookup error

5.1.1.2. Differences between DKIM-Signature and ARC-Seal

No 'bh' value is defined for ARC-Seal.

ARC-Seal does not use the 'h' list of headers that is defined for DKIM-Signatures because the list of applicable headers is fully determined by the construction rules (see Section 5.2).

ARC-Seal does not use the 'c' (canonicalization) tag because only 'relaxed' canonicalization [RFC6376] is allowed for ARC-Seal header canonicalization.

5.1.1.3. Implicit 'h' Value for ARC-Seal

5.1.1.3.1. First instance

The ARC-Seal's (AS(1)) effective "h" scope would be AAR(1):AMS(1):AS(1-no-b).

5.1.1.3.2. Second instance

The ARC-Seal's (AS(2)) effective "h" scope would be AAR(1):AMS(1):AS(1):AAR(2):AMS(2):AS(2-no-b).

5.1.1.3.3. Third instance

The ARC-Seal's (AS(3)) effective "h" scope would be AAR(1):AMS(1):AS(1):AAR(2):AMS(2):AS(2):AAR(3):AMS(3):AS(3-no-b).

5.1.1.4. Computing the 'b' signature value for ARC-Seal

The ARC-Seal instance with an empty 'b' field shall be affixed when computing the signature and the 'b' value added afterward just as in the procedure for DKIM-Signature calculations (section 3.5 of [RFC6376]).

Signing calculation MUST be done in bottom-up order as specified in section 5.4.2 of [RFC6376] and as illustrated above Section 5.1.1.3.

5.1.2. ARC-Message-Signature

The ARC-Message-Signature header is a special variant of a DKIM-Signature [RFC6376], using only the relaxed header canonicalization rules specified in [RFC6376] but with a different rules for the header (h=) list to prevent mis-appropriation as a DKIM-Signature.

The ARC-Message-Signature header field can appear multiple times in a single message but each instance must have a unique "i=" value.

5.1.2.1. Removed

This section was redundant and is removed as of the -02 revision.

5.1.2.2. Differences between DKIM-Signature and ARC-Message-Signature

5.1.2.2.1. 'h' value

When constructing the 'h' list for the ARC-Message-Signature, the following headers must be implicitly signed, but not listed within the 'h' list:

1. Message-ID

2. Date

3. From (valid instance with the value)

4. From (empty instance to prevent multi-From abuse)

5. To

6. Subject (valid instance with the value)

7. Subject (empty instance to prevent multi-Subject abuse)

This provides a unique 'h' list which prevents re-use or misappropriation of the ARC-Message-Signature as if it was a DKIM-Signature.

Because many MTAs will create their own Message-ID, Date, and To headers, ** in progress**

5.1.2.2.1.1. Comparison of ARC 'h' and DKIM 'h'

With the use of "implicit" headers, the order of signing is important for interoperability. The relationship of the ARC 'h' and the DKIM 'h' is as follows:

```
For each header name in implicit list:
   For each instance of the header from the bottom of the headers up:
     SignUpdate(canonical header)
For each header from the bottom of the headers up:
  If header is not implicit:
    SignUpdate(canonical header)
```

This means that the equivalent dkim_h value would be

```
message-id*:date*:from*(:from):to*:subject*(:subject):arc_h
```

5.1.2.2.1.2. Header Fields to Explicitly Include in ARC-Message-Signature 'h'

ARC-Seal headers MUST not be included in the signing scope of any ARC-Message-Signature headers.

Participants may include any other header fields within the scope of the ARC-Message-Signature signature except ARC-Seal headers. In particular, all DKIM-Signature headers are highly recommended to be included. The advice regarding headers to avoid is found in section 5.4 of [RFC6376] and should be observed for ARC-Message-Signatures just as they are for DKIM-Signature exclusion. ARC-Authentication-Results SHOULD be included explicitly within the scope of ARC-Message-Signature headers.

5.1.2.2.2. Implicit Canonicalization: 'c'

The ARC-Message-Signature header MUST be created using the relaxed header canonicalization rules [RFC6376]. The "c=" field MUST not be included in the ARC-Message-Signature.

5.1.2.2.3. 'i' value

For the ARC-Message-Signature, the 'i' value is the corresponding instance which matches the 'i' value of the related ARC-Seal (see Section 5.1.1.1.1).

5.1.2.2.4. 'v'

'v' is not defined for an ARC-Message-Signature and is not allowed.

5.1.2.3. Computing the 'b' value for ARC-Message-Signature

The ARC-Message-Signature instance with an empty 'b' field shall be affixed when computing the signature and the 'b' value added afterward just as in the procedure for DKIM-Signature calculations (section 3.5 of [RFC6376]).

Header signing MUST be done in bottom-up order as specified in section 5.4.2 of [RFC6376].

