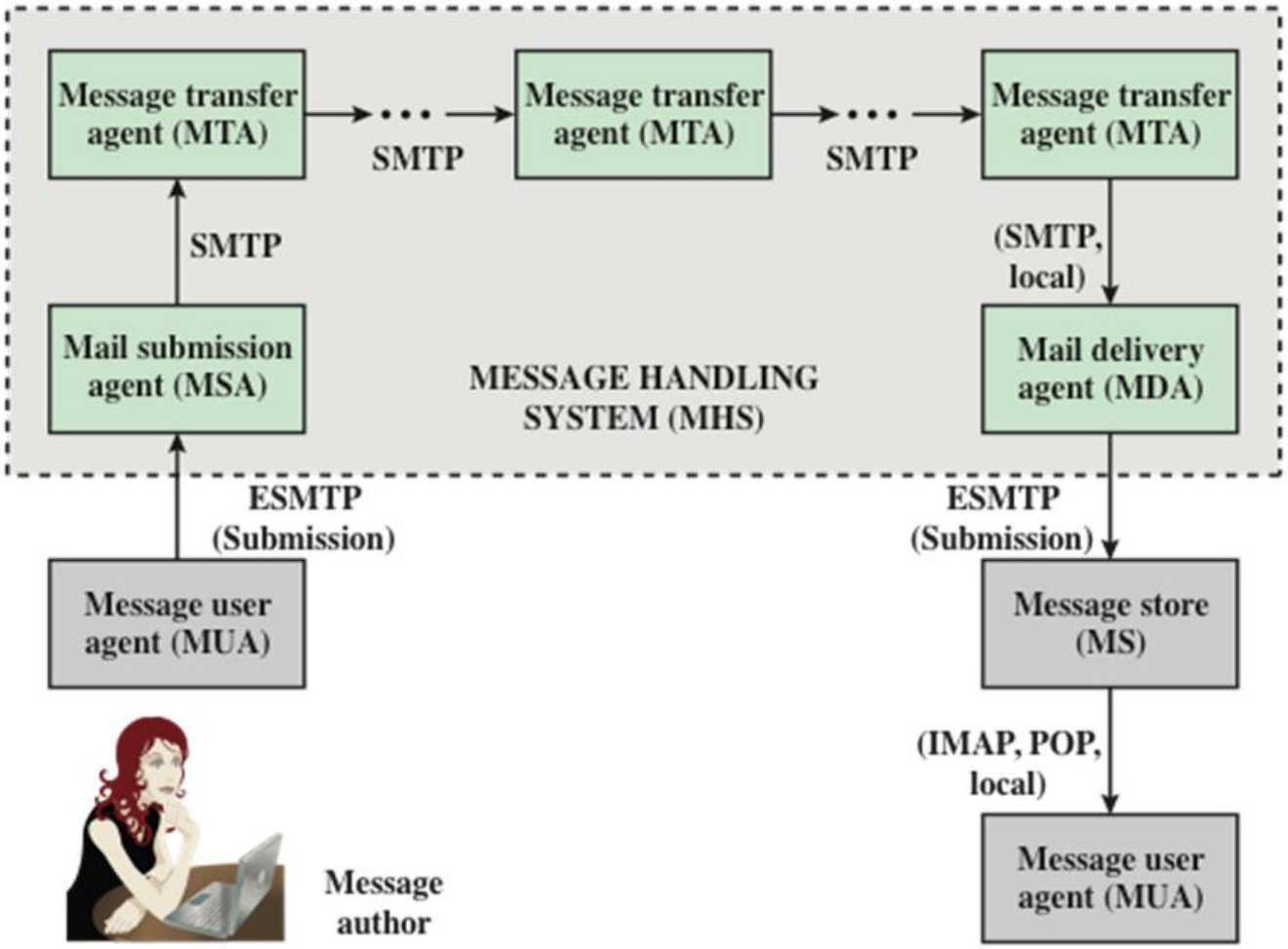
Chap. 8 Email Security

- PGP
- S/MIME

Email Service

- Email service functional model



Email Service

- MUA (Mail User Agent)
  - MUA sender: composes an email and submits the email to MHS (mail Handling System) thru MSA (Mail Submission Agent)
  - MUA receiver: receives an email from the MS (Message Store) and delivers to the user
- MSA (Mail Submission Agent)
  - receives an email from MUA and checks the conformance of the policy of ADMD (Administrative Management Domain) and delivers to MTA (Mail Transfer Agent)

Email Service

- MTA (Mail Transfer Agent)
  - performs one hop transmission of an Email
- MDA (Mail Delivery Agent)
  - delivers an email from MHS to MS (Message Store)

- Email protocol
  - SMTP: MUA sender-MSA, MSA-MTA, MTA-MTA, MTA-MDA, MDA-MS
  - PoP3 or IMAP: MS-MUA receiver

Email Service

- Email message: RFC-822, RFC-5322

Date: October 8, 2009 2:15:49 PM EDT
From: "William Stallings" <ws@shore.net>
Subject: The Syntax in RFC 5322
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual message body, which is delimited from the message heading by a blank line.

Email Service

- MIME: extension of RFC-5322
  - defines new headers to allow multiple types of mail messages
  - MIME-Version: MIME protocol version (1.0)
  - Content-Type: type of payload mail message
  - Content-Transfer-Encoding: transmission type of payload mail message
  - Content-ID: ID of the MIME message
  - Content-Description: description of payload mail message

Email Service

- MIME types: type/subtype

유형	서브유형	설명
텍스트(Text)	Plain Enriched	형식화되지 않은 텍스트; ASCII 또는 ISO 8859 다양한 형식 유연성 제공
멀티파트(Multipart)	Mixed	파트는 서로 독립적이지만 같이 전송된다. 파트는 메일 메시지에 나타나는 순서대로 수신자에게 나타나야만 한다.
	Parallel	수신자에게 파트를 전달하는 순서가 정의되지 않는다는 것이 Mixed와 다르다.
	Alternative	다른 파트는 동일한 정보의 다른 버전이다. 원래 정보에 충실한 정도에 따라 순서가 정해지고 수신자의 메일 시스템은 사용자의 가장 좋은("best") 버전을 나타내야만 한다.
	Digest	Mixed와 비슷하다. 그러나 각 파트의 기본 type/subtype은 message/rfc822이다.

Email Service

- MIME types:

유형	서브유형	설명
메시지(Message)	rfc822	body는 RFC 822에 준하는 캡슐화 된 메시지이다.
	Partial	수신자에게 투명한 방법으로 큰 메일을 단편화 할 수 있게 한다.
	External-body	다른 곳에 있는 객체 포인터를 포함하고 있다.
정지화상(Image)	jpeg	정지 화상은 JPEG 형식이다. JFIF 인코딩이다.
	gif	정지 화상은 GIF 형식이다.
비디오(Video)	mpeg	MPEG 형식이다.
오디오(Audio)	Basic	표본 추출 비율이 8kHz인 단일-채널 8-비트 ISDN μ-law 인코딩이다.
응용(Application)	PostScript	Adobe Postscript.
	Octet-stream	8-비트 바이트로 된 일반적인 2진 데이터이다.

Email Service

- Multipart message:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=frontier

This is a message with multiple parts in MIME format.
--frontier
Content-Type: text/plain

This is the body of the message.
--frontier
Content-Type: application/msword
Content-Transfer-Encoding: base64

PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+VGhpcyBpcyB0aGUg
Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+Cg==
--frontier--
```

Email Service

- Email service threats
  - authentication-related threats
  - confidentiality-related threats
  - integrity-related threats
  - availability-related threats

Pretty Good Privacy (PGP)

- Made by Phil Zimmermann
- Available free
- Provides a confidentiality, integrity, and authentication service for Email
- Standardized in RFC 3156

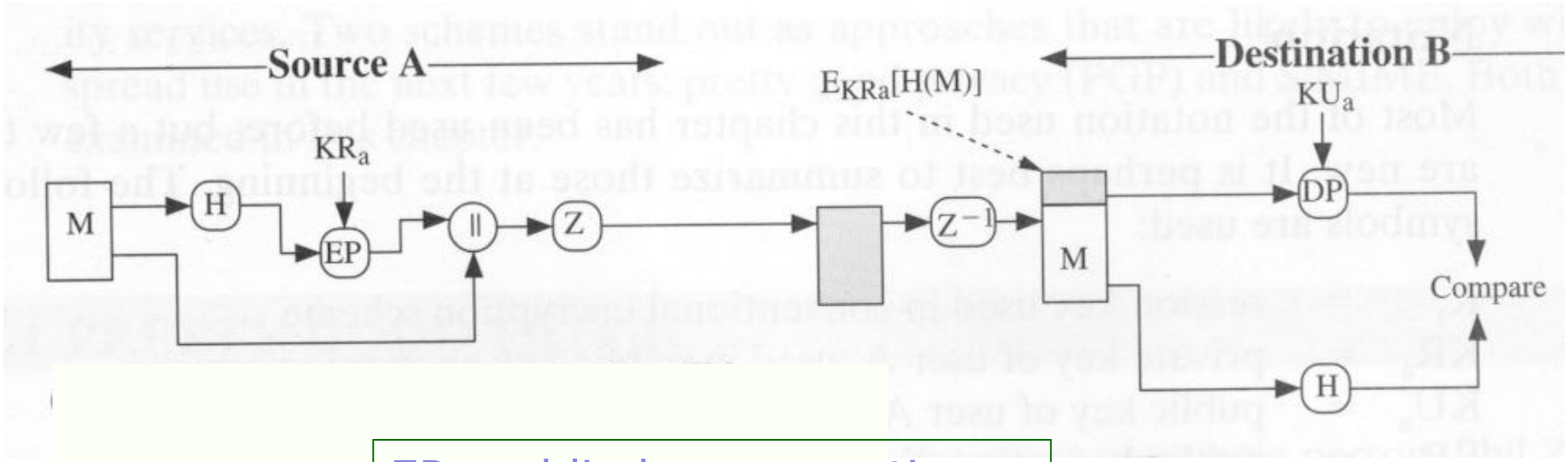
Pretty Good Privacy (PGP)

PGP services

- Message encryption: cast-128, IDEA, or 3-DES
- Digital signature: DSS/SHA or RSA/SHA
- One-time session key for each email message
- Session key distribution: Diffie-Helmann or RSA
- Message compression with ZIP
- Email compatible: radix-64 binary-to-ASCii conversion
- Segmentation: to accommodate max message size limitations

PGP Cryptographic Functions

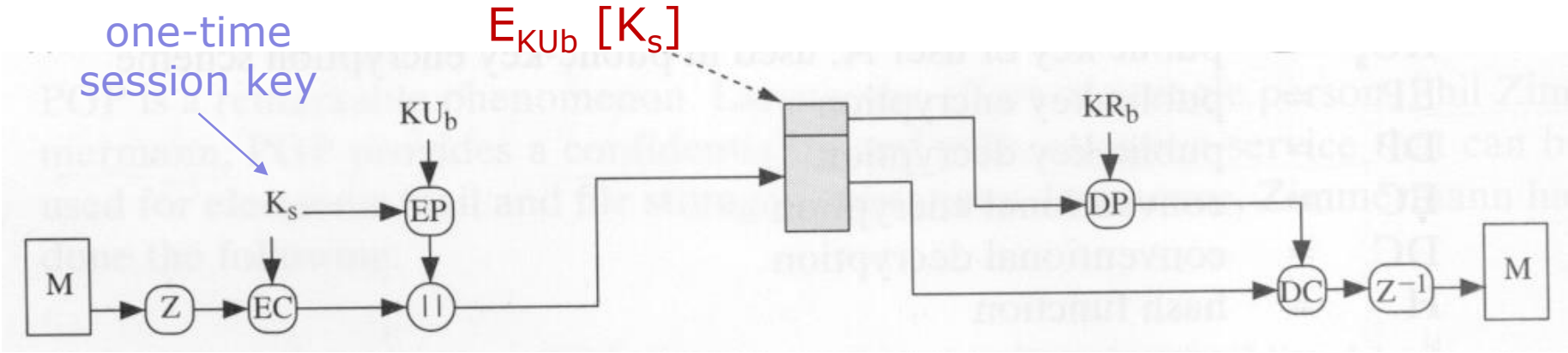
- Authentication only



EP: public-key encryption
EC: secret-key encryption
H: hashing
Z: compression

PGP Cryptographic Functions

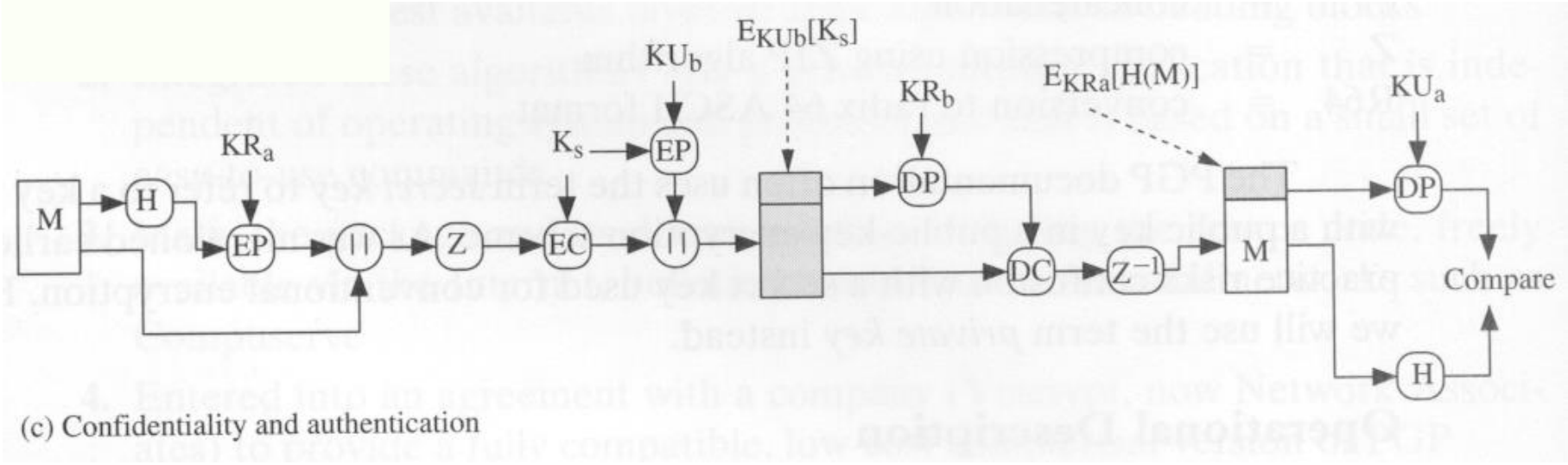
- Confidentiality only



EP: public-key encryption
EC: secret-key encryption
H: hashing
Z: compression

PGP Cryptographic Functions

- Confidentiality and authentication



