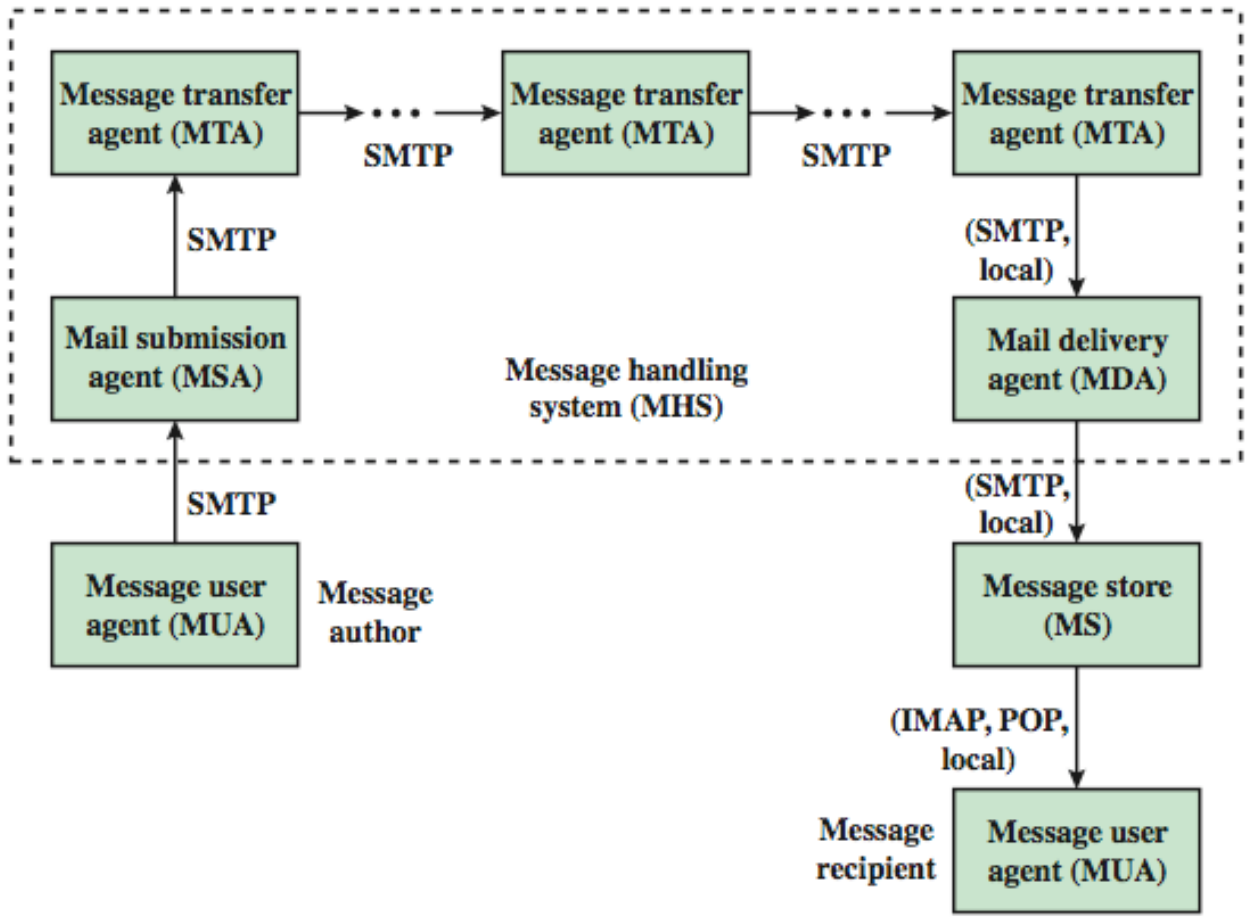
4.3 Domain Keys Identified Mail

- Domain Keys Identified Mail (DKIM) is a specification for cryptographically signing email messages, permitting a signing domain to claim responsibility for a message in the mail stream.
- Message recipients (or agents acting in their behalf) can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.
- DKIM is a proposed Internet Standard (RFC 4871: DomainKeys Identified Mail (DKIM) Signatures). DKIM has been widely adopted by a range of email providers, including corporations, government agencies, gmail, yahoo, and many Internet Service Providers (ISPs).

Internet Mail Architecture



- To understand to operation of DKIM, it is useful to have a basic grasp of the Internet mail architecture.
- At its most fundamental level, the Internet mail architecture consists of a user world in the form of Message User Agents (MUA), and the transfer world, in the form of the Message Handling Service (MHS), which is composed of Message Transfer Agents (MTA).
- A MUA is usually housed in the user's computer, and referred to as a client email program, or on a local network email server.
- The MHS accepts a message from one User and delivers it to one or more other users, creating a virtual MUA-to-MUA exchange environment.
- The MSA accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards.
- This function may be co-located with the MUA or be a separate functional model.
- In the latter case, the Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.
- The MTA relays mail for one application-level hop. Relaying is performed by a sequence of MTAs, until the message reaches a destination MDA.
- The MDA is responsible for transferring the message from the MHS to the MS. An MS can be located on a remote server or on the same machine as the MUA.
- Typically, an MUA retrieves messages from a remote server using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).
- Also an administrative management domain (ADMD) is an Internet email provider.
- The Domain Name System (DNS) is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address.

