NIST Technical Note 1945

Email Authentication Mechanisms: DMARC, SPF and DKIM

Stephen Nightingale

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.1945

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Technical Note 1945

Email Authentication Mechanisms: DMARC, SPF and DKIM

Stephen Nightingale
High Assurance Domains Project
Advanced Network Technology Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.1945

February 2017

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authentication messages contain copious detail with results of all the various mechanisms. The plain text email messages from each of these sources are consequently structured under a series of relevant headings. Thus, Pythentic reply messages start with a Summary of Results section, and continue with the SPF analysis, the fully recursive listing of SPF records, and so on. The labels in Table 5-1 represent these headings, for each authenticator.

Return Path is the closest in function to Pythentic. It provides SPF, DKIM and DMARC results, with the DMARC DNS record analysed. SPF and DKIM alignment results are additionally itemized. The SPF and DKIM records are not analyzed, and Return Path does not provide a summary of results, nor does it incorporate individual protocol results in SMTP headers, in contrast with the X-headers that Pythentic provides to the message recipient.

Port 25 provides SPF check details, DKIM check and DKIM record. There is no DMARC analysis, nor is there a fully recursive SPF record check. Port 25 has additional tests, for the Domain Keys protocol, a predecessor of DKIM, for Sender ID, an experimental alternative to SPF, and also for Spam Assassin. Some discussion of these additional mechanisms is called for here.

> **Domain Keys** [RFC4870]: Provides authentication by signing email at the Admin boundary, with the signature placed in an SMTP header. The public key is retrieved from the DNS, and no certificates are needed. Domain Keys is used for source domain authentication, but there is no role for man-in-the-middle modification checking. RFC4870 has been rendered historic by the IETF, as it is effectively obsoleted by DKIM.
>
> **Sender ID** [RFC4406]: Sender ID is an alternative to SPF that provides a test for spoofing of email domains. This protocol validates the Purported Responsible Address and the Return Path, and receivers should perform at least one of those two tests. The sending domain publishes SPF v2.0 records, which include policy stipulations. RFC4406 has been designated Experimental, and the IESG cautions that it should not be used in parallel with SPF.
>
> **Spam Assassin**[18]: includes recognition of SPF and DKIM checks. This is a Spam filter that uses Bayesian classification together with configurable static rules, to filter Spam. Individually scored, each rule may have a positive or negative score. Any message that cumulatively scores more than 5 points is regarded as spam and is recommended for discard.

Unlock the Inbox: covers a wider range of authentication than all of the above message reflectors. Still, it is not a complete superset of Pythentic. While Unlock the Inbox offers SPF, DKIM and DMARC checks and some of the DNS records, it does not perform the SPF record check – and certainly not the fully recursive check that Pythentic offers.

[18] http://spamassassin.apache.org.