

S/MIME

(Secure/Multipurpose Internet Mail Extension)

S/MIME

(Secure/Multipurpose Internet Mail Extension)

- Originated from RSA Data Security Inc. in 1995.
- Further development by IETF S/MIME working group at: www.ietf.org/html.charters/smime-charter.html.
- Version 3 specified in RFCs2630-2634.
- Allows flexible client-client security through encryption and signatures.
- Widely supported, e.g. in Microsoft Outlook, Netscape Messenger, Lotus Notes.

S/MIME

- MIME is an extension to RFC-822 framework that is intended to address some of the problems and limitations of the use of SMTP.
- 🔒 S/MIME (**Secure/Multipurpose Internet Mail Extension**) is a security enhancement to the MIME Internet e-mail format standard.
- 🔒 S/MIME is ***not restricted to mail***; it can be used with any transport mechanism that transports MIME data, such as HTTP.
- 🔒 S/MIME is ***likely to emerge as the industry standard*** for commercial and organizational use, while PGP will remain the choice for personal e-mail security for many.

S/MIME - Overview

🔒 S/MIME provides the following cryptography security services:

- ✓ Authentication.
 - ✓ Message Integrity.
 - ✓ Non-repudiation of origin.
 - ✓ Privacy and data security.
- By using digital signing
- By using encryption

🔒 There are three versions of S/MIME:

- S/MIME version **1 (1995)**- was specified and officially published in 1995 by RSA Security, Inc.
- S/MIME version **2 (1998)**- was specified in a pair of informational RFC documents - RFC 2311 and RFC 2312 - in March 1998.
- The work was continued in the IETF S/MIME Mail Security (SMIME) WG and resulted in S/MIME version **3 (1999)** specified in RFCs 2630 to 2634 in June 1999.

MIME - Overview


- 🔒 RFC 822 defines a format for text messages that are sent using electronic mail.

SMTP/RFC822 scheme limitations:

1. SMTP **cannot** transmit **executable files** or other **binary** files.
2. SMTP **cannot** transmit text data that includes **national language characters** because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to **7-bit ASCII**.
3. SMTP servers may **reject** mail message **over** a **certain size**.
4. SMTP gateways that translate between ASCII to EBCDIC **suffer translation problems**.
5. Some SMTP implementations do not adhere completely to the SMTP standard defined in RFC 822.

MIME (contd.)

MIME specification includes the following elements:

1. Five new message header fields. These fields provide information about the body of the message.
 2. A number of content formats are defined, thus standardizing representations that supports multimedia e-mail.
 3. Transfer encodings are defined that enable that protect any content format to be altered by the mail system.
-
-  MIME provides a standardized way of dealing with a wide variety of information representations in a multimedia environment.

MIME (contd.)

Here is a summary of the different MIME content types:

Type	Subtype	Description
Text	Plain Enriched	Unformatted text (ASCII or ISO 8859). Provides greater format flexibility.
Multipart	Mixed Parallel Alternative Digest	The different parts are independent but are to be transmitted together. Should be presented to the receiver in their original order. Differs from mixed only in that no order is defined. The different parts are alternative versions of the same information. Similar to Mixed but the default type/subtype of each part is message/rfc822.
Message	rfc822 Partial External body	The body is itself an encapsulated message that conforms to RFC822. Used to allow fragmentation in a transparent way to the recipient. Contains a pointer to an object exists else where.

MIME (contd.)

Type	Subtype	Description
Image	Jpeg gif	The image is in JPEG format. The image is in GIF format.
Video	Mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8kHz
Application	Postscript Octet-stream	Adobe Postscript. General binary data consisting of 8-bit bytes.

MIME (contd.)

- 🔒 The other major component of MIME is a definition of transfer encodings for message contents:

Encoding	Description
7bit	The data are all represented by short lines of ASCII chars.
8bit	The lines are short, but there may be non-ASCII chars.
Binary	Not only may non-ASCII chars be presented but lines are not necessarily short enough for SMTP transport.
Quoted-printable	Encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
Base64	Encodes data by mapping 6-bit blocks to 8-bit printable ASCII characters blocks.
x-token	A nonstandard encoding.

