Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Email Authentication Recommended Best Practices

September 2020

The reference URL for this document is:
https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf

For information on M3AAWG please see www.m3aawg.org.

Table of Contents

1. Abstract

This document recommends a set of best practices for authenticating email messages using the security protocols Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance) DMARC and Authenticated Received Chain (ARC). (Another security protocol, SMTP authentication, meaning the presentation of credentials during the submission of a message by a Mail User Agent (MUA) or Mail Submission Agent (MSA) to a Mail Transfer Agent (MTA) serves a different purpose and is outside the scope of this document.)

This document is not meant to instruct; rather, it presents a checklist of technical requirements that are binary in nature (i.e., they either are or are not implemented), and are consistently applied throughout the ecosystem. For clarity, this document will cite and link to other existing documents rather than covering topics in depth here.

The primary intended audience for this document includes mail operators acting as origination senders, intermediaries (e.g., forwarding services and mailing lists) and receivers (or mailbox providers), but it can be useful for any site handling email.

2. Introduction

The problem of whether or not an email recipient can trust that a message is really from its purported sender has continued to vex operators. Several methods for establishing the authenticity of an email message have been developed, and a handful are in common usage as of this writing, but that usage is not uniform across the email ecosystem.

Proper email authentication is a foundational principle for establishing trust in email and protecting a domain's reputation. If an email passes authentication checks, the receiving domain can apply policy to that email in keeping with the reputation already established for the identities associated with those authentication checks, and the recipient can be assured that those identities are valid.

In addition, mailbox providers regularly speak of a possible email authentication future with the catchphrase "No auth, no entry." There may come a day when an email message will have to pass one or more authentication checks to be considered for delivery to its intended recipient.

To increase trust in email in the present and provide for such a mandate in the future, M³AAWG is publishing this recommended set of best practices for email authentication. In this document, the reader will find guidance that will not only establish trust in email and protect a domain's reputation, but should also pass muster with any "No auth, no entry" standard that may develop in the future.

The goal of these guidelines is to protect the organizational domain as defined in RFC 7489. Specifically, these guidelines target the organizational domain associated with the domain that the message recipient will see in the message body "From:" header, i.e., the RFC5322.From header. This is the domain that will be most closely associated with the email message by the recipient. This implies a reliance on DMARC for email authentication, since DMARC is designed to protect this organizational domain in ways that SPF and DKIM do not.

3. Scope

This document will focus on the following four email authentication protocols, and include references to external documents that will be useful to the reader. The authors recommend that readers familiarize them-

selves with the M³AAWG document "Trust in Email Begins with Authentication" as a background to the information presented here.

SPF (Sender Policy Framework) RFC 7208

SPF is a mechanism that allows domain owners to publish and maintain, via a standard DNS TXT record, a list of systems authorized to send email on their behalf.

DKIM (Domain Keys Identified Mail) RFC 6376

DKIM allows an organization to claim responsibility for transmitting a message in a way that can be validated by the recipient.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) RFC 7489

DMARC is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting that a mail-receiving organization can use to improve mail handling.

ARC (Authenticated Received Chain) RFC 8617

The ARC protocol provides an authenticated chain of custody for a message, allowing each entity that handles the message to identify what entities handled it previously as well as the message's authentication assessment at each hop. ARC is not yet an internet standard, but adoption is increasing.

4. Executive Summary: A Checklist

The following table is presented for the reader seeking a one-page summary of recommended authentication practices. Justification and discussion for each of these recommendations follows.

Actor	Recommended Authentication Practices

Sender	• SPF
	  ○ Publish SPF records for MAIL FROM and EHLO domains.
	  ○ SPF records should end in "~all".
	  ○ SPF records should not authorize more IPs than necessary.
	  ○ MAIL FROM domains should align with RFC5322.From domains where possible.
	  ○ Publish SPF "-all" on domains that do not send mail.
	• DKIM
	  ○ Sign all outbound mail with a domain that aligns with the RFC5322.From domain.
	  ○ Follow best practices for key management.
	• DMARC
	  ○ Policy statements should be "p=reject" where possible, "p=quarantine" otherwise.
	  ■ "p=none", "sp=none", and pct<100 should only be viewed as transitional states, with the goal of removing them as quickly as possible.
	  ○ DMARC policy records should include a rua tag.

Intermediary	• Implement ARC. • Generate DMARC reports.
Receiver	• Perform SPF, DKIM, and DMARC authentication checks. • Honor DMARC policies. • DMARC pass overrides SPF Fail Verdict ○ except when SPF record is "v=spf1 -all". • Send DMARC reports. • Make use of ARC header in received messages.

5. Authentication Recommendation Discussion

The following recommendations are presented as best practices for authentication for each of three classes of entities in the email ecosystem. Each entity is briefly defined.

5.1. Senders

Senders (labeled in RFC 5598 as Authors or Originators) is the traditional term used by M³AAWG membership to refer to the origination point for email messages. For the purposes of this document, this term can include brand owners, mailbox providers, and email service providers (ESPs), but does not apply to end users sending person-to-person email, unless such end users are also domain or brand owners. Practices in this section are to be applied to messages starting their journey to their destination mailbox(es).

SPF

SPF records should be published for any domain used in an RFC5321.From (MAIL FROM) command and for any domain used as an SMTP HELO/EHLO identity for any server sending mail. M³AAWG's Best Practices for Managing SPF Records is a comprehensive resource for what to do here, but several points there must be stressed:

- Ensure that your SPF record is valid, and that it conforms to the DNS Lookup Limits specified in RFC 7208.
- SPF records should end in ~all.
- SPF records should not authorize more IPs than necessary; the smallest possible netblock(s) for IPs authorized to send on behalf of the domain should be used.
- Domains that do not send email should have published SPF "v=spf1 -all" records, per M³AAWG Protecting Parked Domains Best Common Practices.

DKIM

Any domain-based reputation system requires a reliable method for establishing and confirming the identity of the domain(s) taking responsibility for a given email message, and DKIM is the best method available for that at the moment. As such, M3AAWG recommends the following practices for DKIM:

- Sign all outbound mail with a DKIM key that aligns with the domain of the RFC5322.From header.
  - ESPs should strongly consider double-signing with their own domain as well, to allow separate reputation assessments based on each of the domain names.
  - ESPs should use distinct DKIM keys for each customer.
- Sign a reasonable set of header fields, using section 5.4.1 of RFC 6376 as a guideline.
- Follow M³AAWG recommendations for public key management:
  - DKIM Key Rotation Best Common Practices
  - Best Practices To Avoid Key Length Vulnerability

DMARC

A DMARC policy record allows a domain to announce that their email uses authentication; provides an email address to gather feedback about the use of their domain; and specifies a requested policy for the handling of messages that do not pass authentication checks.

- M³AAWG recommends that the policy statement for domains publishing DMARC records be "p=reject".
- M³AAWG recognizes that achieving the above can present operational challenges to some domains; a policy of "p=quarantine" should be considered in other circumstances.

Organizations should consider their particular risk profile relative to active or potential spoofing and phishing of their domain. Policy should be set for balance between protection benefits of a "reject" or "quarantine" policy setting and the potential loss of legitimate mail due to missing or broken signing.

- Any published DMARC policy record, even one with a policy statement of p=none, should include, at a minimum, a rua tag that points to a mailbox for receiving DMARC aggregate reports.
    - The rua tag specifies the destination mailbox(es) for DMARC aggregate reports. These reports are sent by receivers that perform DMARC validation, and contain statistical data on messages seen by the receivers that purport to be from the domain that published the DMARC policy record.
    - Without the ability to receive and process reports, the domain owner cannot know whether or not it is safe to move from p=none to stricter policies, because the domain owner will have no ability to know if all of its legitimate mail is properly authenticated.
- It is generally accepted that, given privacy concerns and the need for redaction of what might be personally identifiable information (PII), DMARC failure reports are neither sent by most receivers nor terribly useful to most domain owners. For that reason, the inclusion of a ruf tag in the DMARC policy record is optional.
    - Neither the rua mailbox(es) nor the ruf mailbox(es) should send replies when receiving a report.

5.2. Intermediaries

This document uses the term "intermediaries" as a catch-all for the RFC 5598 terms Mediators, Relays, or Gateways; examples of these would be forwarding services and mailing list or other discussion group servers. It is also possible for a mailbox provider or other site to function as an intermediary for any given message even when that is not its primary function, as it is not at all uncommon for a mailbox to be configured to forward all mail to another mailbox at a different domain. The design of the SPF, DKIM and DMARC protocols is such that final authentication checks at the receiving service can fail in some cases even though messages have passed through intermediaries. While M³AAWG recognizes that there may be significant resource cost involved, it nonetheless calls upon intermediaries to take steps to minimize the risk of such failures in order to ensure that mail continues to flow as intended. Specifically:

- **Minimize changes to message in transit**

  Authentication checks are dependent on either the content of the headers of the message, and/or the message body. Messages that would pass authentication checks when sent directly from the origination point to the final destination can fail those same checks if they are altered by intermediaries in transit. While M³AAWG recognizes that alteration may be unavoidable for intermediaries such as mailing list servers, it nevertheless recommends that such alteration be kept to a minimum.

- **Mitigate the risk of authentication failures**

  In some cases an intermediary must make alterations to a message that are likely to cause authentication checks to fail at subsequent hops for the message, with such failures likely to cause the message to not be delivered. The intermediary should take steps to mitigate this risk. A common example of such mitigation would be when a mailing list server which adds a header or footer to each list post rewrites the From header, usually following logic something like this:

  - List member sends message to list from address john.jones@dmarc.domain.tld
  - Mailing list software notes that dmarc.domain.tld publishes a DMARC policy
  - Mailing list software rewrites From header to something like john.jones=40dmarc.-domain.tld@list.domain, thereby eliminating the risk of a DMARC failure for the message.

- **Implement ARC**

  ARC provides the ability to record authentication results at each hop of a message's path and requires no changes to the content of the message. ARC can protect against authentication failures at subsequent hops, failures that are due to the message's having passed through the intermediary in the first place.