DKIM Strategy

- DKIM is designed to provide an email authentication technique transparent to the end user.
- In essence, a user's email message is signed by a private key of the administrative domain from which the email originates.

- The signature covers all of the content of the message and some of the RFC 5322 message headers.

- At the receiving end, the MDA can access the corresponding public key via a DNS and verify the signature, thus authenticating that the message comes from the claimed administrative domain.

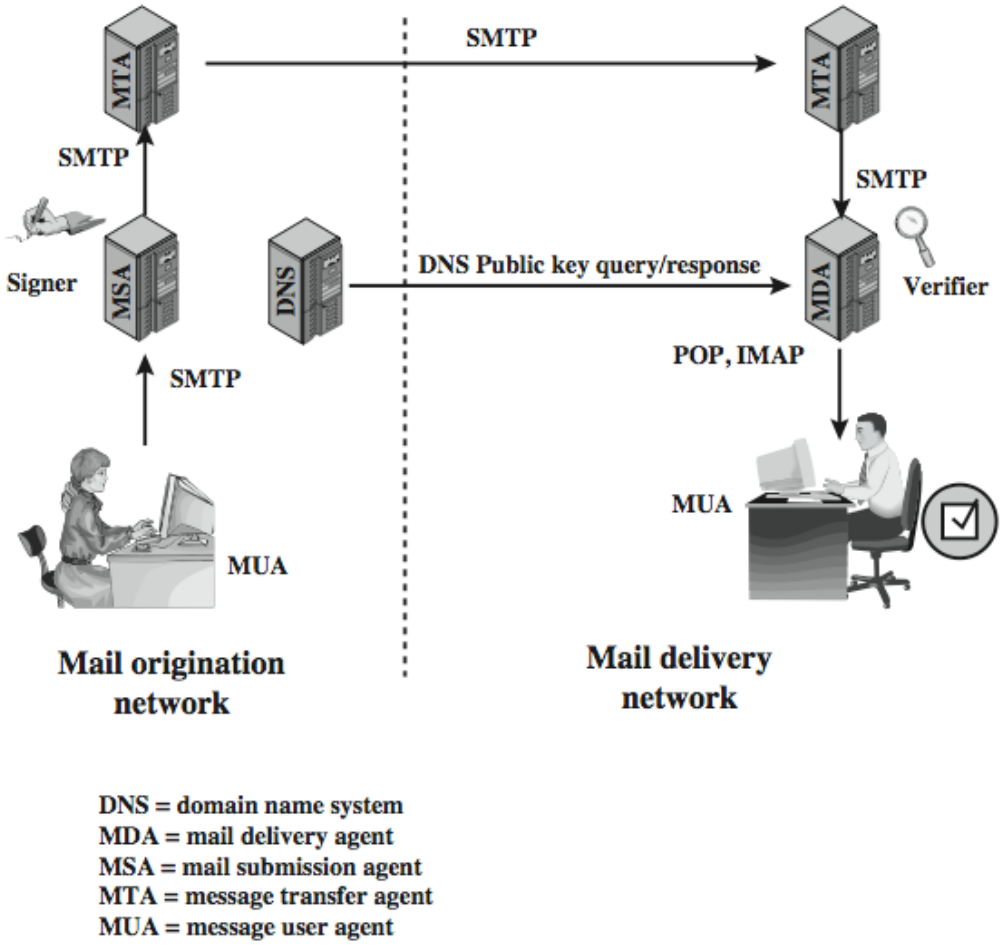
- Thus, mail that originates from somewhere else but claims to come from a given domain will not pass the authentication test and can be rejected.

- This approach differs from that of S/MIME and PGP, which use the originator's private key to sign the content of the message, for various pragmatic reasons Figure shows a simple example of the operation of DKIM. An email message is generated by an email client program.

- The content of the message, plus selected RFC 5322 headers, is signed by the email provider using the provider's private key.

- The signer is associated with a domain, which could be a corporate local network, an ISP, or a public email facility such as gmail.

- The signed message then passes through the Internet via a sequence of MTAs. At the destination, the MDA retrieves the public key for the incoming signature and verifies the signature before passing the message on to the destination email client.
- The default signing algorithm is RSA with SHA-256. RSA with SHA-1 may also be used.