S/MIME - Functions

🔒 **S/MIME is based on the Cryptographic Message Syntax (CMS) specified in RFC 2630.**

🔒 **Enveloped data:**

This consists of encrypted content of any type and encrypted content encryption keys for one or more users. This functions provides **privacy and data security**.

🔒 **Signed data:**

A digital signature is formed by signing the message digest by encrypting that with the signer private key. The content and the signature are then encoded using base64 encoding.

This function provides **authenticity, message integrity and non-repudiation of origin**.

S/MIME - Functions

🔒 **SignerInfo:** allows the inclusion of unsigned and signed attributes to be included along with a signature.

- signingTime
- sMIMECapabilities
- sMIMEEncryptionKeyPreference

🔒 **Clear signed data:**

In this case a digital signature of the content is formed, However only the signature is encoded with base64.

🔒 **Signed and enveloped data:**

Because of S/MIME encapsulating capability (multipart type), signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data may be encrypted.

S/MIME - Cryptography

Used Algorithms:

Function	Requirement
Creation of a message digest.	MUST use SHA-1 . Receiving agents SHOULD support MD5 for the purpose of providing backward compatibility with S/MIME v2.
A message digest encryption to form a digital signature.	Both sending and receiving agents MUST support DSS . Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits. Note that S/MIME v2 clients are only capable of verifying digital signatures using RSA.

S/MIME - Cryptography

Function	Requirement
A session key encryption for transmission with the message.	Both sending and receiving agents MUST support Diffie-Hellman . Sending agents SHOULD support RSA encryption with key sizes 512 to 1024 bits. Receiving agents SHOULD support RSA decryption.
A message Encryption for transmission with one-time session key.	Sending an receiving agent MUST support Encryption/Decryption with 3DES . Receiving agents SHOULD support decryption with RC2/40 . (S/MIME V 2. - Sending agents SHOULD support RSA encryption with 3DES and RC2/40. Receiving agents MUST support decryption with RC2/40.)

