



6 : Email Security and Domain Name System Security

IT6406 - Network Security and Audit

Level III - Semester 6

Overview

6.1. Email Security

- 6.1.1. Internet Mail Architecture

- 6.1.2. Email Formats

- 6.1.3. Email Threats and Comprehensive Email Security

- 6.1.4. S/MIME

- 6.1.5. Pretty Good Privacy (PGP)

6.2. Domain Name System Security

- 6.2.1. DNSSEC

- 6.2.2. DNS-Based Authentication of Named Entities

- 6.2.3. Sender Policy Framework

- 6.2.4. DomainKeys Identified Mail

- 6.2.5. Domain-Based Message Authentication, Reporting, and Conformance

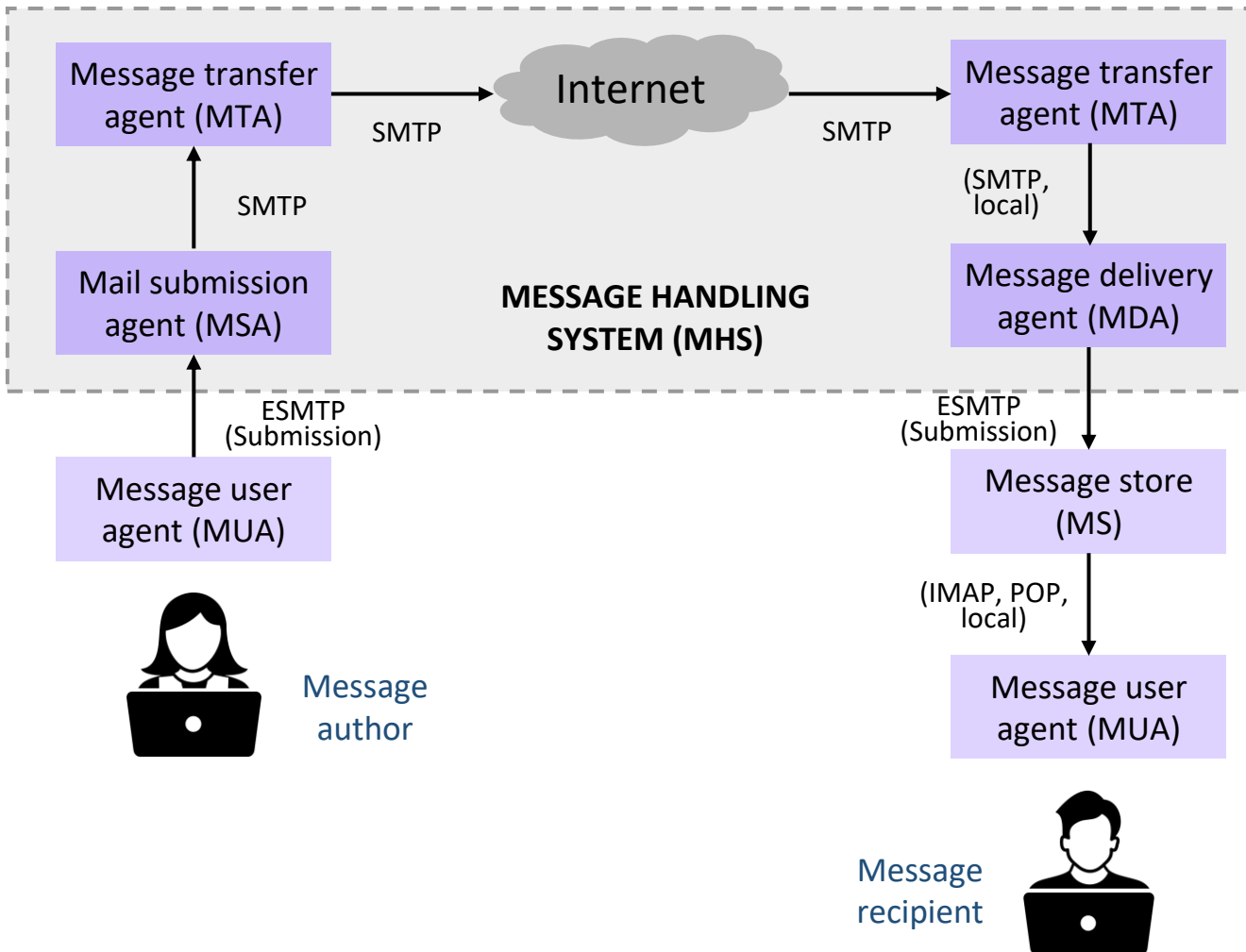
6.1.1. Internet Mail Architecture

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

Read more: Ref 1: Pg. (614-615)

6.1.1. Internet Mail Architecture...(2)

- Email components



Read more: Ref 1: Pg. (614-615)

Email Protocols

- Simple Mail Transfer Protocol (SMTP)
 - SMTP encapsulates an email message in an envelope and is used to relay the encapsulated messages from source to destination through multiple MTAs.
- Mail Access Protocols (POP, ICMP)
 - Post Office Protocol (POP3) allows an email client (user agent) to download an email from an email server (MTA).
 - IMAP is more complex than POP3.
 - IMAP provides stronger authentication than POP3.

