Experiment No. 10

**Aim:** Case study of Secure/Multipurpose Internet Mail Extension (S/MIME)

**Theory:**

Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security. Although both PGP and S/MIME are on an IETF standards track, it appears likely that S/MIME will emerge as the industry standard for commercial and organizational use, while PGP will remain the choice for personal e-mail security for many users. S/MIME is defined in a number of documents—most importantly RFCs 3370, 3850, 3851, and 3852.

In terms of general functionality, S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. In this subsection, we briefly summarize S/MIME capability. We then look in more detail at this capability by examining message formats and message preparation.

S/MIME provides the following functions.

1. Enveloped data: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.
2. 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 base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
3. Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only 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.
4. Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted

S/MIME provides the following cryptographic security services for electronic messaging applications:

* Authentication
* Message integrity
* Non-repudiation of origin (using digital signatures)
* Privacy
* Data security (using encryption)

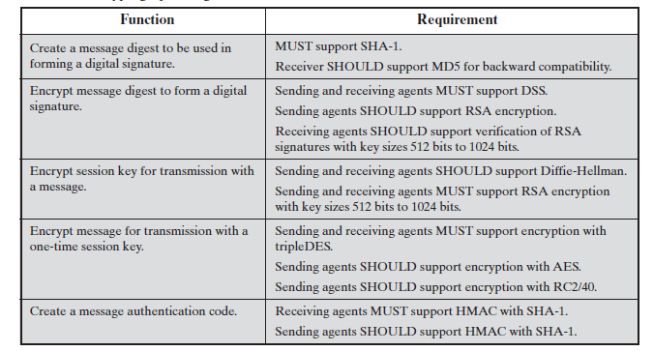
S/MIME specifies the MIME type application/pkcs7-mime (smime-type "enveloped-data") for data enveloping (encrypting) where the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an application/pkcs7-mime MIME entity.

***S/MIME certificates***

Before S/MIME can be used in any of the above applications, one must obtain and install an individual key/certificate either from one's in-house certificate authority (CA) or from a public CA. The accepted best practice is to use separate private keys (and associated certificates) for signature and for encryption, as this permits escrow of the encryption key without compromise to the non-repudiation property of the signature key. Encryption requires having the destination party's certificate on store (which is typically automatic upon receiving a message from the party with a valid signing certificate). While it is technically possible to send a message encrypted (using the destination party certificate) without having one's own certificate to digitally sign, in practice, the S/MIME clients will require the user to install their own certificate before they allow encrypting to others.

A typical basic ("class 1") personal certificate verifies the owner's "identity" only insofar as it declares that the sender is the owner of the "From:" email address in the sense that the sender can receive email sent to that address, and so merely proves that an email received really did come from the "From:" address given. It does not verify the person's name or business name. If a sender wishes to enable email recipients to verify the sender's identity in the sense that a received certificate name carries the sender's name or an organization's name, the sender needs to obtain a certificate ("class 2") from a CA who carries out a more in-depth identity verification process, and this involves making inquiries about the would-be certificate holder.

Depending on the policy of the CA, the certificate and all its contents may be posted publicly for reference and verification. This makes the name and email address available for all to see and possibly search for. Other CAs only post serial numbers and revocation status, which does not include any of the personal information. The latter, at a minimum, is mandatory to uphold the integrity of the public key infrastructure.



***Obstacles to deploying S/MIME in practice***

S/MIME is sometimes considered not properly suited for use via webmail clients. Though support can be hacked into a browser, some security practices require the private key to be kept accessible to the user but inaccessible from the webmail server, complicating the key advantage of webmail: providing ubiquitous accessibility. This issue is not fully specific to S/MIME: other secure methods of signing webmail may also require a browser to execute code to produce the signature; exceptions are PGP Desktop and versions of GnuPG, which will grab the data out of the webmail, sign it by means of a clipboard, and put the signed data back into the webmail page. Seen from the view of security this is a more secure solution. Kopano, an email office suite providing webmail as well as backend for Microsoft Outlook and mobile devices, provides a full and secure S/MIME implementation within their webmail solution.

S/MIME is tailored for end-to-end security. Logically it is not possible to have a third party inspecting email for malware and also have secure end-to-end communications. Encryption will not only encrypt the messages, but also the malware. Thus if mail is scanned for malware anywhere but at the end points, such as a company's gateway, encryption will defeat the detector and successfully deliver the malware. The only solution to this is to perform malware scanning on end user stations after decryption. Other solutions do not provide end-to-end trust as they require keys to be shared by a third party for the purpose of detecting malware. Examples of this type of compromise are:

* Solutions which store private keys on the gateway server so decryption can occur prior to the gateway malware scan. These unencrypted messages are then delivered to end users.
* Solutions which store private keys on malware scanners so that it can inspect messages content, the encrypted message is then relayed to its destination.
* Due to the requirement of a certificate for implementation, not all users can take advantage of S/MIME, as some may wish to encrypt a message, with a public/private key pair for example, without the involvement or administrative overhead of certificates.

Any message that an S/MIME email client stores encrypted cannot be decrypted if the applicable key pair's private key is unavailable or otherwise unusable (e.g., the certificate has been deleted or lost or the private key's password has been forgotten). However, an expired, revoked, or untrusted certificate will remain usable for cryptographic purposes. Indexing of encrypted messages' clear text may not be possible with all email clients. Neither of these potential dilemmas is specific to S/MIME but rather ciphertext in general and do not apply to S/MIME messages that are only signed and not encrypted.

S/MIME signatures are usually "detached signatures": the signature information is separate from the text being signed. The MIME type for this is multipart/signed with the second part having a MIME subtype of application/(x-)pkcs7-signature. Mailing list software is notorious for changing the textual part of a message and thereby invalidating the signature; however, this problem is not specific to S/MIME, and a digital signature only reveals that the signed content has been changed.

**Conclusion:**

To summarize the state of secure e-mail software, we can say that software exists now to establish trust between two individuals or within a small group so they can exchange text-based e-mail. Software is available to secure MIME-based e-mail in a similar manner, although it is not nearly as widespread and is mostly available commercially.