5.1.3. ARC-Authentication-Results

ARC-Authentication-Results is a direct copy of the Authentication-Results header [RFC7601] created for archival purposes by the each MTA outside of the trust boundary of the originating system which is contributing to the chain of ARC headers. (See also [OAR] for a similar usage.) The corresponding instance ("i=") value MUST be prefixed to the Authentication-Results.

The value of the header field (after removing comments) consists of an instance identifier, an authentication identifier, and then a series of statements and supporting data. The statements are of the form "method=result" and indicate which authentication method(s) were applied and their respective results. For each such statement, the supporting data can include a "reason" string and one or more "property=value" statements indicating which message properties were evaluated to reach that conclusion. The header field can appear multiple times in a single message but each instance must have a unique "i=" value.

5.1.3.1. 'i' value

For the ARC-Authentication-Results, the 'i' value is the corresponding instance which matches the 'i' value of the related ARC-Seal (see Section 5.1.1.1.1).

5.2. Constructing the ARC-Seal Header Set

The ARC-Seal is built in the same fashion as the analogous DKIM-Signature [RFC6376], using the relaxed header canonicalization rules specified in [RFC6376] but with a strict ordering component for the headers which are covered by the cryptographic signature:

1. The ARC headers MUST be ordered in descending instance (i=) order.

2. The referenced ARC-Message-Signatures (matching i= value) MUST immediately follow the ARC-Seal instance which included the reference.

3. The associated ARC-Authentication-Results header (matching i= value) MUST be the last item in the list for each set of ARC headers.

Thus, when prefixing ARC headers to the beginning part of the header block,

1. the AAR header would be prefixed first; then

2. the AMS would be calculated and prefixed;

3. lastly the AS would be calculated and prefixed.

5.2.1. Handling Violations in the ARC Header Set

When ordering the ARC set headers, if there are gross violations of this protocol, such as duplicated instance numbers, such header set(s) shall be ordered as follows (when analyzing for validity or subsequent signing):

- Within each set, headers shall be sorted as specified in Section 5.2.

- Any header sets which are complete duplicates shall be deduplicated - leaving only one instance of each unique header set; then any remaining order dependencies between sets shall be ordered as follows:

1. (First) By descending order of i=

2. (First) By descending order of t= (from the ARC-Seal header within the set)

3. (Finally) By ascending US-ASCII [RFC1345] sort order for the entire canonicalized header set

The intent of specifying this ordering is to allow downstream message handlers to add their own ARC header sets in a deterministic manner and to provide some resiliance against mis-behaving downstream MTAs. Participants who wish to have ARC information accrue to their benefit are advised to ensure proper implementation so that this section would never need to be invoked for their ARC headers.

5.3. Key Management and Binding

The public keys for ARC-Seals follow the same requirements and semantics as those for DKIM-Signatures [RFC6376]. Operators may use distinct selectors for the ARC-Seals at their own discretion.

5.3.1. Namespace

All ARC-Seal keys are stored in the same subdomain as DKIM keys [RFC6376]: "_domainkey". Given an ARC-Seal field with a "d=" tag of "example.com" and an "s=" tag of "foo.bar", the DNS query will be for "foo.bar._domainkey.example.com".

6. Usage

For a more thorough treatment of the recommended usage of the ARC headers for both intermediaries and end receivers, please consult [ARC-USAGE].

6.1. Participation

The inclusion of additional ARC header sets should be done whenever a trust boundary is crossed and especially when prior DKIM-Signatures may not survive the handling which is being performed (such as some mailing lists which modify the content of messages or some gateway transformations). Note that trust boundaries may or may not exactly correspond with ADMD boundaries.

Each participating ADMD MUST validate the preceding ARC set of headers as a part of asserting their own seal. Even if the set is determined to be invalid, a participating ADMD SHOULD apply their own seal because this can help in analysis of breakage points in the chain.

6.2. Relationship between DKIM Signatures and ARC Headers

Any DKIM-Signatures SHOULD not include any of the ARC-Seal, ARC-Message-Signature, or ARC-Authentication-Results headers in the scope of their header list.

ARC-Message-Signatures SHOULD include all DKIM-Signatures within their scope.

6.3. Relationship of ARC-Message-Signatures and ARC-Seals

The ARC-Message-Signature(s) should not include any of the ARC-Seal headers in their coverage scope in order maintain a separation of responsibilities. When adding an ARC-Authentication-Results header, it should be added before computing the ARC-Message-Signature. When "sealing" the message, an operator must create the ARC-Message-Signature before the ARC-Seal in order to reference it and embed the ARC-Message-Signature within the ARC-Seal signature scope. (Also refer to Section 5.2)

Each ARC-Seal is connected to its respective ARC-Message-Signature through the i= field.

