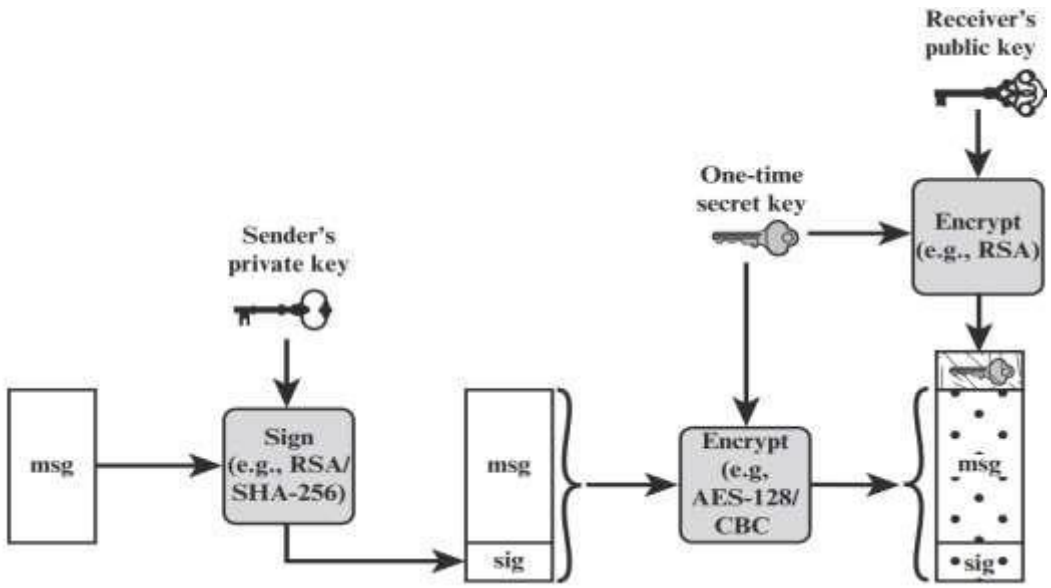
Lecture NS8 2018

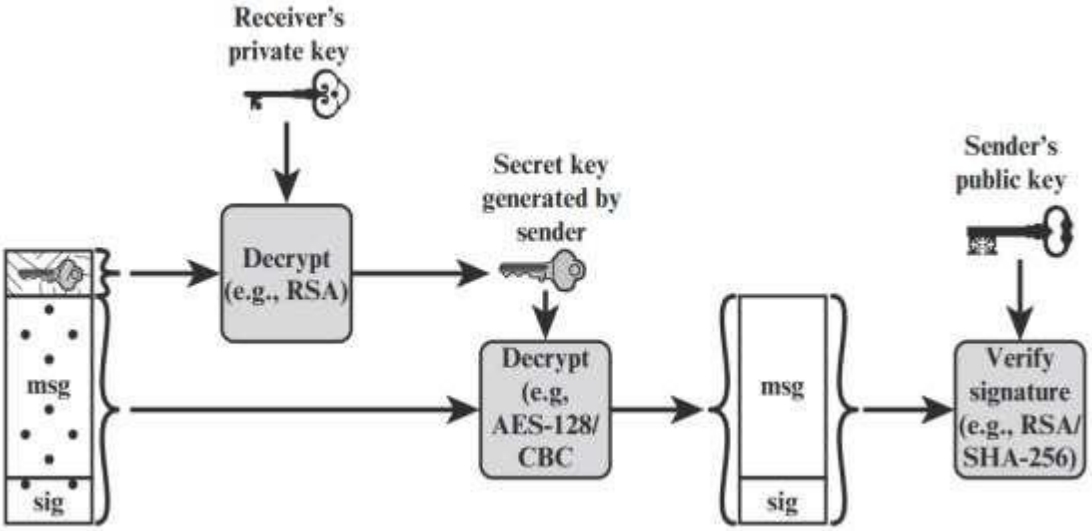
Chapter 19

Q_3: Briefly describe the Simplified S/MIME Functional Flow



Answer:

a. The sender creates a message.
b. SHA-256 is used to generate a 256-bit message digest of the message and use Sender's private key to sign the message
c. AES-128 is used to generate a random 128-bit number, then use a one-time secret key to encrypt the message
d. The key itself is also encrypted with RSA and the result is bound to message.



e. The receiver uses RSA with its private key to decrypt and recover the content-encryption key.
f. Use the secret key generated by sender to decrypt the message.
g. Use sender's public key and 256-bit message digest generated by SHA-256 to verify signature.

Yang Qingqing 29184657

Question1:

Describe The Internet Mail Architecture and what is SMTP , IMAP and POP ?