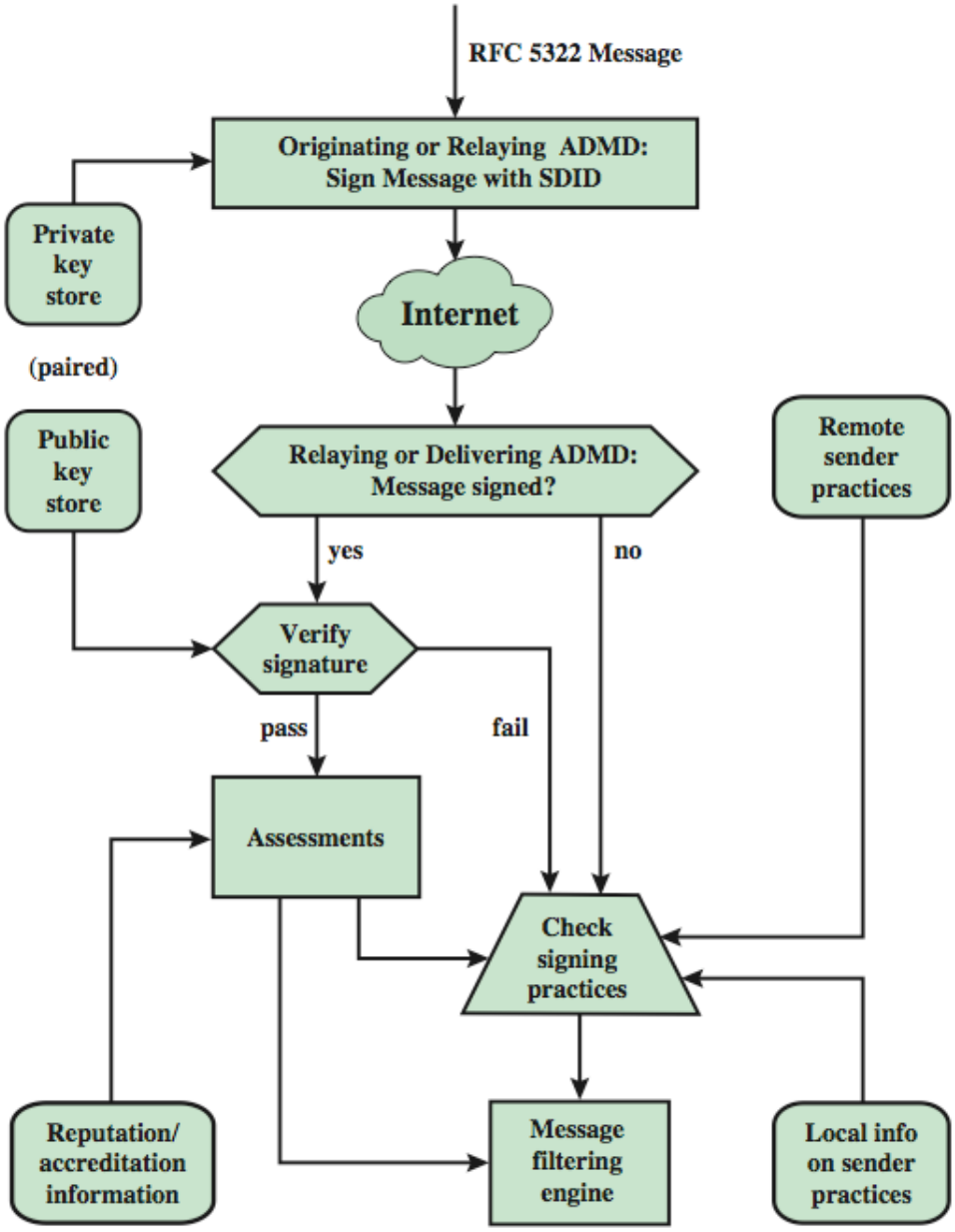


DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

- In essence, a user's e-mail message is signed by a private key of the administrative domain from which the e-mail originates.
- At the receiving end, the MDA can access the corresponding public key via a DNS and verify the signature, thus authenticating that the message comes from the claimed administrative domain.

- Thus, mail that originates from somewhere else but claims to come from a given domain will not pass the authentication test and can be rejected.

DCIM Functional Flow



- Figure provides a more detailed look at the elements of DKIM operation. Basic message processing is divided between a signing Administrative Management Domain (ADMD) and a verifying ADMD.
- Signing is performed by an authorized module within the signing ADMD and uses private information from a Key Store.

- Verifying is performed by an authorized module within the verifying ADMD. The module verifies the signature or determines whether a particular signature was required.
- Verifying the signature uses public information from the Key Store. If the signature passes, reputation information is used to assess the signer and that information is passed to the message filtering system.
- If the signature fails or there is no signature using the author's domain, information about signing practices related to the author can be retrieved remotely and/or locally, and that information is passed to the message filtering system.
- The signature is inserted into the RFC 5322 message as an additional header entry, starting with the keyword DKIM-Signature.
- Before a message is signed, a process known as canonicalization is performed on both the header and body of the RFC 5322 message.
- Canonicalization is necessary to deal with the possibility of minor changes in the message made route. The signature includes a number of fields, as listed in the text.