Read more: Ref 1: Pg. (615-617)

6.1.2. Email Formats

- The structure of message described in RFC 5322 is very simple.
 - It consist of number of header lines and text (body) separated by blank line.
 - Header has some keywords like *From*, *To*, *Subject*, and *Date*.
- Multipurpose Internet Mail Extension (MIME)
 - An extension to the RFC 5322, to solve some problems and limitations in Simple Mail Transfer Protocol (SMTP).

Read more: Ref 1: Pg. (617-624)

6.1.2. Email Formats...(2)

- Header fields defined in MIME
 - MIME-Version
 - Content-Type
 - Content-Transfer-Encoding
 - Content-ID
 - Content-Description

Read more: Ref 1: Pg. (617-624)

6.1.3. Email Threats and Comprehensive Email Security

- Email security threats can be classified as,
 - Authenticity-related threat
 - Integrity-related threats
 - Confidentiality-related threat
 - Availability-related threats

Read more: Ref 1: Pg. (625-626)

6.1.3. Email Threats and Comprehensive Email Security...(2)

- Some standardised protocols designed as solutions for the threats
 - STARTTLS
 - S/MIME
 - DNS Security Extensions (DNSSEC)
 - DNS-based Authentication of Named Entities (DANE)
 - Sender Policy Framework (SPF)
 - DomainKeys Identified Mail (DKIM)
 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Read more: Ref 1: Pg. (625-626)

6.1.4. S/MIME

- Secure/Multipurpose Internet Mail Extension (S/MIME)
- Security enhancement to the MIME Internet email format standard.
- It is based on technology from RSA.
- S/MIME provides
 - Authentication
 - Confidentiality
 - Compression
 - Email compatibility

Read more: Ref 1: Pg. (627-638)

6.1.4. S/MIME...(2)

- Authentication
 - Provides by digital signature. Most commonly RSA with SHA-256.
- Confidentiality
 - Provides confidentiality by encrypting messages. Use AES-128 with CBC
- Compression
 - Compress a messages to save the space in transmission and storage.
- Email compatibility
 - Many electronic mail systems only permit the use of blocks consisting of ASCII text. S/MIME provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters.

Read more: Ref 1: Pg. (627-638)

6.1.4. S/MIME...(3)

- S/MIME Message Content Types
 - Data
 - SignedData
 - EnvelopedData
 - CompressedData

Read more: Ref 1: Pg. (627-638)

6.1.5.Pretty Good Privacy (PGP)

- Email security protocol
- Has the same functionality as S/MIME
- OpenPGP was developed as a new standard protocol based on PGP version 5.x.
- Differences between S/MIME and OpenPGP
 - Key Certification
 - S/MIME uses X.509 certificates that are issued by Certificate Authorities.
 - In OpenPGP, users generate their public key and private keys. OpenPGP public key is trusted if it is signed by another OpenPGP public key that is trusted by the recipient (Web-of-Trust).
 - Key Distribution
 - OpenPGP does not include the sender's public key with each message.

Read more: Ref 1: Pg. (638-639)

6.2.1. DNSSEC

- Domain Name System (DNS) is a service which provide a mapping between Domain names and the IP addresses.
- DNS Security Extensions (DNSSEC) secure the data exchange in DNS.
- It protect DNS clients from accepting forged or altered DNS resource records by using digital signatures.
- DNSSEC provides,
 - Data origin authentication
 - Data integrity verification

Read more: Ref 1: Pg. (639-642)

6.2.2. DNS-Based Authentication of Named Entities

- DNS-Based Authentication of Named Entities (DANE)
- If a CA in the internet compromised, the attacker can use the private key of CA and issue false certificates.
- The purpose of DANE is to replace reliance on the security of the CA system with reliance on the security provided by DNSSEC.
- DANE defines a new DNS record type, TLSA, that can be used for a secure method of authenticating SSL/TLS certificates.
- DANE can be used in conjunction with SMTP over TLS to more fully secure email delivery.