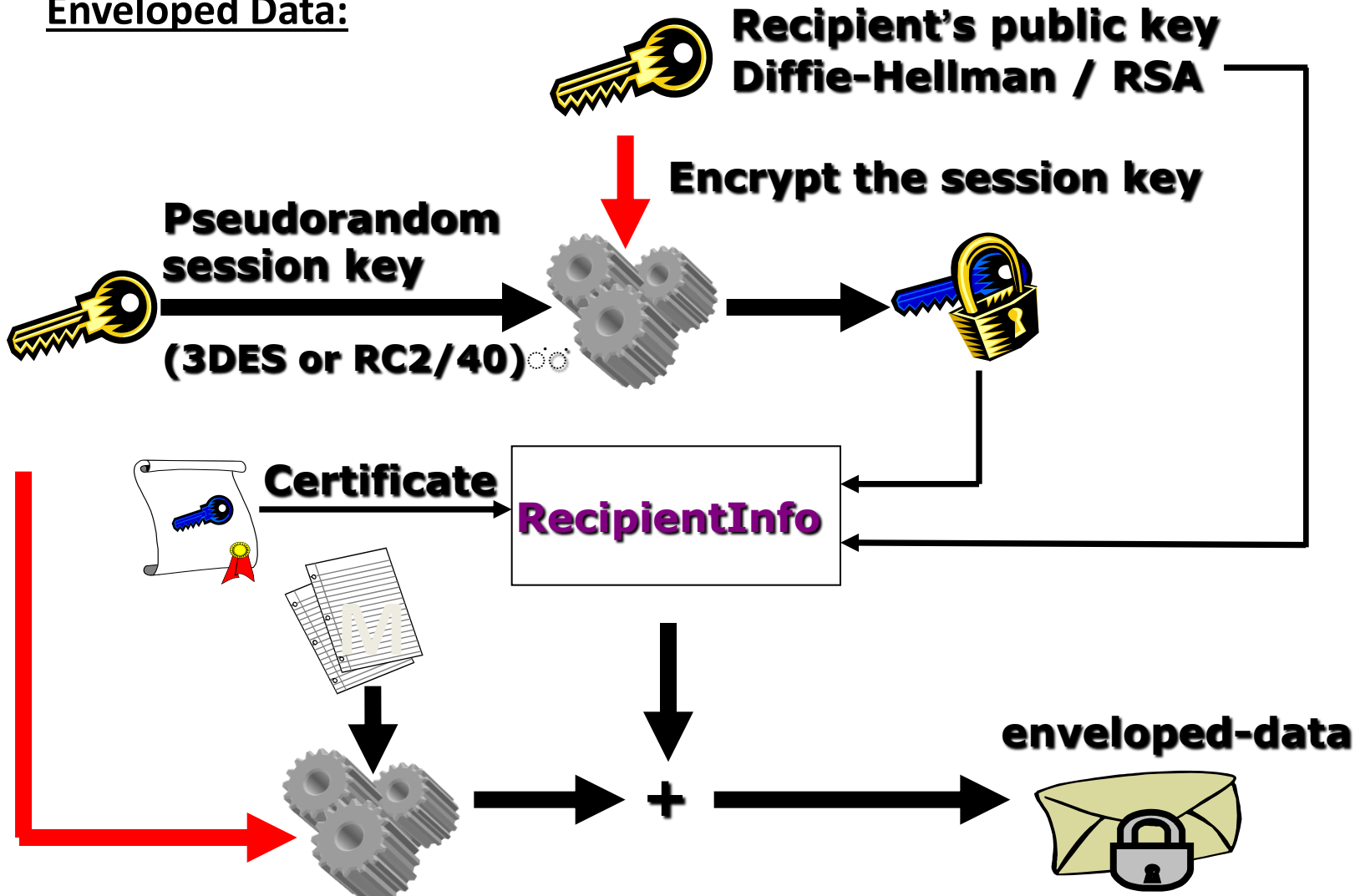
S/MIME - Message

🔒 S/MIME makes use of a number of new MIME content types:

Type	Subtype	S/MIME parameter	Description
Multipart	Signed		A clear message in two parts: One is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	Pkcs7-signature	--	multipart/signed message.
	pkcs10-mime	--	A certificate registration request message.