(c) Confidentiality and authentication

EP: public-key encryption
EC: secret-key encryption
H: hashing
Z: compression

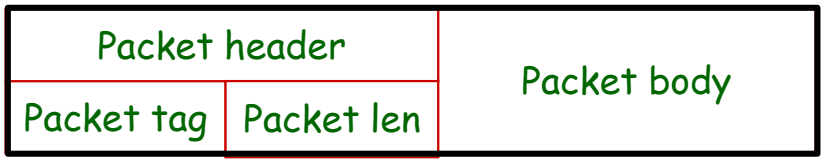
PGP Cryptographic Keys

- One-time session key
  - A session key is generated by sender for each message
- Public and private keys
  - users can have multiple public/private key pairs
  - Session key encrypted using recipient's public key
  - Sender sends the keyID (the least significant 64 bits of the key) of the public key used for the encryption
- Passphrase-based encryption of private key
  - Users store their own private key in encrypted form
  - Password used to encrypt the owner's private key

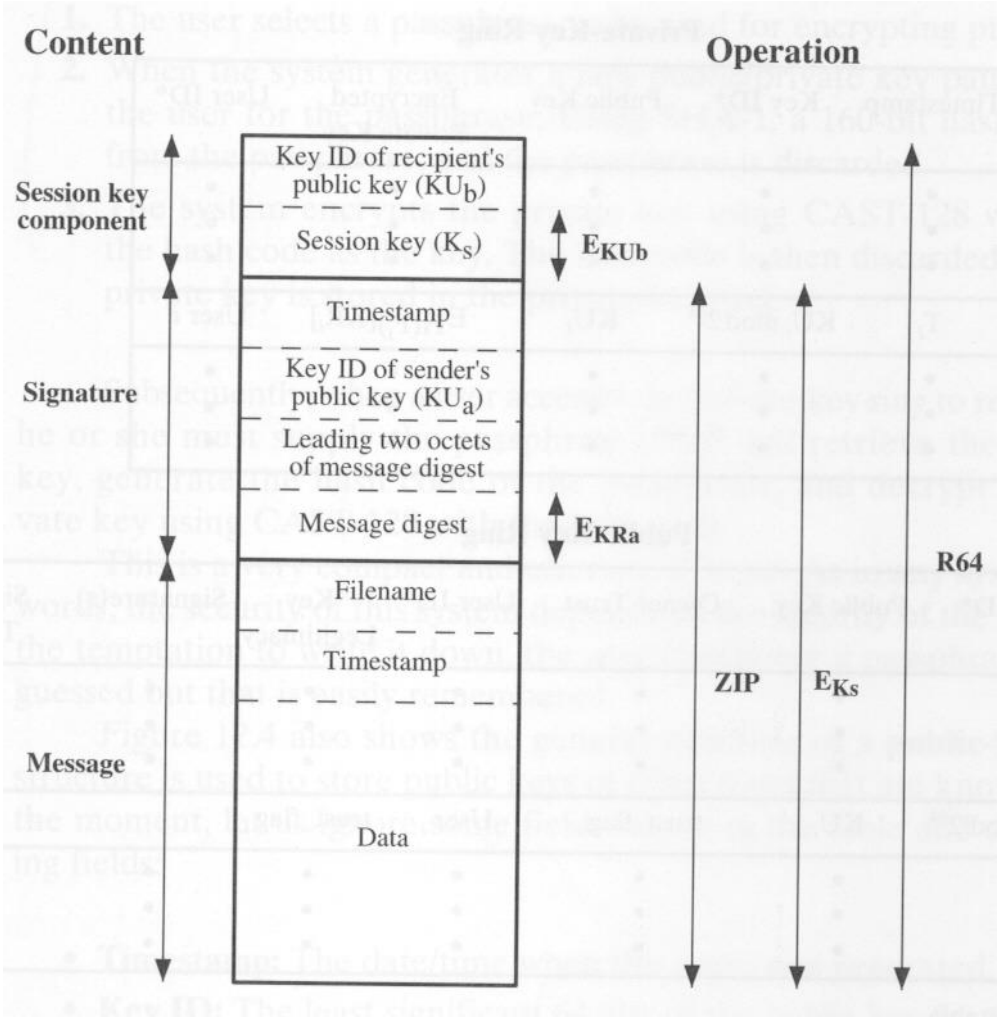
PGP Packet Format

- A PGP message consists of
  - Message packet
  - Signature packet
  - Session key packet

- Packet format



Packet tag: denotes the type of packet in the packet body



PGP Message Format

- Message component
  - Data to be transmitted
- Signature component
  - Timestamp: time at which the signature is made
  - Message digest: 160-bit SHA digest encrypted with sender's private key
  - keyID of sender's public key
- Session key component
  - Session key
  - keyID of recipient's public key used to encrypt session key

PGP Key Rings

- Private-key ring
  - Stores the public/private key pairs owned by that node