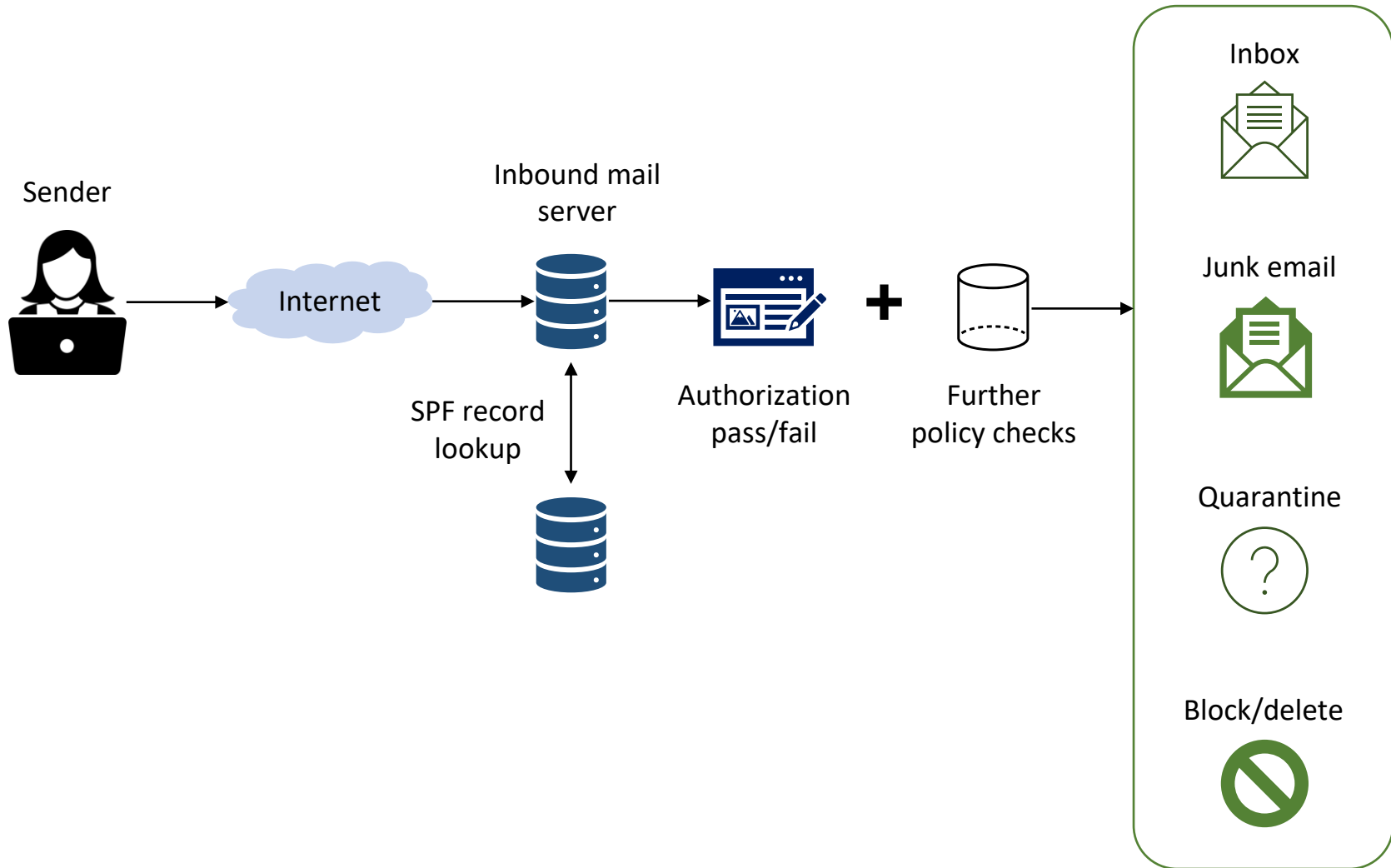
Read more: Ref 1: Pg. (643-644)

6.2.3. Sender Policy Framework

- SPF is the standardised way for a sending domain to identify and assert the mail senders for a given domain.
 - With the current email infrastructure, any host can use any domain name for each of the various identifiers in the mail header.
- SPF provides a protocol by which Administrative Management Domain (ADMD) can authorise hosts to use their domain names in the "MAIL FROM" or "HELO" identities.
- With SPF, it is difficult for the sender to alter the domain of the sender email.