Answer1:

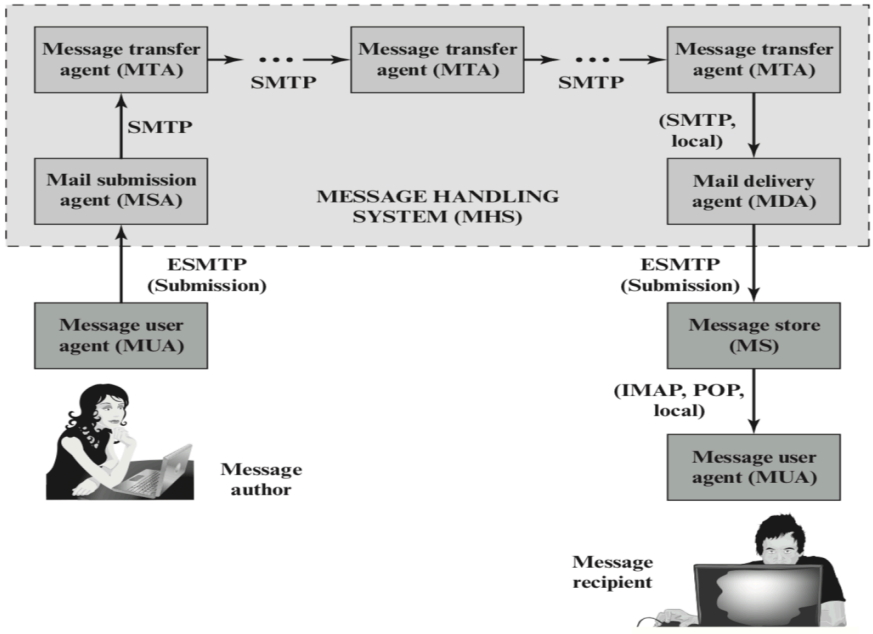


Figure 19.1 Function Modules and Standardized Protocols Used between them in the Internet Mail Architecture

The figure illustrates the key components of the Internet mail architecture

- Step1: Message User Agent(MUA) submits the message to the Message Submission Agent (MSA). The Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.
- Step2: Message Transfer Agent (MTA) relays mail for one application-level hop. It is like a packet switch or IP router in that its job is to make routing assessments and to move the message closer to the recipients. SMTP is used between MTAs and between an MTA and an MSA or MDA.

- Step3: Mail Delivery Agent (MDA) receives the message from MTA and is responsible for transferring the message from the Message Handling System (MHS) to the MS.
- Step4: Mail is stored in Message Store (MS). The message recipient retrieves messages from a remote server using POP or IMAP.

Simple Mail Transfer Protocol (SMTP) is used to move messages through the Internet from source to destination.

Internet mail access protocol (IMAP) and Post Office Protocol(POP) are mail access protocol, which are used to transfer messages between mail.

Question2:

Encode the text "plaintext" using the following techniques. Assume characters are stored in 8-bit ASCII with zero parity.

a. Radix-64

b. Quoted-printable

Answer2:

(a)The first step is to convert the characters into 8-bit ASCII with zero parity. Consulting the table in Appendix Q, we have the following correspondence:

p 01110000.

l 01101100.

a 01100001.

i 01101001.

n 01101110.

t 01110100.

e 01100101.

x 01111000.

t 01110100.

Next, we block these off into groups of 6 bits, show the 6-bit decimal value, and do the encoding.

011100 000110 110001 100001 011010 010110 111001 110100.

28	6	49	33	26	22	57	52
c	G	x	h	a	W	5	0

011001 010111 100001 110100

25	23	33	52
Z	X	h	0

So the radix-64 encoding is cGxhaW50ZXh0

(b) All of the characters are "safe", so the quoted-printable encoding is simply plaintext

The Radix-64 Table:

6-bit Value	Character Encoding	6-bit Value	Character Encoding	6-bit Value	Character Encoding	6-bit Value	Character Encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

Question3:

What is S/MIME, DKIM/DNSSEC?

Answer3:

- S/MIME: Provides authentication, integrity, non-repudiation (via digital signatures) and confidentiality (via encryption) of the message body carried in SMTP messages.
- DomainKeys Identified Mail (DKIM): Enables an MTA to sign selected headers and the body of a message. This validates the source domain of the mail and provides message body integrity.
- DNS Security Extensions (DNSSEC): Provides authentication and integ- rity protection of DNS data, and is an underlying tool used by various email security protocols.

Zheng Rui
29184614

Q1: Briefly describes the steps for preparing a `signedData` MIME entity.

A1: The steps for preparing a `signedData` MIME entity are as follows：

1. Select a message digest algorithm (SHA or MD5).
2. Compute the message digest (hash function) of the content to be signed.
3. Encrypt the message digest with the signer's private key.
4. Prepare a block known as `SignerInfo` that contains the signer's public-key certificate, an identifier of the message digest algorithm, an identifier of the algorithm used to encrypt the message digest, and the encrypted message digest.