6.4. Validating the ARC set of headers

Validation of the ARC headers can be performed step-wise by building up the sequence in order as defined in Section 5.2 and evaluating the correctness of the b= signature at each step. If a violation of the construction rules is found, for instance missing or repeated instance numbers or an otherwise invalid ARC-Seal header, validation fails and should be indicated as 'P'(ermanent error).

6.5. Assessing violations of ARC set validity

There are a wide variety of ways in which the ARC set of headers can be broken. Receivers should be wary of ascribing motive to such breakage although patterns of common behaviour may provide some basis for adjusting local policy decisions.

This proposal is exclusively focused on well-behaved, participating intermediaries that result in a valid chain of ARC-related headers. The presence of such a well-formed valid chain should also not be over-interpreted since malicious content can be easily introduced by otherwise well-intended senders through machine or account compromises. All normal content-based analysis should still be performed on any messages bearing an ARC sequence.

6.6. Reporting violations of ARC set validity

If a receiver determines that the ARC set of headers has a permanent error, the receiver MAY signal the breakage through the extended SMTP response code 5.7.7 [RFC3463] "message integrity failure" [ENHANCED-STATUS].

The extended SMTP response code should be paired with a 550 reply code. (550 = Requested action not taken: mailbox unavailable (e.g., mailbox not found, no access, or command rejected for policy reasons) [RFC5321])

6.7. Recording results of ARC evaluation

Receivers may add an "arc=pass" or "arc=fail" method annotation into their local Authentication-Results [RFC7601] header.

6.7.1. RFC6651 Failure Reporting for ARC

Due to very limited adoption, ARC evaluation results are not recommended for failure reporting as described for DKIM in [RFC6651].

6.7.2. Reporting ARC Effects for DMARC Local Policy

Receivers SHOULD indicate situations in which ARC evaluation influenced the results of their local policy determination. Usage in the DMARC reporting may look something like (utilizing a list of the ARC participants that were found):

```
<policy_evaluated>
  <disposition>delivered</disposition>
  <dkim>fail</dkim>
  <spf>fail</spf>
  <reason>
   <type>local_policy</type>
   <comment>arc=pass d=d1.example,d2.example</comment>
  </reason>
</policy_evaluated>
```

7. Privacy Considerations

The ARC-Seal chain provides a verifiable record of the handlers for a message. Anonymous remailers will probably not find this to match their operating goals.

8. IANA Considerations

This proposal adds three new headers as defined below.

8.1. Update to RFC7601 header method list

This proposal adds a new method to the [RFC7601] header: "arc=" for recording the results of the ARC header validation.

8.2. Definitions of the ARC headers

This proposal adds three new header fields to the "Permanent Message Header Field Registry", as follows:

o Header field name: ARC-Seal

  Applicable protocol: mail

  Status: draft

Author/Change controller: OAR-Dev Group

Specification document(s): [I-D.ARC]

Related information: [RFC6376]

- Header field name: ARC-Message-Signature

  Applicable protocol: mail

  Status: draft

  Author/Change controller: OAR-Dev Group

  Specification document(s): [I-D.ARC]

  Related information: [RFC6376]

- Header field name: ARC-Authentication-Results

  Applicable protocol: mail

  Status: standard

  Author/Change controller: IETF

  Specification document(s): [I-D.ARC]

  Related information: [RFC7601] [OAR]

9. Security Considerations

Recipients are cautioned to treat messages bearing ARC-Seal chains with the same suspicion that they apply to all other email messages. This includes appropriate content scanning and other checks for potentially malicious content. The handlers which are identified within the ARC-Seal chain may be used to provide input to local policy engines in cases where the sending system's DKIM-Signature does not validate.

9.1. Preventing Repurposing of ARC Headers

The ARC headers have been designed in such a way that they can not be re-used as standard DKIM-Signatures to prevent mis-use.

9.2. Messages Which Transit the Same ADMD More Than Once

Messages which loop in and out of an ADMD may lead to confusion about the scope of a particular set of ARC headers. The use of coordinated instance (i=) values and the non-confusability of the ARC-Message-Signature vs. a DKIM-Signature are designed to prevent misunderstandings.

10. References

10.1. Normative References

[RFC1345] Simonsen, K., "Character Mnemonics and Character Sets", RFC 1345, DOI 10.17487/RFC1345, June 1992, <http://www.rfc-editor.org/info/rfc1345>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2142] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, DOI 10.17487/RFC2142, May 1997, <http://www.rfc-editor.org/info/rfc2142>.

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, DOI 10.17487/RFC2606, June 1999, <http://www.rfc-editor.org/info/rfc2606>.

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, DOI 10.17487/RFC3463, January 2003, <http://www.rfc-editor.org/info/rfc3463>.