Read more: Ref 1: Pg. (645-647)

6.2.3. Sender Policy Framework...(2)



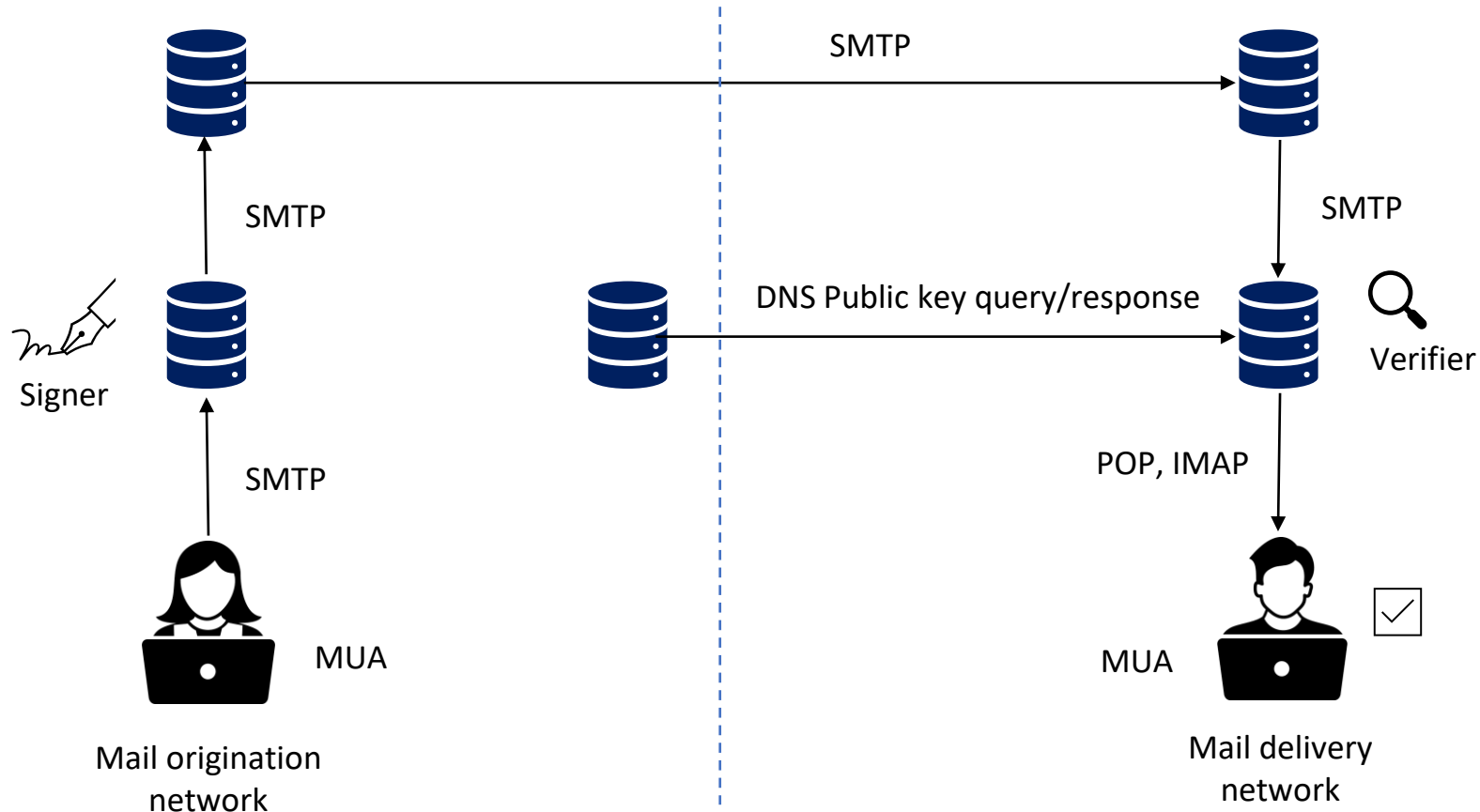
Read more: Ref 1: Pg. (645-647)

6.2.4.DomainKeys Identified Mail

- DomainKeys 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.
- DKIM authentication is transparent to the end user.
- User's email message is signed by a private key of the administrative domain from which the email originates.
- At the receiving end, the Mail Delivery Agent (MDA) can access the corresponding public key via a DNS and verify the signature.

Read more: Ref 1: Pg. (648-653)

6.2.4.DomainKeys Identified Mail...(2)



DNS = Domain Name System
MDA = Mail Delivery Agent
MSA = Mail Submission Agent
MTA = Message Transfer Agent
MUA = Message User Agent

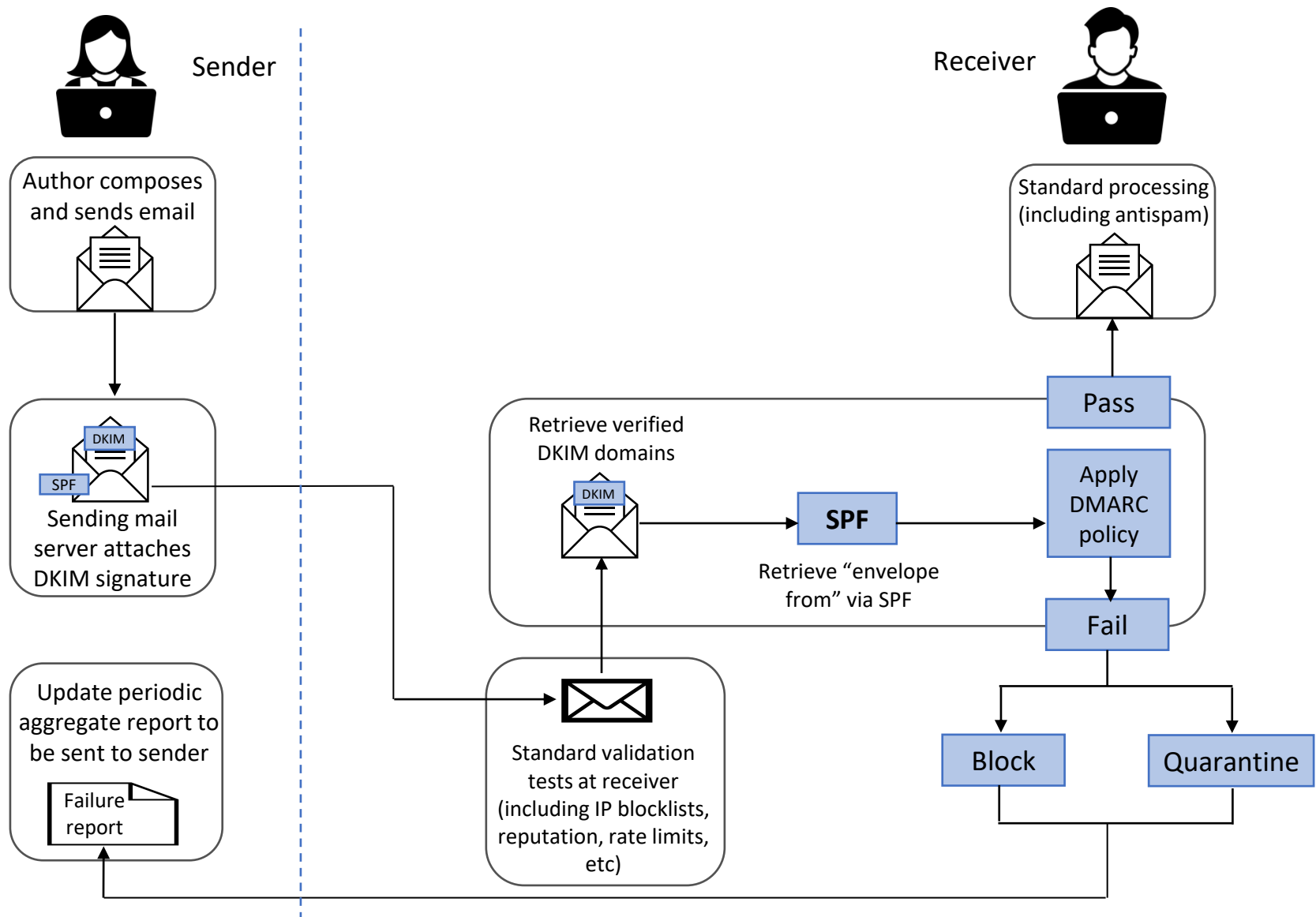
Read more: Ref 1: Pg. (648-653)

6.2.5. Domain-Based Message Authentication, Reporting, and Conformance

- It allows email senders to,
 - specify policy on how their mail should be handled,
 - the types of reports that receivers can send back,
 - the frequency those reports should be sent.

Read more: Ref 1: Pg. (654-658)

6.2.5. Domain-Based Message Authentication, Reporting, and Conformance...(2)



6.2.5. Domain-Based Message Authentication, Reporting, and Conformance...(3)

- DMARC reporting provides the sender's feedback on their SPF, DKIM, Identifier Alignment, and message disposition policies.
- Reports includes,
 - The sender's DMARC policy for that interval.
 - The message disposition by the receiver.
 - SPF result for a given SPF identifier.
 - DKIM result for a given DKIM identifier.
 - Results classified by sender subdomain.
 - The sending and receiving domain pair...etc

Read more: Ref 1: Pg. (654-658)

Reference

- Ref1: Cryptography and Network Security, Principles and Practice, 7th Edition, William Stallings. Online Chapter 23.2