M³AAWG Technology Summaries

Domain Keys Identified Mail (DKIM)

September 2023

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

What DKIM is:

DKIM is an email authentication protocol that creates an association between a domain and the messages it sends using digital signatures. A sequence of messages signed with the same domain name is assumed to provide a reliable base of information about mail associated with the domain name's owner, which may feed into an evaluation of the domain's reputation.

What DKIM does:

- DKIM associates a domain name with the message in a DKIM-Signature: header field. Multiple signatures are allowed. The association is done by validating a digital signature that covers parts of the message.
- Receiving servers use the digital signature to validate the sender's authenticity and to identify if the message headers and content that are covered by the signature have been modified since the signature was created.
- A failed DKIM signature is ignored and is not further considered in any way. A failed signature does not count against the message's evaluation.
- The DKIM signature validation typically survives basic email relaying, and some types of re-postings where the covered parts are not altered. Mailing lists typically alter the message in ways that make DKIM validation fail.

What DKIM does not do:

- DKIM does not attest to the authenticity or quality of the message's content and does not ensure that the message is "good" or "legitimate".
- DKIM validation will not survive modification to the covered header fields or to the message's main body. A mailing list, for example, will often put a prefix on the message's Subject header field, or will add a footer to the message body.
- A failed DKIM validation does not necessarily signal malicious or bad activity.

References:

RFC 6376, "DomainKeys Identified Mail (DKIM) Signatures"
RFC 6377, "DomainKeys Identified Mail (DKIM) and Mailing Lists"

"M3AAWG Email Authentication Recommended Best Practices"
"M3AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability"
"M3AAWG DKIM Key Rotation Best Common Practices"

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