  - Implied in this recommendation to implement ARC is to also perform the authentication checks (SPF, DKIM, and DMARC) for which results are captured in the ARC-Authentication-Results header.

- **Generate DMARC Reports**

  Intermediaries should generate and send DMARC aggregate reports. See below for more on this topic.

5.3. Receivers

This document defines receivers as those domains that will accept and store a message for reading, foldering, deleting, etc., by its recipient(s), and not the individual recipients of the messages themselves. Within M³AAWG, the terms "receiver" and "mailbox provider" have become synonymous over the years, but since a high percentage of email terminates at domains that are not traditional mailbox providers, the more generic term "receiver" is used here.

These mechanisms recommended here are likely to be increasingly required. However they may be beyond the skill level of some IT departments, especially at smaller domains, but as more businesses move their email to cloud hosting services, M³AAWG calls upon those services to implement these recommendations.

- **Perform authentication checks**

  Obviously, a "No auth, no entry" policy requires that authentication checks be done, but not all receivers have signed on to this idea yet. Whether or not a receiver adopts this posture, M³AAWG believes that checking authentication (SPF, DKIM, and DMARC) on inbound mail and using the results of these checks to inform acceptance and filtering decisions is a best practice for protecting mailbox holders from some forms of fraudulent email.

- **Honor DMARC policies**

  If a domain publishes a DMARC policy, especially one of p=reject, the recipient expects that messages which pass DMARC checks can be trusted to be from the domain shown in the From: line. In such cases, a receiver who refuses to honor the published policy on a

DMARC failure chips away at that trust, risking a negative impact to both the brand and the receiver. Policy overrides should be both a) relatively infrequent and b) clearly justified and documented via the aggregate reporting policy override and comment functionality.

- **A DMARC pass overrides an SPF fail verdict...**

  Because a DMARC pass requires only a DKIM **or** SPF pass (with proper domain alignment) and because it's not uncommon for a Return-Path (RFC5321.From) domain to not align with the header From (RFC5322.From) domain, an SPF Fail verdict (which occurs when the SPF record ends in "-all" and the SPF check does not pass) should not result in a message rejection until after DMARC has been evaluated and been found to not pass.

- **...except if "v=spf1 -all"**

  The only exception to the above is when an SPF record indicates no allowed use, specifically "v=spf1 -all"; in that case, if the receiver (or intermediary) wishes to take preemptive action on the SPF failure, it may.

- **Send DMARC aggregate reports**

  The reporting component of DMARC is a valuable tool for domain owners that publish DMARC policy, as such reports help them tighten up their email authentication whether or not they move toward a policy of p=reject. Without reports, they cannot identify legitimate mail streams that aren't authenticating, or get a picture of how frequently others try to impersonate their brand or even use it legitimately (e.g., a poorly configured vendor). While a number of large mailbox providers that do DMARC validation have made the decision that sending aggregate reports does not conflict with existing privacy laws, M³AAWG recommends that entities sending reports take into consideration current legal opinions regarding such laws.

- **Make use of ARC headers**

  If a message with one or more sets of ARC headers arrives at a receiver, the receiver should consider the information in those header sets as part of the final authentication verdict and subsequent disposition of the email.

6. Conclusion

M³AAWG believes that proper email authentication is a foundational principle for establishing trust in email, and domain-based authentication requires it. This document spells out M³AAWG best practices for domain-based authentication practices that will not only protect the organizational domain for any mail message, but also suffice for any future "No auth, no entry" practice that becomes standard in the email ecosystem. M³AAWG encourages its members to implement these practices to the fullest practical extent as soon as they are able to do so.

7. References

RFC Standards

RFC 5598 Internet Mail Architecture
https://tools.ietf.org/html/rfc5598#section-2.2.1(originator)

RFC 6376 DomainKeys Identified Mail (DKIM) Signatures
https://tools.ietf.org/html/rfc6376

RFC 7208 Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1

https://tools.ietf.org/html/rfc7208

RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC)
https://tools.ietf.org/html/rfc7489#section-3.2

RFC 8617 The Authenticated Received Chain (ARC) Protocol
https://tools.ietf.org/html/rfc8617

M³AAWG Best Practices Documents

M³AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability rev. July 2017
https://www.m3aawg.org/sites/default/files/m3aawg-key-implementation-bp-revised-2017-07.pdf

M³AAWG Best Practices for Managing SPF Records
https://www.m3aawg.org/sites/default/files/m3aawg_managing-spf_records-2017-08.pdf

M³AAWG DKIM Key Rotation Best Common Practices rev. March 2019
https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

M³AAWG Protecting Parked Domains Best Common Practices rev. Dec. 2015
https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

M³AAWG Trust in Email Begins with Authentication
https://www.m3aawg.org/sites/default/files/document/M3AAWG_Email_Authentication_Update-2015.pdf

Other References

DomainKeys Identified Mail Teaser
http://www.dkim.org/info/DKIM-teaser-03.pdf

Report on the Compliance of DMARC with the EU GDPR
https://certified-senders.org/wp-content/uploads/2018/08/Report_DMARC_and_GDPR.pdf

---

As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates.

M3AAWG-134