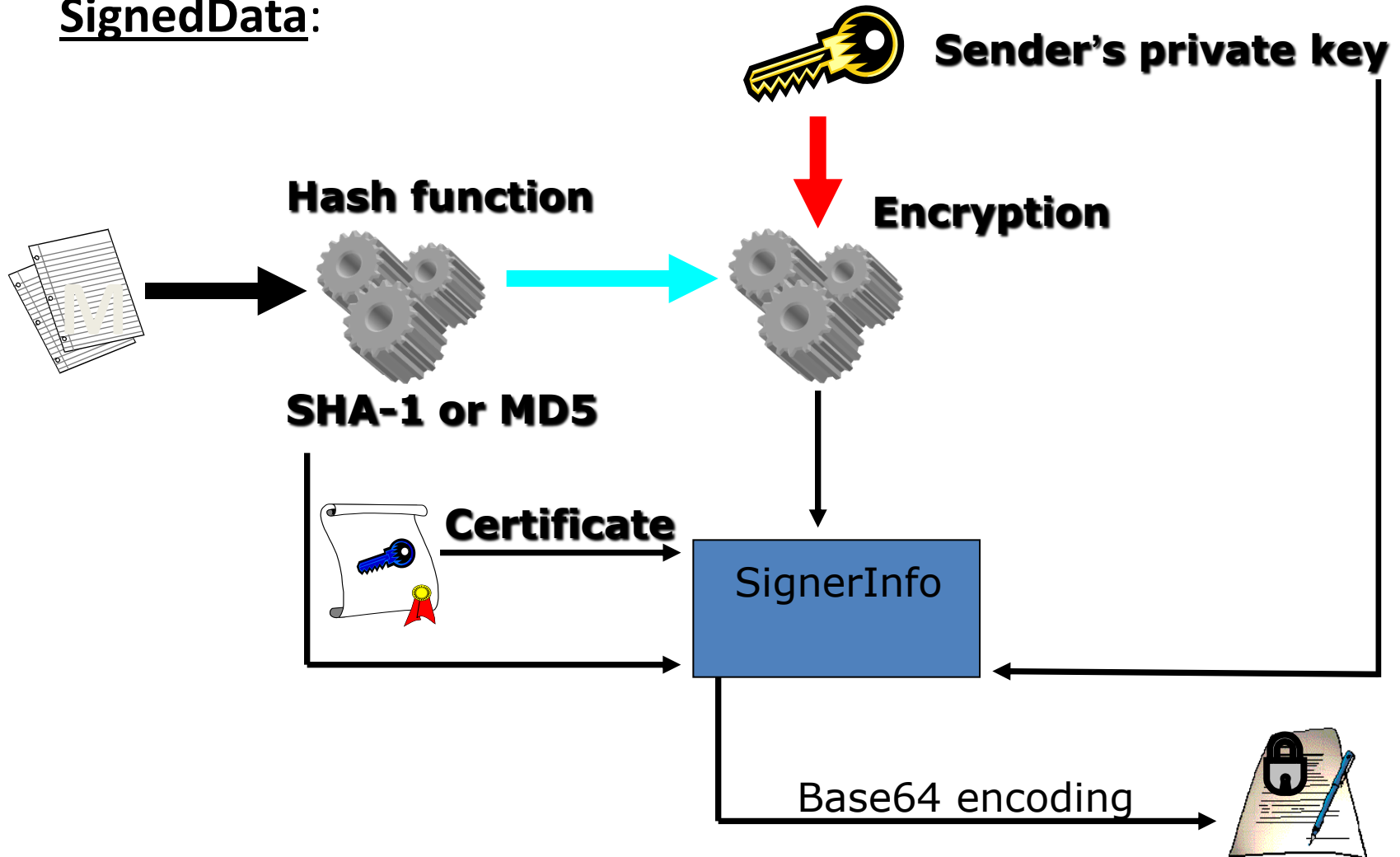
S/MIME - Message

Enveloped Data:



S/MIME - Message

SignedData:



S/MIME - Message

Content-Type: multipart/signed;
protocol="application/pkcs7-signature";
micalg=sha1; boundary=boundary42

This parameter indicates that this is a two part clear-signed entity.

--boundary42

Content-Type: text/plain

This parameter indicates the type of message digest used.

This is a clear-signed message.

--boundary42

Content-Type: application/pkcs7-signature;

name=smime.p7s

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7s

SignerInfo
Header

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jh77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4

--boundary42--

Unsigned
Data

S/MIME - Message

Certificate-only message:

- 🔒 Used to transport certificates.
- 🔒 contains only certificates or a certificate revocation list (CRL).
- 🔒 Sent in response to a registration request.
- 🔒 The message is an application/pkcs7-mime type/subtype.