[RFC4686] Fenton, J., "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)", RFC 4686, DOI 10.17487/RFC4686, September 2006, <http://www.rfc-editor.org/info/rfc4686>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

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

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

[RFC5585] Hansen, T., Crocker, D., and P. Hallam-Baker, "DomainKeys Identified Mail (DKIM) Service Overview", RFC 5585, DOI 10.17487/RFC5585, July 2009, <http://www.rfc-editor.org/info/rfc5585>.

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

[RFC5863] Hansen, T., Siegel, E., Hallam-Baker, P., and D. Crocker, "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations", RFC 5863, DOI 10.17487/RFC5863, May 2010, <http://www.rfc-editor.org/info/rfc5863>.

[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, <http://www.rfc-editor.org/info/rfc6376>.

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

[RFC6651] Kucherawy, M., "Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting", RFC 6651, DOI 10.17487/RFC6651, June 2012, <http://www.rfc-editor.org/info/rfc6651>.

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

10.2. Informative References

[ARC-USAGE] Jones, S., Adams, T., Rae-Grant, J., and K. Andersen, "Recommended Usage of the ARC Headers", October 2015, <https://tools.ietf.org/html/draft-jones-arc-usage-00>.

[DMARC-INTEROP]
Martin, F., Lear, E., Draegen, T., Zwicky, E., and K. Andersen, "Interoperability Issues Between DMARC and Indirect Email Flows", January 2016, <https://tools.ietf.org/html/draft-ietf-dmarc-interoperability-14>.

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

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

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

10.3. URIs

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

Appendix A. Appendix A - Example Usage

A.1. Example 1: Simple mailing list

A.1.1. Here's the message as it exits the Origin:

```
Return-Path: <jqd@d1.example>
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
    s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
     Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijrvQw
     bv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4Gd3TRJl
     gotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@dmarc.org
Subject: Example 1

Hey gang,
This is a test message.
--J.
```

A.1.2. Message is then received at example.org

A.1.2.1. Example 1, Step A: Message forwarded to list members

Processing at example.org:

- example.org performs authentication checks
- No previous Auth-Results or ARC-Seal headers are present
- example.org adds ARC-Auth-Results header
- example.org adds Received: header
- example.org adds a ARC-Seal header

Here's the message as it exits example.org:

```
Return-Path: <jqd@d1.example>
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF1F5
     vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3A+m4bw
     a6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=1; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
    s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
     Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijr
     vQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4G
     d3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@example.org
Subject: [Lists] Example 1

Hey gang,
This is a test message.
--J.
```

A.1.3. Example 1: Message received by Recipient

Let's say that the Recipient is example.com

Processing at example.com:

- example.com performs usual authentication checks
- example.com adds Auth-Results: header, Received header
- Determines that message fails DMARC
- Checks for ARC-Seal: header; finds one
- Validates the signature in the ARC-Seal: header, which covers the ARC-Authentication-Results: header
- example.com can use the ARC-Authentication-Results values or verify the DKIM-Signature from lists.example.org

Here's what the message looks like at this point:

```
Return-Path: <jqd@d1.example>
Received: from example.org (example.org [208.69.40.157])
    by clothilde.example.com with ESMTP id
    d200mr22663000ykb.93.1421363207
    for <fmartin@example.com>; Thu, 14 Jan 2015 15:02:40 -0800 (PST)
Authentication-Results: clothilde.example.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@example.org; dmarc=fail; arc=pass
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF
     1F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3
     A+m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=1; lists.example.org;
```

```
     spf=pass smtp.mfrom=jqd@d1.example;
     dkim=pass (1024-bit key) header.i=@d1.example;
     dmarc=pass
 Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
     (authenticated bits=0)
     by segv.d1.example with ESMTP id t0FN4a8O084569;
     Thu, 14 Jan 2015 15:00:01 -0800 (PST)
     (envelope-from jqd@d1.example)
 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
     s=20130426; t=1421363082;
     bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
     h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
      Content-Transfer-Encoding;
     b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijrvQw
      bv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4Gd3TRJl
      gotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
 Message-ID: <54B84785.1060301@d1.example>
 Date: Thu, 14 Jan 2015 15:00:01 -0800
 From: John Q Doe <jqd@d1.example>
 To: arc@example.org
 Subject: [Lists] Example 1

 Hey gang,
 This is a test message.
 --J.
```

A.2. Example 2: Mailing list to forwarded mailbox

A.2.1. Here's the message as it exits the Origin:

```
Return-Path: <jqd@d1.example>
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
    s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
     Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijrvQw
     bv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4Gd3TRJl
     gotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@example.org
Subject: Example 1

Hey gang,
This is a test message.
--J.
```

A.2.2. Message is then received at example.org

A.2.2.1. Example 2, Step A: Message forwarded to list members

Processing at example.org:

- example.org performs authentication checks
- example.org applies standard DKIM signature
- No previous Auth-Results or ARC-Seal headers are present
- example.org adds ARC-Auth-Results header
- example.org adds usual Received: header
- example.org adds a ARC-Seal header

Here's the message as it exits Step A:

```
Return-Path: <jqd@d1.example>
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz6
     1TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L
     69EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF
     1F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3
     A+m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=1; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
    s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
     Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijr
     vQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4G
     d3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@example.org
Subject: [Lists] Example 1

Hey gang,
This is a test message.
--J.
```

A.2.2.2. Example 2, Step B: Message from list forwarded

The message is delivered to a mailbox at gmail.com
Processing at gmail.com:

- gmail.com performs usual authentication checks
- gmail.com adds Auth-Results: and Received: header
- Determines that message fails DMARC
- Checks for ARC-Seal: header; finds one
- Validates the signature in the ARC-Seal: header, which covers the ARC-Authentication-Results: header
- Uses the ARC-Auth-Results: values, but:
- Instead of delivering message, prepares to forward message per user settings
- Applies usual DKIM signature
- gmail.com adds it's own ARC-Seal: header, contents of which are
  - version
  - sequence number ("i=2")
  - hash algorithm (SHA256 as example)
  - timestamp ("t=")
  - selector for key ("s=notary01")
  - domain for key ("d=gmail.com")
  - headers included in hash ("h=ARC-Authentication-Results:ARC-Seal")
  - Note: algorithm requires only ARC-Seals with lower sequence # be included, in ascending order
  - signature of the header hash

Here's what the message looks like at this point:

Return-Path: <jqd@d1.example>

```
ARC-Seal: i=2; a=rsa-sha256; t=1421363253;
    s=notary01; d=gmail.com; cv=V;
    b=sjHDMriRZ0Mui5eVEOGscRHWbQHcy97lvrduHQ8h+f2CfIrxUiKOE44x3LQwDWR
     YbDjf5fcM9MdcIahC+cP59BQ9Y9DHwMDzwRTnM7NVb4kY+tSaVnLoIOaP9lF/sut
     txO+RRNr0fCFw==
ARC-Message-Signature: i=2; a=rsa-sha256;
    d=gmail.com; s=20120806;
    h=mime-version:content-type:x-original-sender:
     x-original-authentication-results:precedence:mailing-list:
     list-id:list-post:list-help:list-archive:sender:reply-to:
     list-unsubscribe:DKIM-Signature;
    bh=2+gZwZhUK2V7JbpoO2MTrU19WvhcA4JnjiohFm9ZZ/g=;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0Ab8Oi1ebYV/hIBmfhS
     LF1E80hMPcMijONfTQB6g5Hoh/kE6N2fgp6aSngL/WA3+g3Id8ElhXHvIGcJRFeM
     KdJqiW5cxdqPTRW+BnR5ee6Tzg06kr265NTDIAU8p8fQNuLfZj49MMA+QwDBJtXw
     bQoZyRtb6X6q0mYaszUB8kw==
Received: by mail-yk0-f179.google.com with SMTP id 19so2728865ykq.10
    for <mailbox@gmail.com>; Thu, 14 Jan 2015 15:02:45 -0800 (PST)
Authentication-Results: i=2; gmail.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@example.org; dmarc=fail; arc=pass
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=N:
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF
     1F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3
     A+m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=1; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
```

```
        (envelope-from jqd@d1.example)
    DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
        s=20130426; t=1421363082;
        bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
        h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
         Content-Transfer-Encoding;
        b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijr
         vQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4G
         d3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
    Message-ID: <54B84785.1060301@d1.example>
    Date: Thu, 14 Jan 2015 15:00:01 -0800
    From: John Q Doe <jqd@d1.example>
    To: arc@example.org
    Subject: [Lists] Example 1

    Hey gang,
    This is a test message.
    --J.
```

A.2.3. Example 2: Message received by Recipient

Let's say that the Recipient is example.com
Processing at example.com:

- example.com performs usual authentication checks

- example.com adds Auth-Results: header, Received header

- Determines that message fails DMARC

- Checks for ARC-Seal: header; finds two

- Validates the signature in the highest numbered ("i=2") ARC-Seal: header, which covers all previous ARC-Seal: and ARC-Authentication-Results: headers

- Validates the other ARC-Seal header ("i=1"), which covers the ARC-Authentication-Results: header