Q2: Why the NIST 800-177 recommends the use of the S/MIME rather than PGP?

A2: NIST 800-177 recommends the use of S/MIME rather than PGP because of the greater confidence in the CA system of verifying public keys. S/MIME uses X.509 certificates that are issued by Certificate Authorities (or local agencies that have been delegated authority by a CA to issue certificates). In OpenPGP, users generate their own OpenPGP public and private keys and then solicit signatures for their public keys from individuals or organizations to which they are known.

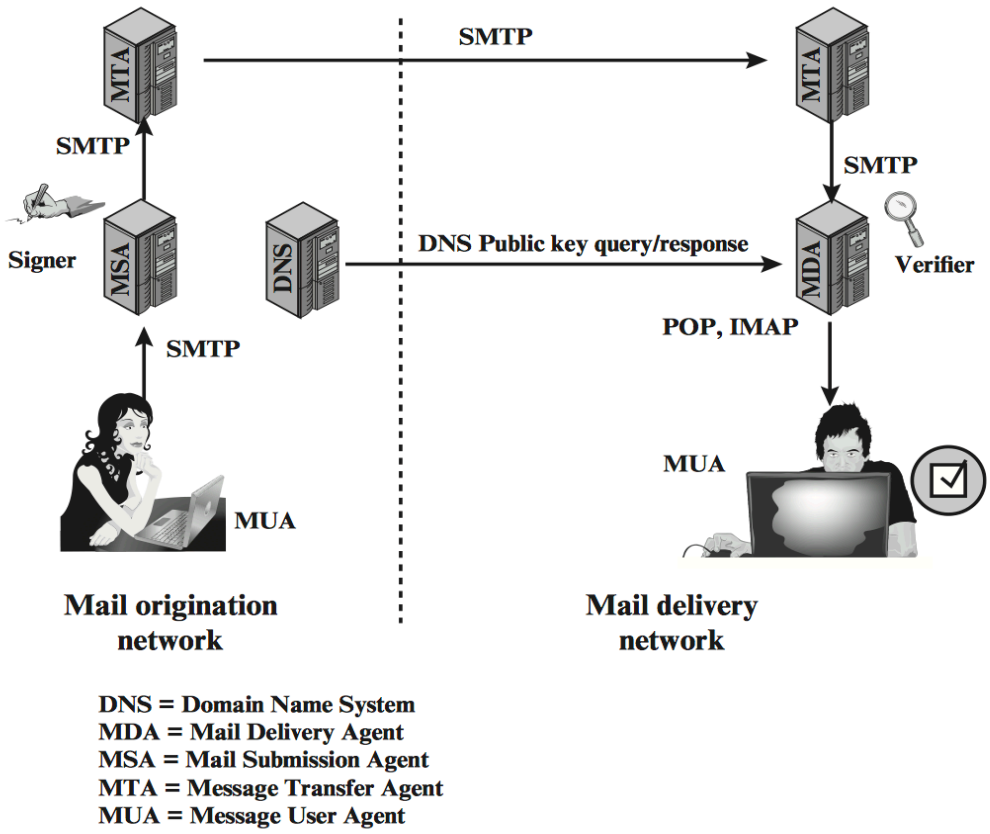
Q3: The S/MIME specification includes a discussion of the procedure for deciding which content encryption algorithm to use. A sending agent has two decisions to make. Describe the two decisions.

A3: First, the sending agent must determine if the receiving agent is capable of decrypting using a given encryption algorithm. Second, if the receiving agent is only capable of accepting weakly encrypted content, the sending agent must decide if it is acceptable to send using weak encryption.

Guo Lele 29184428

Q1 The following figure is a simple example of the operation of DKIM.

Based on this picture, can you describe the example briefly?



Answer:

A message is generated by a client program. The content of the message, plus selected RFC 5322 headers, is signed by the 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 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 client. The default signing algorithm is RSA with SHA-256. RSA with SHA-1 may also be used.

Q2 Write something you know about the following terms.

DANE, SPF, DKIM, DMARC

Answer:

DANE– DNS-based authentication of named entities

• a way to authenticate TLS client and server entities without a certificate authority (CA)

• to replace reliance on the security of the CA system with reliance on the security provided by DNSSEC

SPF-Sender policy framework

• the standardized way for a sending domain to identify and assert the mail senders for a given domain

•addresses the following problem:

– any host can use any domain name for each of the various identifiers in the mail header, not just the domain name where the host is located(two major drawbacks)

DKIM-Domain Keys 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.

DMARC-Domain-Based Message Authentication, Reporting, and Conformance

- 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

- works with SPF and DKIM