S/MIME Version 3.x
Certificate Handling

- Thomas Donner -
Based on

- RFC 2632
- Draft IETF S/MIME RFC 2632bis 05
Agenda

- Certificates
  - Introduction
  - Composition
  - Public Key Infrastructure (PKI)
  - Validity
  - Example

- S/MIME Certificate Handling
  - Introduction
  - Cryptographic Message Syntax (CMS)
  - Contents
  - Certificate Processing
  - Inhibition
  - Security
  - Changes from Version 3.0 to Version 3.1
Part of the cryptographically field of “Key Exchange and Entity Authentication”

- Examples
  - Kerberos (Secure-Network-Communication)
  - Diffie-Hellmann key agreement (pk cryptography)
  - Key exchange with mutual authentication
  - Station-to-Station protocol (ISDN telephone security)
  - PK management techniques
    - Certificates
Certificates
- Introduction 2/2-

- How it works (basically)…

Alice wants to encrypt a message or verify a signature allegedly produced by Bob.

Alice retrieves Bob’s certificate (either from Bob or from a certificate directory).

Alice verifies the certification authority’s signature.

If the verification is successful, Alice can be sure she received the public key from Bob’s certificate and so she now can use it.

Trusted party C
Certificates
- Composition -

- ITU – Standard X.509 V.3

**Signature of the issuer**
- Version (e.g. X.509v3)
- Serial number
- Signature- and hashalgorithm
- Issuer
- Validity
  - not before
  - not after
- Subject
- Public key of the subject
- Extensions
  - 1..n

**Global unique ID**

**Composition**
- CN = Name of the instance
- OU = Division within the organization
- O = Organization
- L = Location
- S = federal state (only for America)
- C = Country

© Thomas Donner
Certificates
- Public Key Infrastructure -

- Composition
  - Root instance (signed by the root itself)
  - Certification authorities (CA) (signed by the root)
  - Users (signed by a CA)

- Possible for SSL, E-Mail, S/MIME, …
Certificates
- Validity -

- Normal period of validity
  - Root: 20 years at least
  - CA: 5 to 10 years
  - Users: 1 year (mostly)

- Invalid certificates: Certificate Revocation List (CRL)

- Reasons for becoming invalid
  - Something changed
  - Private key has been lost/ cracked
  - The certificate has been certificated wrong
Certificates
- Example -
S/MIME Certificate Handling
- Introduction -

Sending Agent → Internet → Mail Server with S/MIME support → Receiving Agent

My order

Decrypt and scan for viruses

My order
S/MIME Certificate Handling
- Cryptographic Message Syntax (CMS) -

- Defined in RFC 2630 and RFC 2633
- Certificate Revocation List (CRL)
  - Syntax defined in RFC 2459
  - Must be supported by both Agents
- Certificate Choice
  - Agents must support PKIX v2 and v3
  - Agents should support X.509 attribute certificates
- Certificate Set
  - Sending Agents should include the CL up to (but without) the CA or root that it believes that the recipient may trust as authoritative
  - Receiving Agents should be able to handle messages without certificates by using a database or directory lookup scheme
The “Subject” is not always a “distinguished name”, but often something arbitrarily in practice.

Recommendation of using an email address, as described in RFC 822, as unique id in the “subjectAltName” – Field of the extensions.
S/MIME Certificate Handling
- Contens 2/3 -

- Problem:

- Not signed

  Date: Tue, 20 Apr 2004 12:34:56 +0200
  From: name@host.network
  Subject: Text
  To: name2@host.network
  Mime-Version: 1.0
  Content-Type: text/plain; charset =“iso-8859-1”
  Content-Transfer-Encoding: quoted-printable

- Signed

  Some Text
S/MIME Certificate Handling
- Contens 3/3 -

Solution:

- Sending agent: From field should match an Internet mail address in the signer’s certificate
- Receiving agent must check that these both addresses are a match, if this fails the recipient should be displayed a message with details of the certificate
- This means, all subject and issuer names must be populated, or the certificate will not be accepted.

[But exceptions possible (look RFC 2632 section 3)]
S/MIME Certificate Handling
- Certificate Processing 1/3 -

- Certificate retrieval mechanisms CRM
  - X.500 directory service (ITU)
  - Directory Servers (PKIX Workgroup)
  - Certificate retrieval services based on DNS (IETF)
  - Minimum: local “address book” of certificates

- Certificate revocation list CRL
  - Updated automatically in a specific interval and for each verification of a certificate by a CA
  - Agents should be able to recognize CRL’s in a message

- Im- and export of certs/ CRL’s must be supported
S/MIME Certificate Handling
- Certificate Processing 2/3 -

- Certificate chain validation CCV
  - Must be performed before using the public key of Bob
  - Incoming certs/ CRL’s should be cached for use in CCV and be used to augment other CRM

- Certificate and CRL signing algorithms
  - S/MIME Version 2:
    - Hash: MD-5, SHA-1
    - Signatur: RSA (512- 2048bit)
  - S/MIME Version 3:
    - Hash: SHA-1, MD-5
    - Signatur: DSA (DSS), RSA (512- 2048bit)
S/MIME Certificate Handling
- Certificate Processing 3/3 -

- PKIX certificate extensions
  - Basic constrains certificate extension
  - Key usage certificate extension
    - Key usage in Diffie-Hellmann key exchange certificates
  - Subject alternative name extension
S/MIME Certificate Handling
- Inhibition -

- CRL’s
  - Problem:
    - Needs to be updated every day, for each stored CA. (size!)
    - You are not interested in invalid certs you don’t even know

- Online Certificate Status Protocol (RFC 2560)
  - Allows you to view the actual validity online, signed by a CA
  - Problem:
    - Each inquiry has to be signed and send off (traffic!)
    - So, only suitable for emails with a high security demand

- Possible Solution: Combination of CLR’s and OCSP
S/MIME Certificate Handling
- Security -

- Certificate checking might fail because:
  - No internet mail address in the cert matches the sender
  - No certificate chain leads to a trusted CA
  - No ability to check the CRL for a certificate
  - An invalid CRL was received
  - The CRL being checked is expired
  - The certificate is expired
  - The certificate has been revoked

- How does the user/ software handle this?
S/MIME Certificate Handling
- Changes from Version 3.0 to Version 3.1 -

- Several CA’s with the same subject and pk but different validity periods must be supported
- Version 2 cert attributes should be supported
- Version 1 cert attributes must not be used
- MD2 use for certificate signature discouraged, and security language added
- Clarified use of email address use in certificates
- Results of a verification should be displayed
- Signatures with the “digitalSignature” or “nonRepudiation” bit unset are to refuse
- Clarifications for the interpretation of the key usage and extended usage extensions (Draft Section 4.4.4)