- example.com uses the ARC-Authentication-Results: values

Here's what the message looks like at this point:

```
    Return-Path: <jqd@d1.example>
    Received: from mail-ob0-f188.google.com (mail-ob0-f188.google.com
        [208.69.40.157]) by clothilde.example.com with ESMTP id
        d200mr22663000ykb.93.1421363268
        for <fmartin@example.com>; Thu, 14 Jan 2015 15:03:15 -0800 (PST)
```

```
Authentication-Results: clothilde.example.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@gmail.com; dmarc=fail; arc=pass
ARC-Seal: i=2; a=rsa-sha256; t=1421363253;
    s=notary01; d=gmail.com; cv=V;
    b=sjHDMriRZ0Mui5eVEOGscRHWbQHcy97lvrduHQ8h+f2CfIrxUiKOE44x3LQwDWR
     YbDjf5fcM9MdcIahC+cP59BQ9Y9DHwMDzwRTnM7NVb4kY+tSaVnLoIOaP9lF/sut
     txO+RRNr0fCFw==
ARC-Message-Signature: i=2; a=rsa-sha256;
    d=gmail.com; s=20120806;
    h=mime-version:content-type:x-original-sender:
     x-original-authentication-results:precedence:mailing-list:
     list-id:list-post:list-help:list-archive:sender:reply-to:
     :list-unsubscribe:DKIM-Signature;
    bh=2+gZwZhUK2V7JbpoO2MTrU19WvhcA4JnjiohFm9ZZ/g=;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0Ab8Oi1ebYV/hIBmfhS
     LF1E80hMPcMijONfTQB6g5Hoh/kE6N2fgp6aSngL/WA3+g3Id8ElhXHvIGcJRFeM
     KdJqiW5cxdqPTRW+BnR5ee6Tzg06kr265NTDIAU8p8fQNuLfZj49MMA+QwDBJtXw
     bQoZyRtb6X6q0mYaszUB8kw==
Received: by mail-yk0-f179.google.com with SMTP id 19so2728865ykq.10
    for <mailbox@gmail.com>; Thu, 14 Jan 2015 15:02:45 -0800 (PST)
Authentication-Results: i=2; gmail.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@example.org; dmarc=fail; arc=pass
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF
     1F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3
     A+m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=1; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
```

```
       (authenticated bits=0)
       by segv.d1.example with ESMTP id t0FN4a8O084569;
       Thu, 14 Jan 2015 15:00:01 -0800 (PST)
       (envelope-from jqd@d1.example)
   DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
       s=20130426; t=1421363082;
       bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
       h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
        Content-Transfer-Encoding;
       b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijr
        vQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4G
        d3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
   Message-ID: <54B84785.1060301@d1.example>
   Date: Thu, 14 Jan 2015 15:00:01 -0800
   From: John Q Doe <jqd@d1.example>
   To: arc@example.org
   Subject: [Lists] Example 1

   Hey gang,
   This is a test message.
   --J.
```

A.3. Example 3: Mailing list to forwarded mailbox with source

A.3.1. Here's the message as it exits the Origin:

```
Return-Path: <jqd@d1.example>
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=origin2015; d=d1.example; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61T
     X6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69EU
     8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=d1.example; s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=MIME-Version:CC:Content-Type:Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijrv
     Qwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4Gd3
     TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@example.org
Subject: Example 1

Hey gang,
This is a test message.
--J.
```

A.3.2. Message is then received at example.org

A.3.2.1. Example 3, Step A: Message forwarded to list members with source

Processing at example.org:

- example.org performs authentication checks

- example.org applies standard DKIM signature

- Checks for ARC-Seal: header; finds one (i=1)

- Validates the signature in the ARC-Seal (i=1): header, which covers the d1.example ARC-Message-Signature: header

- example.org adds ARC-Auth-Results header

- example.org adds usual Received: header

- example.org adds a DKIM-Signature
- example.org adds a ARC-Seal header, contents of which are
  - sequence number ("i=2")
  - hash algorithm (SHA256 as example)
  - timestamp ("t=")
  - chain validity ("cv=")
  - selector for key ("s=seal2015")
  - domain for key ("d=example.org")
  - signature ("b=")

Here's the message as it exits Step A:

```
Return-Path: <jqd@d1.example>
ARC-Seal: i=2; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=V;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz6
     1TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L
     69EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=2; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:From:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF
     1F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3
     A+m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=2; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=origin2015; d=d1.example; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=d1.example; s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=MIME-Version:CC:Content-Type:Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijr
     vQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4G
     d3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@example.org
Subject: [Lists] Example 1

Hey gang,
This is a test message.
--J.
```

A.3.2.2. Example 3, Step B: Message from list forwarded with source

The message is delivered to a mailbox at gmail.com
Processing at gmail.com:

