BSCIT

Network Security

Unit 6

Electronic Mail Security

Unit 6

Electronic Mail Security

3 Topics

1. Pretty Good Privacy (PGP)
2. S/MIME
3. Domain Keys Identified Mail (DKIM)

1. Pretty Good Privacy (PGP)

- Authentication -> SHA/RSA
- Confidentiality -> DES / Diffie Hellman
- Compression
- E-mail Compatibility -> Radix64

2. S/MIME (Secure MIME)

- Multipurpose Internet Mail Extensions
  - Allowed media types to be encoded in emails
- S/MIME is very similar to PGP.
- Both offer the ability to sign and/or encrypt messages.

S/MIME Functions

Create a message digest to be used in forming a digital signature.

Encrypt message digest to form a digital signature.

Encrypt session key for transmission with a message.

Encrypt message for transmission with a one-time session key.

Create a message authentication code.

3. Domain Keys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream.

Internet Mail Architecture

- Message User Agent (MUA)
- Mail Submission Agent (MSA)
- Message Transfer Agent (MTA)
- Mail Delivery Agent (MDA)
- Message Store (MS)

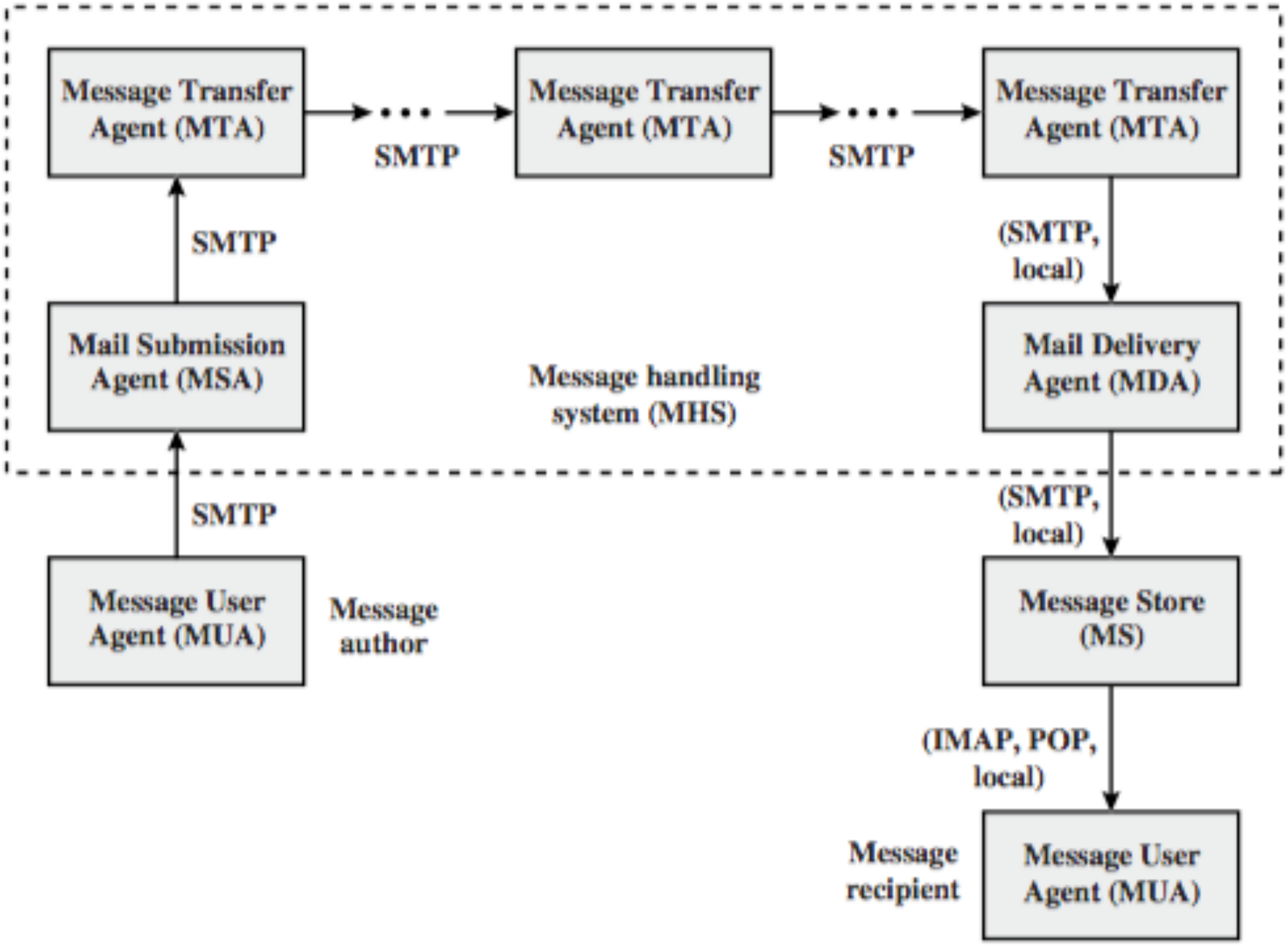

Figure 18.9 Function Modules and Standardized Protocols for the Internet

Threats in email architecture

DKIM Strategy

DKIM allows good senders to prove that they did send a particular message and to prevent forgers from masquerading as good senders.

