An email consists of:

- **mandatory headers**
  - “From “, “Date: “

- **optional headers**
  - “From: “, “To: “, “Subject: “, ...

- **content of the message**
  - content independent of SMTP
  - Multipurpose Internet Mail Extensions (MIME) enables non-ascii, multipart, encodings, ...

A much more bare-bones email.
Back in the old days, any SMTP MTA would accept and relay mail from anybody for anybody.

This lead to a lot of abuse; today, most mail servers only accept mail for domains they consider themselves responsible for.

There are a few so-called “open relays” still operating on the internet, but reputation-based Spam detection systems diminish their usefulness.
SMTP provides no authenticity guarantees whatsoever.

- "From " can be set to anything
- "From: “ can be different from "From "

- The receiver can decide who it will accept (relay) mail for, but how can the receiver decide who should be allowed to send mail from?
SPF Hard Fail

Authentication-Results: spf=fail (sender IP is 54.80.35.155)
smtp.mailfrom=microsoft.com; stevens.edu; dkim=none (message not signed)
header.d=none;stevens.edu; dmarc=fail action=reject
header.from=microsoft.com;

Received-SPF: Fail (protection.outlook.com: domain of microsoft.com does not designate 54.80.35.155 as permitted sender)
receiver=protection.outlook.com;
client-ip=54.80.35.155; helo=localhost;

SPF Soft Fail

Authentication-Results: spf=softfail (sender IP is 54.80.35.155)
smtp.mailfrom=obama.org; stevens.edu; dkim=none (message not signed)
header.d=none;stevens.edu; dmarc=fail action=reject
header.from=obama.org;

Received-SPF: SoftFail (protection.outlook.com: domain of transitioning obama.org discourages use of 54.80.35.155 as permitted sender)
This mail will be forwarded by Stevens to my personal mail server.
From: Michelle Obama <michelle@obama.org>
To: Jan Schaumann <jschauma@netmeister.org>
Subject: Friday

Jan,
I’m afraid Barack has to cancel. He has other obligations that night.

Michelle

From: Michelle Obama <michelle@obama.org>
To: Jan Schaumann <jschauma@netmeister.org>
Subject: Friday

Jan,
I’m afraid Barack has to cancel. He has other obligations that night.

Michelle

From: Barack Obama <barack@obama.org>
To: Jan Schaumann <jschauma@netmeister.org>
Subject: Friday

Yo,
Party at my place, 6pm.
BYOB.

-B

Authentication-Results: spf=softfail (sender IP is 54.80.35.155)
smtph.mailfrom=obama.org; stevens.edu; dkim=none (message not signed)
header.d=none; stevens.edu; dmarc=fail action=reject
header.from=obama.org;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
obama.org discourages use of 54.80.35.155 as permitted sender)
DomainKeys Identified Mail aka DKIM

DKIM can help detect email spoofing by providing a *digital signature* across parts of the message.

- combines efforts by Yahoo ("enhanced DomainKeys") and Cisco ("Identified Internet Mail")
- original RFC4871, 2007; current RFC6376
- adds *DKIM-Signature* headers
- more DNS TXT records (<s>._domainkey.<domain>)
DKIM Signature includes:

- the domain responsible (d=...)
- a “selector” to identify the correct public key (s=...)
- the hash of the email body (bh=...)
- the signed header fields (h=...)
- the actual signature data (b=...)

For validation, retrieve the correct public key via the DNS by combining the selector, the string “_domainkey”, and the domain.
Domain-based Message Authentication, Reporting and Conformance

DMARC (RFC7489) provides a policy of which validation mechanisms should be employed for a given domain.

- uses SPF and DKIM
- extends across “From “ and “From:” alignment
- provides report mechanism
- more DNS TXT records (_dmarc.<domain>)
• SPF checks that SMTP MAIL FROM is authorized; DMARC ensures alignment with “From:”

• DKIM allows parts of the message to be signed; DMARC allows the domain owner to specify what to do if e.g., the signature is wrong

• DMARC allows for aggregate reports of failed attempts
Summary

• SMTP headers:
  • some are mandatory, some optional
  • lack of some may be used as a signal of spamminess
  • each hop may add additional headers

• SPAM protections:
  • recipient restrictions (no open relays)
  • sender IP reputation (e.g., via DNS lookups in community databases)
  • Sender Policy Framework (SPF) specifies who is authorized to send mail on a domain’s behalf
  • DomainKeys Identified Mail (DKIM) signs parts of the mail
  • DMARC lets responsible domain specify what recipients should do upon mismatches
E-Mail Service Implications

• spam protections
• phishing protections
• high volume traffic demands fine-tuned systems
• high volume traffic implications on logging
• mail delivery cannons for notifications vs. spam lists
• outsourcing versus in-house
• privacy considerations
Links

• Sender Policy Framework: http://www.open-spf.org/
• DomainKeys Identified Mail (DKIM): http://www.dkim.org/
• Domain-based Message Authentication, Reporting & Conformance: https://dmarc.org/
• https://en.wikipedia.org/wiki/Authenticated_Received_Chain
• https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf
• https://postmaster.verizonmedia.com/faq