- o gmail.com performs usual authentication checks
- o gmail.com adds Auth-Results: and Received: header
- o Determines that message fails DMARC
- o Checks for ARC-Seal: header; finds two
- o Validates the signature in the ARC-Seal (i=2): header, which covers the ARC-Authentication-Results: header
- o Validates the signature in the ARC-Seal (i=1): header, which covers the d1.example ARC-Message-Signature: header
- o Uses the ARC-Auth-Results: values, but:
- o Instead of delivering message, prepares to forward message per user settings
- o Applies usual DKIM signature
- o gmail.com adds it's own ARC-Seal: header, contents of which are
    - * version
    - * sequence number ("i=2")
    - * hash algorithm (SHA256 as example)
    - * timestamp ("t=")
    - * selector for key ("s=notary01")
    - * domain for key ("d=gmail.com")
    - * Note: algorithm requires only ARC-Seals with lower sequence # be included, in ascending order
    - * signature of the chain

Here's what the message looks like at this point:

Return-Path: <jqd@d1.example>

```
ARC-Seal: i=3; a=rsa-sha256; t=1421363253;
    s=notary01; d=gmail.com; cv=V;
    b=sjHDMriRZ0Mui5eVEOGscRHWbQHcy97lvrduHQ8h+f2CfIrxUiKOE44x3LQwD
     WRYbDjf5fcM9MdcIahC+cP59BQ9Y9DHwMDzwRTnM7NVb4kY+tSaVnLoIOaP9lF
     /suttxO+RRNr0fCFw==
ARC-Message-Signature: i=3; a=rsa-sha256;
    d=gmail.com; s=20120806;
    h=mime-version:content-type:x-original-sender
     :x-original-authentication-results:precedence:mailing-list
     :list-id:list-post:list-help:list-archive:sender
     :list-unsubscribe:reply-to;
    bh=2+gZwZhUK2V7JbpoO2MTrU19WvhcA4JnjiohFm9ZZ/g=;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz6
     1TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L
     69EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0Ab8Oi1ebYV/hIBm
     fhSLF1E80hMPcMijONfTQB6g5Hoh/kE6N2fgp6aSngL/WA3+g3Id8ElhXHvIGcJ
     RFeMKdJqiW5cxdqPTRW+BnR5ee6Tzg06kr265NTDIAU8p8fQNuLfZj49MMA+QwD
     BJtXwbQoZyRtb6X6q0mYaszUB8kw==
Received: by mail-yk0-f179.google.com with SMTP id 19so2728865ykq.10
    for <mailbox@gmail.com>; Thu, 14 Jan 2015 15:02:45 -0800 (PST)
Authentication-Results: i=3; gmail.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@example.org; dmarc=fail; arc=pass
ARC-Seal: i=2; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=V;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=2; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF1
     F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3A+
     m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=2; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
```

```
        (envelope-from jqd@d1.example)
   ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
       s=origin2015; d=d1.example; cv=N;
       b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
        TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
        EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
   ARC-Message-Signature: i=1; a=rsa-sha256;
       d=d1.example; s=20130426; t=1421363082;
       bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
       h=MIME-Version:CC:Content-Type:Content-Transfer-Encoding;
       b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYij
        rvQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD
        4Gd3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
   Message-ID: <54B84785.1060301@d1.example>
   Date: Thu, 14 Jan 2015 15:00:01 -0800
   From: John Q Doe <jqd@d1.example>
   To: arc@example.org
   Subject: [Lists] Example 1

   Hey gang,
   This is a test message.
   --J.
```

A.3.3. Example 3: Message received by Recipient

Let's say that the Recipient is example.com
Processing at example.com:

- example.com performs usual authentication checks

- example.com adds Auth-Results: header, Received header

- Determines that message fails DMARC

- Checks for ARC-Seal: header; finds three

- Validates the signature in the highest numbered ("i=2") ARC-Seal: header, which covers all previous ARC-Seal: and ARC-Authentication-Results: headers

- Validates the other ARC-Seal header ("i=2"), which covers the ARC-Authentication-Results: header

- Validates the other ARC-Seal header ("i=1"), which covers the d1.example ARC-Message-Signature: header

