4.2 S/MIME

S/MIME is a security enhancement to MIME. S/MIME will emerge as the industry standard for commercial and organizational use.

To understand the S/MIME, we need first to have a general understanding of the e-mail format RFC822.

RFC822

RFC 822 defines a format for text messages that are sent using e-mail. In RFC 822 messages are said to have an envelope and contents.

Envelop: Information needed for transmission and delivery is present.

Content: It contains the object to be delivered to the receiver.

Each line in the header consists of a keyword such as ***From, To, Subject, Date*.** The following are the limitations of SMTP/RFC 82 scheme.

- SMTP cannot transmit executable or other binary data.
- SMTP cannot transmit text data that includes natural language characters.
- SMTP server may reject mail message over a certain type

Overview of MIME

1. Five new message header fields are defined, which may be included in an RFC 822 header.

2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.

3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

The five header fields defined in MIME are as follows

MIME-Version: This field must have a parameters value of 1.

Content-Type: This deals with the definition of variety of content types.

In general content type specifies the type of data.

Content-Transfer-Encoding: Indicates the type of transformation that has been used to represent the body of the message.

Content-ID: Used to identify MIME entities.

Content-Description: A text description of the object within the body.

Content-Type

There are seven different major types of content and total of 15 subtypes.

Type	Subtype	Description
Text	Plain	Unformatted text;
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted
	Parallel	The multiple parts can be presented in parallel.
	Alternative	The different representation of the same
	Digest	Similar to Mixed, but the default type/subtype of
Message	rfc822	The body is itself an encapsulated message.
	Partial	Used to allow fragmentation of large mail items.
	External-	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN.
Applicatio	PostScript	Adobe Postscript.
	octet-stream	General binary data consisting of 8-bit bytes.

MIME Transfer Encodings

The objective is to provide reliable delivery across a largest range of environments.

7bit	The data are all represented by short lines of ASCII characters.
8bit	The lines are short, but there may be non-ASCII characters.
binary	The lines are not necessarily short enough and non-ASCII
quoted-	Data being encoded are mostly ASCII text.
base64	Encodes data by mapping 6-bit blocks of input to 8-bit blocks
x-token	A named nonstandard encoding.

S/MIME functionality

S/MIME provides the following functions

Enveloped Data: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.

Signed Data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded
using base 64 encoding.

Clear-signed Data: The digital signature is encoded using base64. As a result recipients without
S/MIME capability can view the message content, although they cannot verify the signature.

Signed and enveloped data: Signed only and encrypted only entities may be nested, so that encrypted data may be signed.

S/MIME messages

S/MIME secures a MIME entity with a signature, encryption or both.

Type	Subtype	smime	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the
Application	pkcs 7-mime	signedData	A signed S/MIME entity.
	pkcs 7-mime	envelopedDat	An encrypted S/MIME entity
	pkcs 7-mime	degen	s An entity containing only public- key
	pkcs 7-mime	Compressed	A compressed S/MIME
	pkcs 7-	signedData	The content type of the signature subpart

Content Type of S/MIME

Enveloped Data

The steps for preparing an enveloped Data are as follows

1. Generate a pseudo-random session key for a particular symmetric encryption algorithm.
2. For each recipient, encrypt the session key with the recipient's public RSA key.
3. For each recipient, prepare a block known as RecipientInfo that contains the sender's public- key certificate, an identifier for the algorithm used to encrypt the session key, and the encrypted session key.

4. Encrypt the message content with the session key.

SignedData

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

1. Select a message digest algorithm.

2. Compute the message digest, or 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.

S/MIME Certificate Processing

S/MIME user has several key-management functions to perform:

Key generation: Must be capable of generating separate Diffie-Hellman and DSS key pairs and should be capable of generating RSA key pairs. Each key pair must be generated from a good source of nondeterministic random input and be protected in a secure fashion.

Registration: A user's public key must be registered with a certification authority in order to receive an X.509 public-key certificate.

Certificate storage and retrieval: The list of certificates could be maintained by the user or by some local administrative entity on behalf of a number of users.

VeriSign Certificates

VeriSign provides a service that is intended to be compatible with S/MIME and a variety of other applications. VeriSign issues X.509 certificates with the product name VeriSign Digital ID. Each digital ID contains

- Owner's public key
- Owner's name or alias
- Expiration date of the Digital ID
- Serial number of the Digital ID
- Name of the certification authority that issued the Digital ID

Enhanced Security Services

- Signed Recepits
- Security Labels
- Secure Mailing Lists

S/MIME Cryptographic Algorithms

- Hash functions: SHA-1 & MD5
- Digital signatures: DSS & RSA
- Session key encryption: ElGamal & RSA
- Message encryption: Triple-DES, RC2/40 and others