

E-mail authentication

MX, SPF, DKIM and DMARC: what each check can tell you.

MX: inbound routing

MX identifies the servers that receive mail for a domain. Lower preference values are tried first. MX does not authorise outbound senders or prove that a mailbox exists. A Null MX explicitly says the domain accepts no e-mail.

SPF: sending infrastructure

SPF checks the connecting IP against the envelope sender domain, or HELO identity where applicable. Publish one SPF policy at a name. A policy can span several TXT character strings.

SPF essentials

ip4 / ip6 authorise address ranges.

include incorporates another policy.

redirect= delegates policy evaluation.

-all fail; **~all** softfail; **?all** neutral; **+all** authorises everyone.

SPF limits DNS-query-causing terms to 10 across evaluation, including nested policies. This is not simply a count of TXT queries.

DKIM: message signatures

Read **d=** (signing domain) and **s=** (selector) from DKIM-Signature. The public key is at **selector._domainkey.domain**. Finding a key does not prove a particular message has a valid signature.

DMARC: authentication plus alignment

DMARC passes when at least one of SPF or DKIM passes and aligns with the visible From domain. SPF alignment uses the authenticated envelope sender domain; DKIM alignment uses **d=**. Relaxed and strict alignment apply different domain matching rules.

Read the policy

Query **_dmarc.example.com TXT**.

p=none requests monitoring.

p=quarantine requests suspicious treatment.

p=reject requests rejection.

rua= specifies aggregate reporting destinations.

A receiver can apply local policy. Do not enforce a stricter policy until legitimate senders have been checked.

Quick queries

`dig example.com MX +short`

Inbound mail servers.

`dig example.com TXT +short`

Find the SPF policy.

`dig selector1._domainkey.example.com TXT`

Replace selector1 with the actual selector.

`dig _dmarc.example.com TXT +short`

Read the published DMARC policy.

Diagnose a real message

Use authentication results from a trusted receiving system. Compare the visible From domain, envelope sender and DKIM signing domains. Forwarding may break SPF; message changes may break DKIM. DNS-only checks do not replace a real delivery test.