- example.com uses the ARC-Authentication-Results: values

Here's what the message looks like at this point:

```
Return-Path: <jqd@d1.example>
Received: from mail-ob0-f188.google.com (mail-ob0-f188.google.com
    [208.69.40.157]) by clothilde.example.com with ESMTP id
    d200mr22663000ykb.93.1421363268
    for <fmartin@example.com>; Thu, 14 Jan 2015 15:03:15 -0800 (PST)
Authentication-Results: clothilde.example.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@gmail.com; dmarc=fail; arc=pass
ARC-Seal: i=3; a=rsa-sha256; t=1421363253;
    s=notary01; d=gmail.com; cv=V;
    b=sjHDMriRZ0Mui5eVEOGscRHWbQHcy97lvrduHQ8h+f2CfIrxUiKOE44x3LQwDW
     RYbDjf5fcM9MdcIahC+cP59BQ9Y9DHwMDzwRTnM7NVb4kY+tSaVnLoIOaP9lF/s
     uttxO+RRNr0fCFw==
ARC-Message-Signature: i=3; a=rsa-sha256;
    d=gmail.com; s=20120806;
    h=mime-version:content-type:x-original-sender
     :x-original-authentication-results:precedence
     :mailing-list:list-id:list-post:list-help:list-archive:sender
     :list-unsubscribe:reply-to;
    bh=2+gZwZhUK2V7JbpoO2MTrU19WvhcA4JnjiohFm9ZZ/g=;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz6
     1TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L
     69EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0Ab8Oi1ebYV/hIBm
     fhSLF1E80hMPcMijONfTQB6g5Hoh/kE6N2fgp6aSngL/WA3+g3Id8ElhXHvIGcJ
     RFeMKdJqiW5cxdqPTRW+BnR5ee6Tzg06kr265NTDIAU8p8fQNuLfZj49MMA+QwD
     BJtXwbQoZyRtb6X6q0mYaszUB8kw==
Received: by mail-yk0-f179.google.com with SMTP id 19so2728865ykq.10
    for <mailbox@gmail.com>; Thu, 14 Jan 2015 15:02:45 -0800 (PST)
Authentication-Results: i=3; gmail.com; spf=fail
    smtp.from=jqd@d1.example; dkim=pass (1024-bit key)
    header.i=@example.org; dmarc=fail; arc=pass
ARC-Seal: i=2; a=rsa-sha256; t=1421363107;
    s=seal2015; d=example.org; cv=V;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz6
     1TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L
     69EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=2; a=rsa-sha256;
    d=example.org; s=clochette; t=1421363105;
    bh=FjQYm3HhXStuzauzV4Uc02o55EzATNfL4uBvEoy7k3s=;
    h=List-Id:List-Unsubscribe:List-Archive:List-Post:
     List-Help:List-Subscribe:Reply-To:DKIM-Signature;
    b=Wb4EiVANwAX8obWwrRWpmlhxmdIvj0dv0psIkiaGOOug32iTAcc74/iWvlPXpF1
     F5vYVF0mw5cmKOa824tKkUOOE3yinTAekqnly7GJuFCDeSA1fQHhStVV7BzAr3A+
     m4bwa6RIDgr3rOPJil678dZTHfztFWyjwIUxB5Ajxj/M=
Received: from segv.d1.example (segv.d1.example [72.52.75.15])
    by lists.example.org (8.14.5/8.14.5) with ESMTP id t0EKaNU9010123
```

```
    for <arc@example.org>; Thu, 14 Jan 2015 15:01:30 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Authentication-Results: i=2; lists.example.org;
    spf=pass smtp.mfrom=jqd@d1.example;
    dkim=pass (1024-bit key) header.i=@d1.example;
    dmarc=pass
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
ARC-Seal: i=1; a=rsa-sha256; t=1421363107;
    s=origin2015; d=d1.example; cv=N;
    b=pCw3Qxgfs9E1qnyNZ+cTTF3KHgAjWwZz++Rju0BceSiuwIg0Pkk+3RZH/kaiz61
     TX6RVT6E4gs49Sstp41K7muj1OR5R6Q6llahLlQJZ/YfDZ3NImCU52gFWLUD7L69
     EU8TzypfkUhscqXjOJgDwjIceBNNOfh3Jy+V8hQZrVFCw0A=
ARC-Message-Signature: i=1; a=rsa-sha256;
    d=d1.example; s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=MIME-Version:To:CC:Subject:Content-Type:Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijr
     vQwbv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4G
     d3TRJlgotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: arc@example.org
Subject: [Lists] Example 1

Hey gang,
This is a test message.
--J.
```

Appendix B. Acknowledgements

This draft is the work of OAR-Dev Group.

The authors thank all of the OAR-Dev group for the ongoing help and though-provoking 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.

Grateful appreciation is extended to the people who provided feedback through the discuss mailing list.

Appendix C. Comments and Feedback

Please address all comments, discussions, and questions to arc-discuss@dmarc.org [1][mailto:arc-discuss@dmarc.org].

Appendix D. Historical Note

The ARC-Authentication-Results header is a direct copy of the normal Authentication-Results header ([RFC7601]) used in a similar fashion as that proposed in [OAR] but has the instance (i=) value added to provide correlation within the set of ARC headers.

Authors' Addresses

OAR-DEV Group

Email: arc-discuss@dmarc.org

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

Email: kurta@linkedin.com

John Rae-Grant (editor)
Google

Email: johnrg@google.com

Brandon Long (editor)
Google

Email: blong@google.com

J. Trent Adams (editor)
Paypal

Email: trent.adams@paypal.com

Steven Jones (editor)
TDP

Email: smj@crash.com