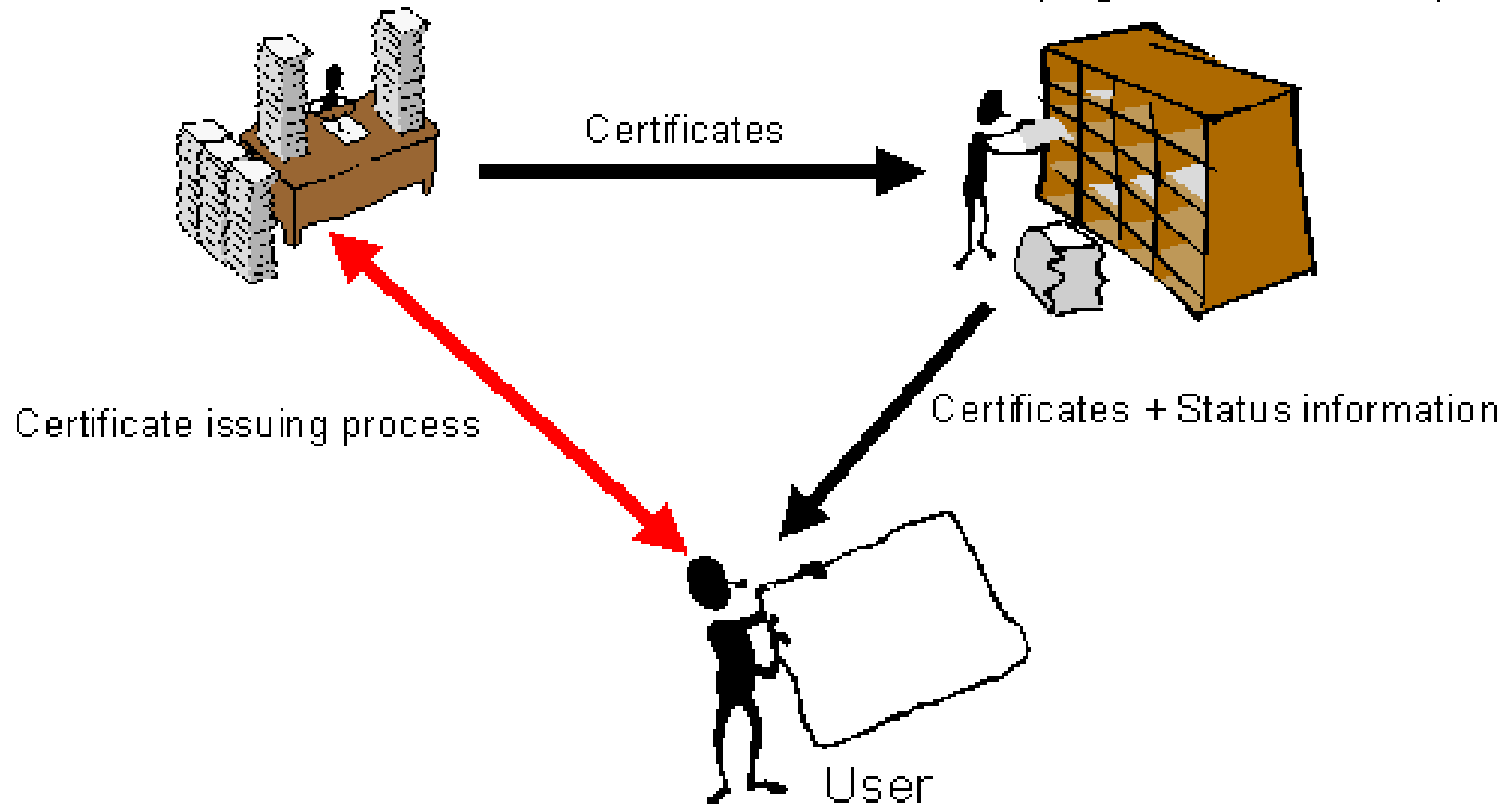
S/MIME - Certificates

- 🔒 S/MIME uses public-key certificates that conform to version 3 of X.509.
- 🔒 A hybrid between a strict X.509 certification hierarchy and PGP's web of trust.
- 🔒 A receiving agent **MUST** provide some certificate retrieval mechanism.
- 🔒 Receiving and sending agents **SHOULD** also provide a mechanism to allow a user to "store and protect" certificates

S/MIME - Certificates

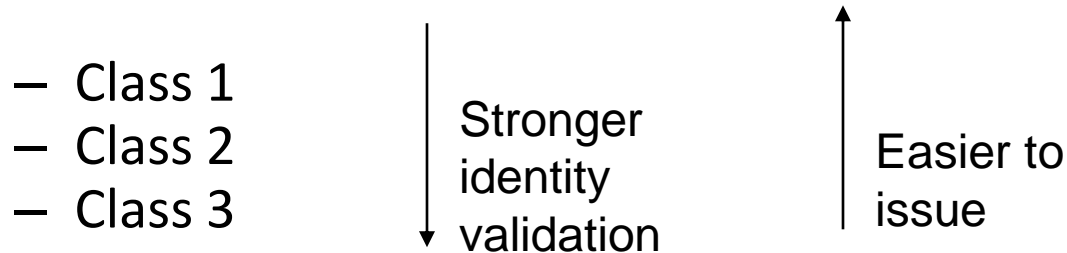
Certification Authority (CA)
and Registration Authority (RA)

Directory service
(e.g. LDAP server)



S/MIME Certificate Processing and CAs

- One should obtain a certificate from a CA in order to send signed messages
- Certificates classes (common practice by most CAs)



- CA certification policies (Certificate Practice Statement)
 - ID-control practices
 - Class 1: only email address check
 - Class 2: class1 + against third party database / fax documents
 - Class 3: class1 + apply in person and submit picture IDs and/or paper documents

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
- have a procedure to decide which algorithms to use