Privacy Enhanced Mail (PEM) Secure Multipurpose Internet Mail Extensions (S/MIME)

General Principles

IETF Specs for PEM and S/MIME

- RFC 1421 PEM Message Format
- RFC 1422 PEM CA Hierarchy
- RFC 1423 Cryptographic Algorithms for PEM
- RFC 1424 Certificate and CRL Comms for PEM
- RFC 2045 MIME
- RFC 2633 S/MIME

PEM Overview (I)

- Assumes security only at source and destination – mail gateways must see “standard mail”
- Supports private and public key algorithms
- Standard practice is private key systems for encryption and public key systems for authentication and key management

PEM Overview (II)

- Supports RSA, DSS, DES, 3DES and AES
- Allows different parts of message different levels of security
- Each part has marker before and after (e.g. *begin privacy – enhanced message* and *end privacy – enhanced message*)

PEM Security Levels

- *unsecured* data
- *integrity protected unmodified* data (**MIC-CLEAR**) – assumes mail infrastructure will not alter message
- *integrity protected encoded* data (**MIC-ONLY**) – encoding designed to prevent modification by mail infrastructure
- *encoded encrypted integrity- protected* data (**ENCRYPTED**) integrity – encrypt - encode

Establishing Encryption Keys

- Per-message encryption key randomly selected
- Encryption key encrypted under destination public key
- Destination public key provided with certificate and CA chain

PEM Certificates

- Based on X.500 names
- PEM Header contains certificates
- Hierarchical naming scheme A/B/C/D/E
  - A issues certificates for B
  - B issues certificates for C etc
- E.g. A = country = UK
  B = organisation type = academic
  C = university = Imperial
  D = department = EEE
  E = name = A.N. Other

PEM Certificate Hierarchy (I)

- Root CA is Internet Policy Registration Authority
- Operating under root CA are Policy Certification Authorities
- 3 levels of security policy
  - High Assurance
  - Discretionary Assurance
  - No Assurance

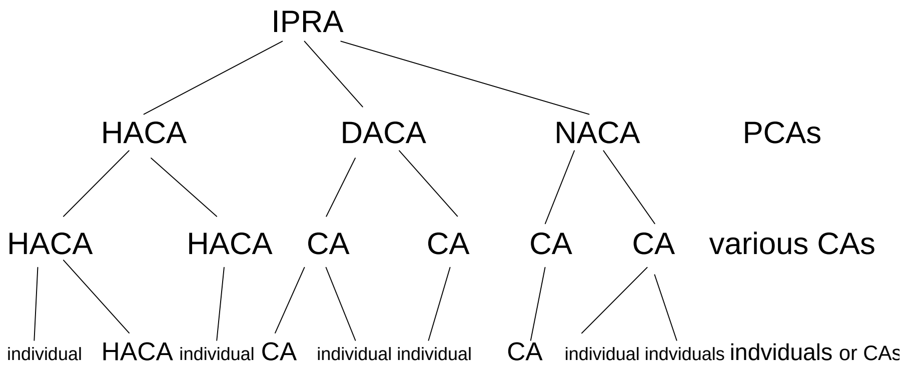
High Assurance

- Strong physical security for certificate production and tamper-resistance for private key used in certification
- Strict personnel security
- Will not grant certificates to organisations with lower levels of security

Discretionary and No Assurance

- Discretionary Assurance
  - security management as for High Assurance
  - no restriction on those to whom it grants certificates
- No Assurance
  - issues certificates without any constraints

PEM Certificate Hierarchy



N.B. No cross-links allowed in certificate chain

Encryption

- Randomly selected private key
- CBC mode used with 64-bit Initialisation Vector (IV)
- In PEM IV adds complexity to exhaustive key search on known plaintext

Source Authentication and Integrity Protection

- Add Message Integrity Code (MIC)
- Initial message digest uses MD2 or MD5
- Message digest signed with private key of public key pair

S/MIME

- MIME is generally a multipart message
- application/pkcs7 – signature holds detached signatures within a multipart signed structure
- application/pkcs7 – mime allows a multipart signed message to be signed and encrypted

S/MIME Certificate Hierarchy

- S/MIME does not specify a particular PKI
- PKI options are
  - Public certifier in which a business issues certificates with various levels of cost/assurance
  - Organisational certifier (e.g. an employer)
  - Certificates from any CA