  - Private keys are encrypted using a key based on the user's passphrase (SHA hash code of the passphrase)

Private-Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(P_i)}[KR_i]$	User *i*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

PGP Key Rings

- Public-key ring
  - Stores other's public keys known at this node
  - PGP allows multiple public/private key pairs for each user
  - Public keys can be obtained in various ways

Public-Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_i	KU_i mod 2^{64}	KU_i	trust_flag $_i$	User $_i$	trust_flag $_i$		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

PGP Key Rings

- Public-key ring
  - Owner trust: trust value for the key owner;
    - assigned by the user when the user enters a new public key: unknown, untrusted, marginally trusted, completely trusted
  - Signatures: signatures attached to the key
  - Signature trusts: trust value for the owner of this signature attached to the key
    - "unknown" value is assigned if owner is not known

PGP Key Rings

- Public-key ring
  - Key legitimacy:
    - the extent to which PGP will trust the key
    - derived from the values in the signature trusts fields
    - weighted sum of the signatures trust values
  - web of trust model

PGP Trust Model

- User A can obtain B's public key by many ways
  - physically get the key from B
  - obtain B's key from a mutual trusted individual D
  - obtain and verify B's key by telephone
  - obtain B's key from a trusted certifying authority

- Trust of people: determined by himself
- Trust of public key: web of trust model
  - A user can sign a key if he/she trusts that key
  - Public key trust is determined by the signatures in the key

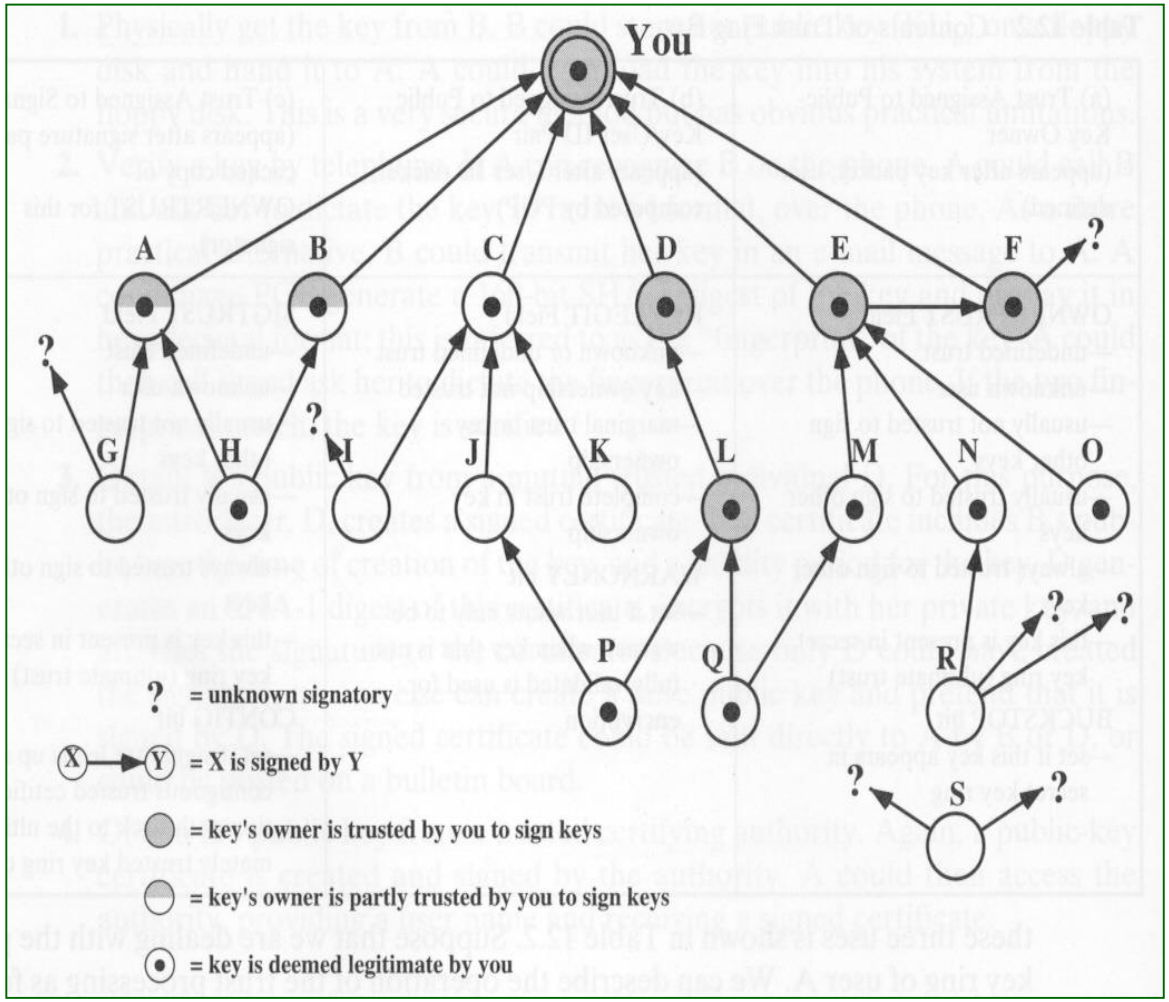
PGP Trust Model

- Inserting a new public key on public-key ring
  - assigns the trust value of the key's owner given by the user
  - the trust value for each signature attached at the key is given to the OwnerTrust value for the owner of the signature;
  - if the owner for the signature is not in the key ring, it is given to an unknown user value
- Key legitimacy value is calculated based on the signature trust fields present in the entry

PGP Key Trust Model

PGP trust model example (public-key ring)

- The user signs keys whose owners are fully or partly trusted (except L)
- One trusted signature or two partly trusted signatures are sufficient to trust a key, but the key's owner may not be trusted
- Key revocation by issuing a key revocation certificate



S/MIME

- Industrial standard for commercial and organizational use
- RFC 822
  - Traditional email format for transmitting text messages
  - Header + blankLine + Body

