M^{3}AAWG Technology Summaries

Email Authentication

September 2023

The reference URL for this document is https://www.m3aawg.org/ts_emailauthentication

What email authentication is:

Email authentication involves one or more technical processes used by sending and receiving mail systems to verify the email originated with an authorized domain name server and is received in a valid format. Email authentication creates signals about the mail that can be used in spam filtering and other mail handling decisions, and may even point to fraudulent senders.

Two widely used email authentication protocols are Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM). Both SPF and DKIM provide information used by the receiving domain to verify the sender of the message was authorized by the sending domain. DKIM can also determine if the content received is the same as it was when sent.

Domain-based Message, Reporting, and Conformance (DMARC) is a protocol that is layered on top of SPF and DKIM. DMARC helps receiving domains decide how best to handle messages that fail authentication.

What email authentication does:

- Email authentication associates an identity (usually a domain name) with an email message by verifying key information that indicates the identity handled the message in some way.
- The identity informs how the message is processed. For instance, if the domain has a poor reputation (frequently associated with spam), the system may classify the message as spam.
- A single message might be associated with multiple identities, each separately authenticated, that are used to inform the processing of the message.

What email authentication does not do:

- Email authentication does not attest to the authenticity or quality of the message's content or ensure that the message is "good" or "legitimate."
- Email authentication makes no statement about what entity actually wrote the message.
- Email could fail authentication for legitimate reasons such as mail server configuration or syntax errors. Failed authentication by SPF or DKIM is equivalent to–and is no worse than–the absence of authentication, absent other indications (such as DMARC).

References:

RFC 6376, "DomainKeys Identified Mail (DKIM) Signatures"
RFC 7208, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1"
RFC 7489, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)"
"M^{3}AAWG Email Authentication Recommended Best Practices"

As with all documents that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates.