UNIT II

E-MAIL SECURITY & FIREWALLS

S/MIME

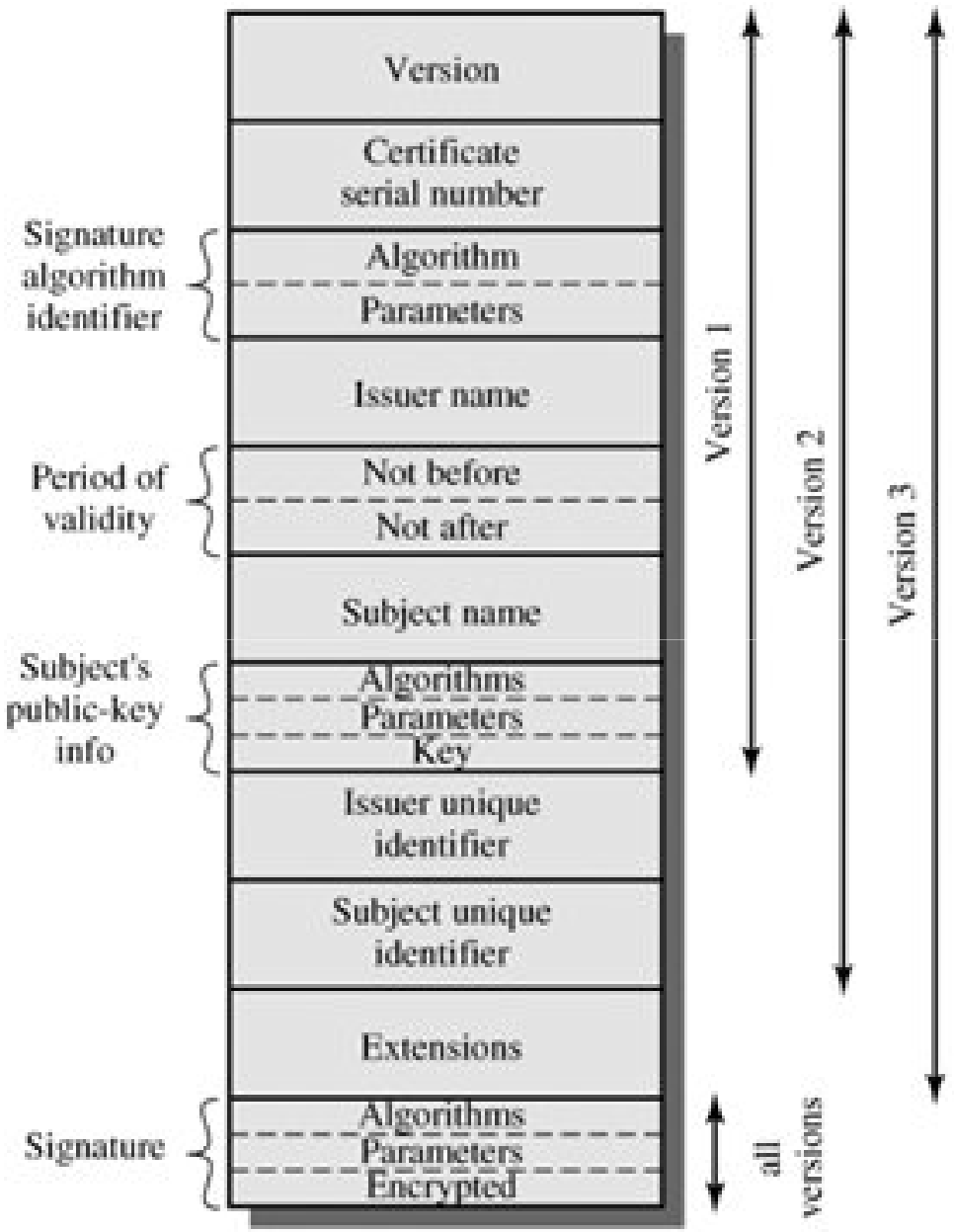
- Provides a secure way to send and receive MIME data
- Provides the following cryptographic security services for electronic messaging applications
  - Authentication
  - Message integrity
  - Non-repudiation of origin (using digital signatures)
  - Data confidentiality (using encryption)
  - Supplementary service - Message Compression

S/MIME

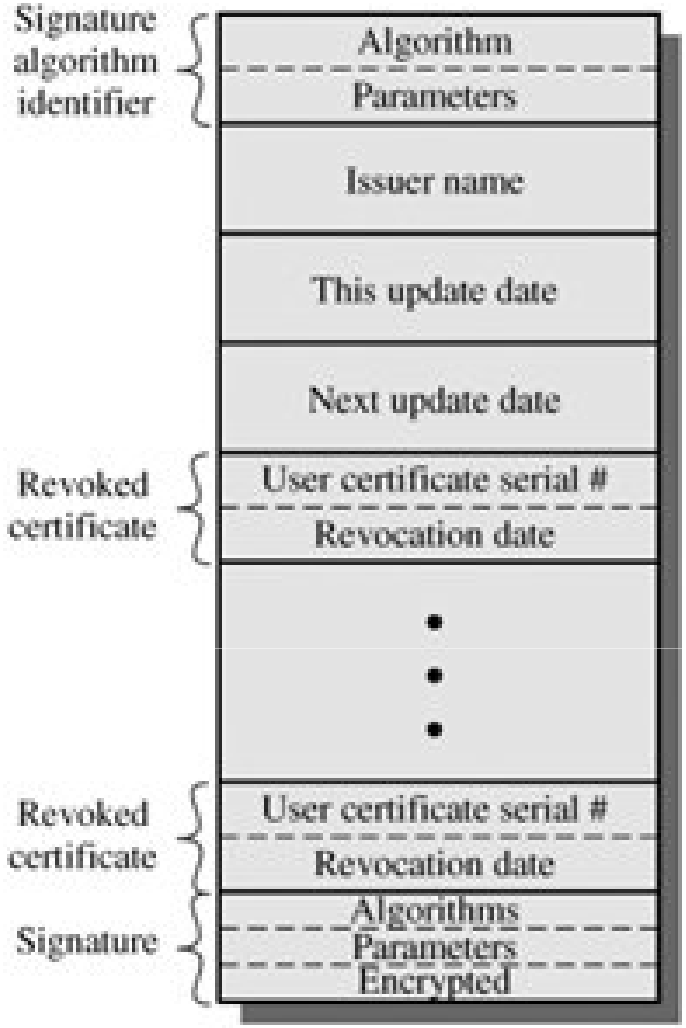
- Used by traditional mail user agents (MUAs)
  - To add cryptographic security services to mail that is sent
  - To interpret cryptographic security services in mail that is received
- Not restricted to mail
  - Can be used with any transport mechanism that transports MIME data, such as HTTP or SIP

X.509 Certificates

- Issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (*from* - *to* dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)
- Notation "CA<<A>>" denotes certificate for A signed by CA



(a) X.509 certificate



(b) Certificate revocation list

S/MIME

- Definitions
- The following definitions are to be applied:
  - ASN.1 :
    - Abstract Syntax Notation One, as defined in ITU-T X.680– 689.
  - BER:
    - Basic Encoding Rules for ASN.1, as defined in ITU-T X.690.
  - DER:
    - Distinguished Encoding Rules for ASN.1, as defined in ITU-T X.690.
  - Certificate:
    - Name to a public key with a digital signature
    - Defined in the PKIX certificate and CRL profile
    - The certificate also contains the distinguished name of the certificate issuer (the signer), an issuer-specific serial number, the issuer's signature algorithm identifier, a validity period and extensions also defined in that certificate

    - **PKIX** - Public Key Infrastructure (X.509)
    - **CRL - certificate revocation list**

S/MIME

- Definitions
  - CRL:
    - The Certificate Revocation List
    - Contains information about certificates whose validity the issuer has prematurely revoked
    - The information consists of an issuer name, the time of issue, the next scheduled time of issue, a list of certificate serial numbers and their associated revocation times, and extensions
  - Attribute certificate:
    - Each X.509 AC binds one or more attributes with one of the subject's PKIXs
    - Authorization information
  - Sending agent:
    - Software that creates S/MIME
  - Receiving agent:
    - Software that interprets and processes S/MIME CMS objects
  - S/MIME agent:
    - User software that is a receiving agent, a sending agent, or both.

S/MIME

- *Cryptographic Message Syntax (CMS) Options*
  - CMS is cryptographically protected message
  - CMS allows for a wide variety of options in content and algorithm support
  - CMS provides additional details regarding the use of the cryptographic algorithms

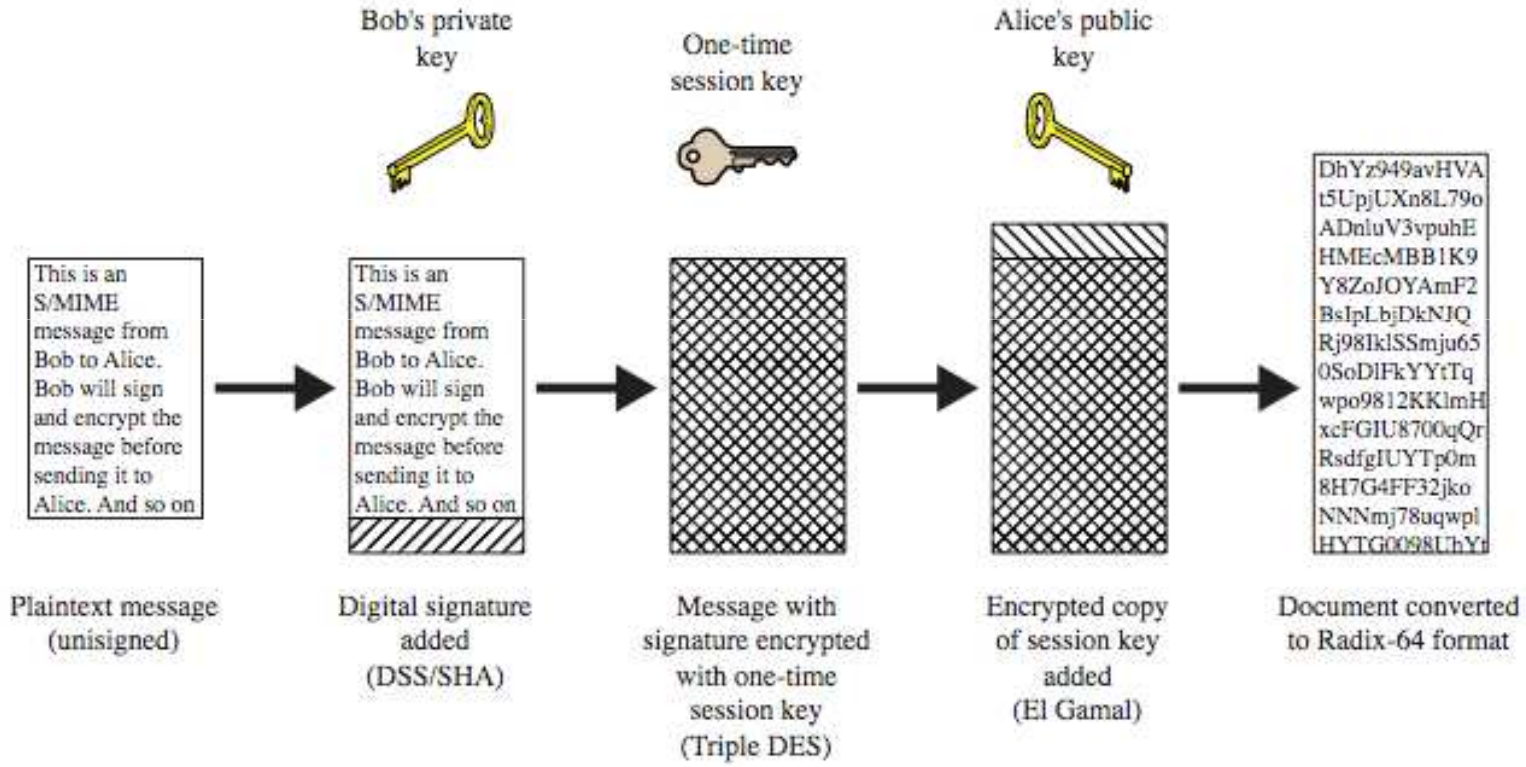
S/MIME

- *Cryptographic Message Syntax (CMS) Options*
  - **Digest Algorithm Identifier**
    - Identifies a message digest algorithm
      - Maps the message to the message digest
    - Sending and receiving agents must support SHA-1
    - Receiving agents should support MD5 for the purpose of providing backward compatibility
  - **Signature Algorithm Identifier**
    - Sending and receiving agents must support ID-DSA defined in DSS
    - Receiving agents should support RSA Encryption
      - DSS (**Digital Signature Standard)**
      - DSA (digital signature algorithm)

S/MIME

- *Cryptographic Message Syntax (CMS) Options*
  - **Key Encryption Algorithm Identifier**
    - Identifies a key encryption algorithm under which a content encryption key can be encrypted
    - Supports encryption and decryption operations
    - Sending and receiving agents must support
      - Diffie–Hellman key exchange
      - rsa Encryption
    - Incoming encrypted messages contain symmetric keys which are to be decrypted with a user's private key

S/MIME Process



S/MIME

- **General syntax**
  - Support six different content types:
    - Data
    - Signed data
    - Enveloped data
    - Signed-and-enveloped data
    - Digested data
    - Encrypted data
  - Only the data, signed data and enveloped data types are currently used for S/MIME
  - There are two classes of content types
    - Base -Data with no cryptographic enhancement
    - Enhanced - cryptographic enhancements
      - Encrypted
      - Encapsulated -Outer content contains the inner enhanced content

```
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7
77n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHUujhJhjH
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh
6YT64V0GhIGfHfQbnj75
```

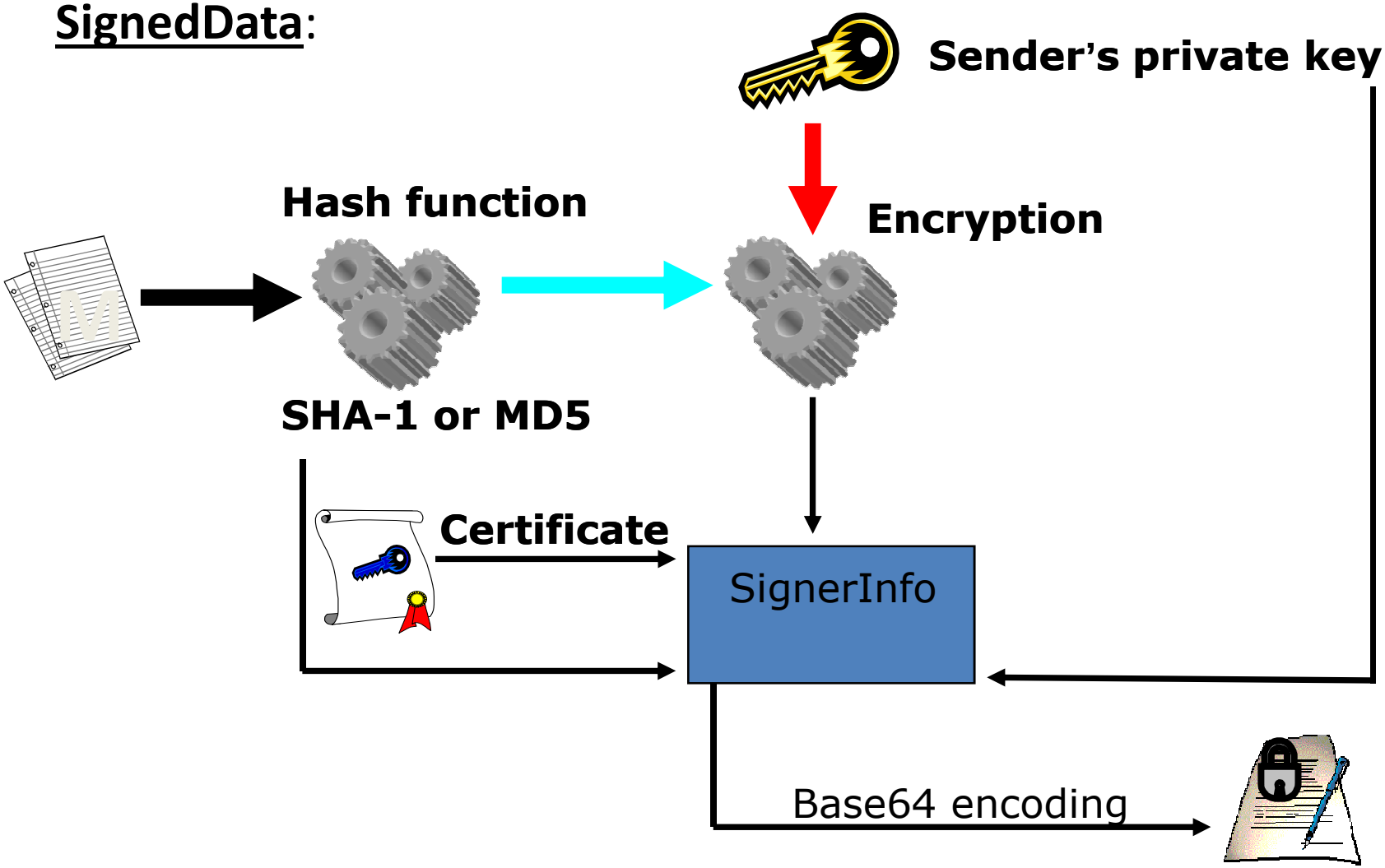
S/MIME

- **General syntax**
  - *Data content type:*
    - *Arbitrary octet strings, such as ASCII text files*
    - Data ::= OCTET STRING
    - Sending agents must use the id-data content-type identifier to indicate the message content

S/MIME

- **General syntax**
  - *Signed-data content type:*
    - Used when a digital signature is applied to a message
    - Any type of content can be signed by any number of signers in parallel
    - Some cases this type convey certificates and CRL
    - Process to construct signed data:
      - A message digest is computed on the content with a signer-specific message digest algorithm
      - A digital signature is formed by taking the message digest of the content to be signed and then encrypting it with the private key of the signer
      - The content plus signature are then encoded using Base64 encoding
      - A recipient verifies the signed-data message by decrypting the encrypted message digest for each signer with the signer's public key, then comparing the recovered message digest to an independently computed message digest.

S/MIME - Message



S/MIME

- **General syntax**
  - *Enveloped-data content type:*
    - content type: *application/prcs7-mime*
    - Privacy protection to a message
    - The type consists of
      - Encrypted content of any type
      - Encrypted-content encryption keys
    - Called a *digital envelope*
    - Any type of content can be enveloped for any number of recipients in parallel

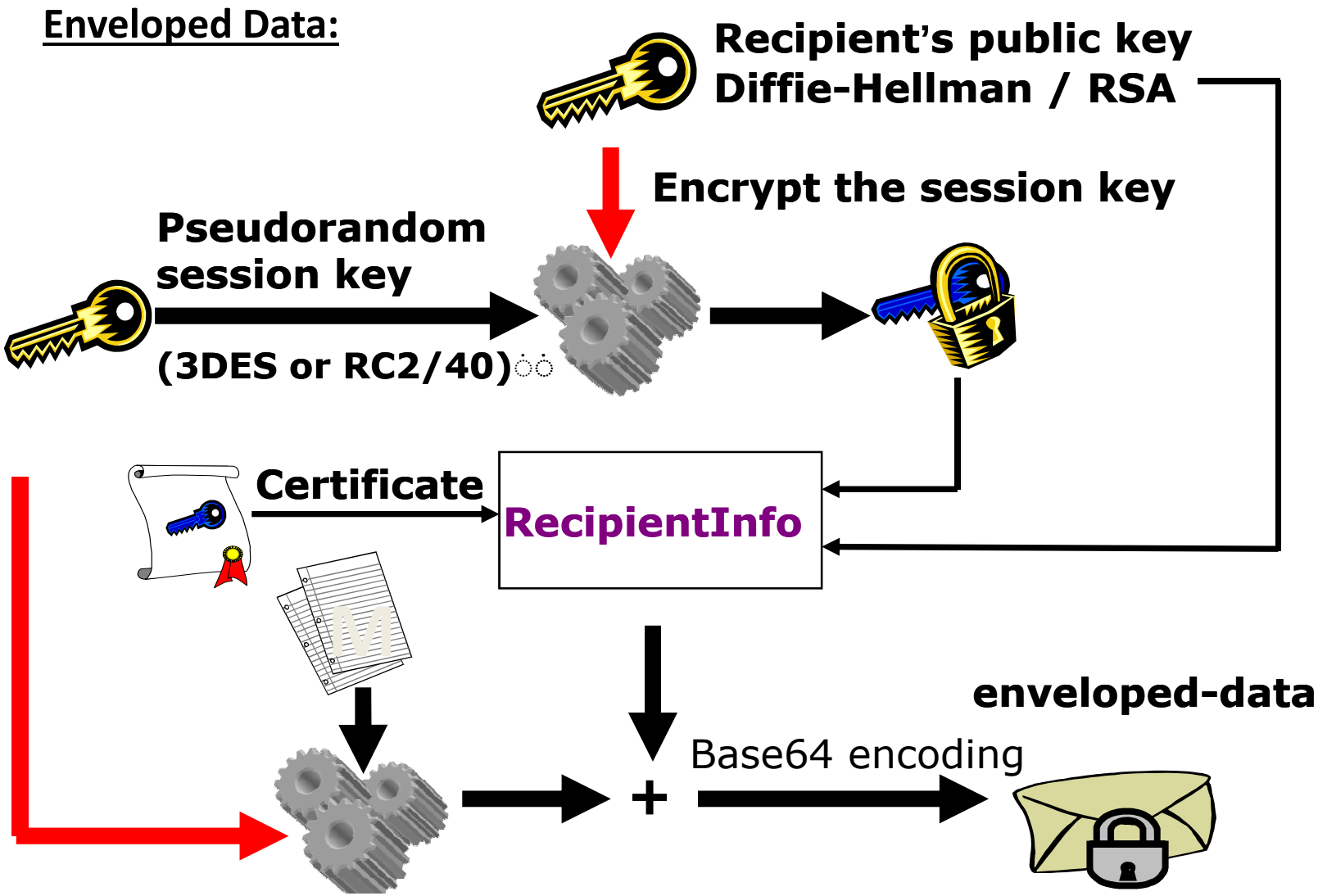
S/MIME

- **General syntax**
  - *Enveloped-data content type:*
    - The process by which enveloped data is constructed involves the following:
      - A content-encryption key (a pseudo-random session key) is generated at random and is encrypted with the recipient's public key for each recipient
      - The content is encrypted with the content-encryption key
      - An EnvelopedData value: The recipient-specific information values for all the recipients
      - This information is then encoded into Base64

S/MIME

- **General syntax**
  - *Enveloped-data content type:*
    - Recipient
      - Remove off the Base64 encoding
      - Opens the envelope by decrypting one of the encrypted content encryption keys with the recipient's private key
      - Decrypt the encrypted content with the recovered content-encryption key (the session key)
    - This content type does not provide authentication

S/MIME - Message



S/MIME

- **General syntax**
  - *Digested-data content type:*
    - *Contains*
      - *Content of any type*
      - *a message* digest of the content
    - Add integrity to content
    - A message digest is computed on the content with a message digest algorithm
    - The message digest algorithm and the message digest are combined with the content into a DigestedData value
    - A recipient verifies the message digest by comparing the message digest to an independently computed message digest

S/MIME

- **General syntax**
  - *Encrypted-data content type:*
    - *Consists*
      - *Encrypted content*
    - Unlike the enveloped-data content type, the encrypted-data content type has neither recipients nor encrypted content-encryption keys.
    - Keys are assumed to be managed by other means
    - Used for local storage of data
    - Key is generally the password

S/MIME

- **Enhanced Security Services for S/MIME**
  - The security services extensions to S/MIME version 3
    - *Triple wrapped message*
      - *A triple* wrapped message is one that has been signed, then encrypted and then signed again
      - The signers of the inner and outer signatures may be different entities or the same entity
      - No limit in the number of nested encapsulations
      - There may be more than three wrappings

S/MIME

- **Enhanced Security Services for S/MIME**
  - Inside signature provides
    - Content integrity
    - Non-repudiation with proof of origin
    - Binding attributes to the original content
      - These attributes go from the originator to the recipient, regardless of the number of intermediate entities such as mail list agents that process the message
      - Signed attributes can be used for access control to the inner body
  - The encrypted body provides
    - confidentiality
  - The outside signature provides
    - Authentication
    - Integrity
    - Binding attributes to the encrypted body
      - These attributes can be used for access control and routing decisions

S/MIME

- **Enhanced Security Services for S/MIME**
  - *Triple Wrapped Message*
    - The steps to create a triple wrapped message are as follows:
      1. Start with the original content (a message body)
      2. Encapsulate the original content with the appropriate MIME content-type headers
      3. Sign the inner MIME headers and the original content
      4. Add an appropriate MIME construct to the signed message

      The resulting message is called the *inside signature*

      – Construct eg: content type of multipart/signed

      content type of application/pkcs7-signature

      optional MIME headers

      a body part

S/MIME

- **Enhanced Security Services for S/MIME**
  - *Triple Wrapped Message*
    5. Encrypt the step 4 result as a single block, turning it into an application/pkcs7-mime object
    6. Add the appropriate MIME headers: a content type of application/pkcs7-mime with parameters, and optional MIME headers such as Content-Transfer-Encoding and Content-Disposition
    7. Sign the step 6 result (the MIME headers and the encrypted body) as a single block
    8. The resulting message is called the *outside signature, and is* also the triple wrapped message

S/MIME

- *Security Services with Triple Wrapping*
  - The **receipt request** must be requested for inside signature, not in the outside signature
  - A secure mailing list agent may change the receipt policy in the outside signature of a triple wrapped message when the message is processed by the mailing list
  - A security label attribute may be included in either the inner signature or the outer signature, or both
    - The inner security label is used for access control decisions related to the original plaintext content
    - The outer security label is used for access control and routing decisions related to the encrypted message.

S/MIME

- *Security Services with Triple Wrapping*
  - Secure mail list message processing depends on the structure of S/MIME layers present in the message
    - The agent never changes the data that was hashed to form the inner signature, if such a signature is present
    - If an outer signature is present, then the agent will modify the data that was hashed to form that outer signature
  - Attributes should be placed in the inner or outer SignedData message
    - Some attributes must be signed
    - Signing is optional for others
    - Some attributes must not be signed
  - Some security gateways sign messages that pass through them
    - If the message is of any type other than a SignedData
      - Gateway Wrapp messgae in a SignedData block and MIME headers and then sign
    - If the message is a SignedData
      - Gateway Can sign the message by inserting SignerInfo into the SignedData block

S/MIME

- *Signed Receipts*
  - Returning a signed receipt provides to the originator **proof of delivery** of a message
  - Receipt allows the originator to demonstrate to a third party that the **recipient was able to verify the signature** of the original message
  - This receipt is **bound to the original message** through the signature
  - This service may be requested **only if a message is signed**
  - The receipt sender may optionally also **encrypt a receipt to provide confidentiality** between the sender and recipient of the receipt

S/MIME

- *Signed Receipts*
  - **The originator** of a message **may request** a signed receipt from the message's recipients
  - The request is indicated by adding a receiptRequest attribute to the signedAttributes field of the SignerInfo object
  - The receiving user agent software should automatically create a signed receipt when requested to do so, and return the receipt
  - Return receipt must fix to mailing list expansion options, local security policies and configuration options

S/MIME

- *Signed Receipts*
  - Receipts involve the interaction of two parties: the sender and the receiver.
  - The sender is the agent that sent the original message that includes a request for a receipt
  - The receiver is the party that received that message and generated the receipt

S/MIME

- *Signed Receipts*
  - The interaction steps in a typical transaction are:
    1. Sender creates a signed message including a receipt request attribute
    2. Sender transmits the resulting message to the recipient(s).
    3. Recipient receives message and determines if there are a valid signature and receipt request in the message
    4. Recipient creates a signed receipt
    5. Recipient transmits the resulting signed receipt message to the sender
    6. Sender receives the message and validates that it contains a signed receipt for the original message

S/MIME

- *Receipt Request Creation*
  - Multilayer S/MIME messages may contain multiple SignedData layers
  - Receipts are requested only for **the innermost Signed Data layer** in a multilayer S/MIME message such as a triple wrapped message
  - **Only one receipt request** attribute can be included in the signed Attributes of SignerInfo