```
Date: Tue, 16 Jan 1998 10:37:17 (EST)
From: "William Stallings" <ws@shore.net>
Subject: The Syntax in RFC 822
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual message body, which is
delimited from the message heading by a blank line.
```

MIME

- MIME (Multipurpose Internet Mail Extensions)
  - Extends RFC822 to support many types of messages
- New headers
  - MIME-Version:
  - Content-Type: type of content in the message body (text/plain, multipart/mixed, video/mpeg, …)
  - Content-Transfer-Encoding: type of transmission of the message body to be transmitted by the MTA
  - Content-ID: to overcome the mail size limitations
  - Content-Description:

S/MIME Functionality

- Enveloped data: encrypted data and encrypted encryption key
- Signed data: content + digital signature; encoded using base64 encoding
- Clear-signed data: content + digital signature; only digital signature is encoded using base64 encoding
- Signed and enveloped data: content + digital signature; encrypted using a session key

S/MIME Cryptographic Algorithms

- Encryption: 3DES, RC2
- Digital signature: DSS, 160bit SHA-1, 128bit MD5
- Session key encryption: Diffie-Hellmann, RSA
- Sending agent and receiving agent determines the encryption algorithm via negotiation

S/MIME Public Key Management

- S/MIME key management: a hybrid of X.509 and PGP key management model
  - Certificates are managed locally but the certificates are signed by certification authorities
- S/MIME user agent
  - generate his own public/private pairs
  - register the public key and receive X.590 certificate for the key
  - store other's certificates in a local storage and verify the incoming certificates