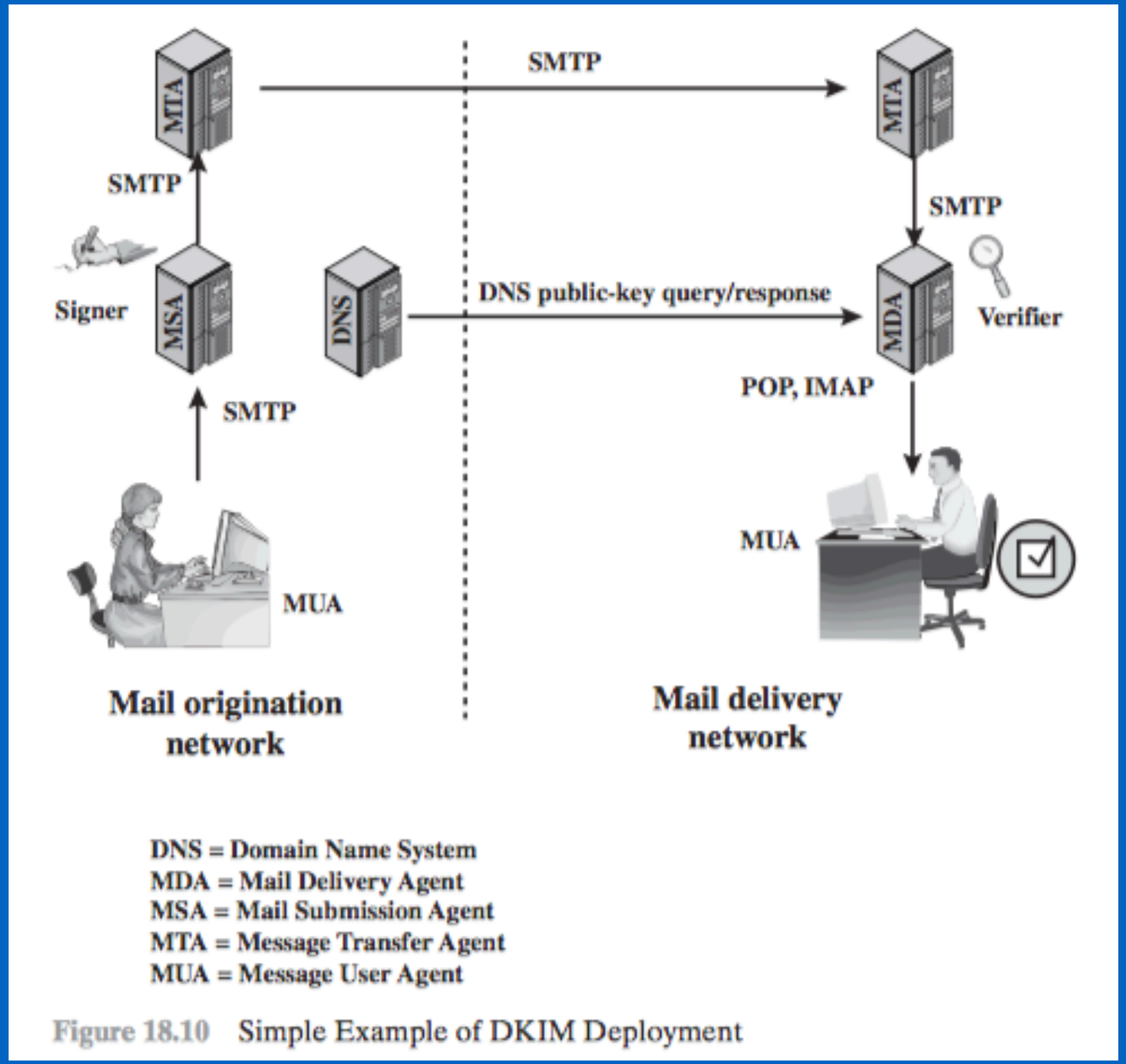

Figure 18.10 Simple Example of DKIM Deployment