4. Protocoale de Securitate la Nivel Aplicaţie

Securitatea la nivel aplicaţie

- **Pretty Good Privacy (PGP)**
- **Secure Multipurpose Internet Mail Extensions (S/MIME)**
- Secure Shell (SSH)

...

Pretty Good Privacy

- Phil Zimmerman, 1991
- Aplicaţie pentru protecţia mesageriei electronice şi a fişierelor stocate local
- Bazat pe algoritmi criptografici moderni
- Cod sursă disponibil free
- Disponibil pentru diferite tipuri de platforme (Windows, Unix, Mac OS, etc.)
- Standard Internet
  - OpenPGP Message Format (IETF RFC 4880)
  - MIME Security with OpenPGP (IETF RFC 3156)

Servicii oferite

1. Autentificare
2. Confidenţialitate
3. Compresie date
4. Compatibilitate e-mail

Notaţii

Ks – cheie de sesiune

KRa – cheia privată a utilizatorului A

KUa – cheia publică a utilizatorului A

EP – proces de criptare cu chei publice

DP – proces de decriptare cu chei publice

EC - proces de criptare cu chei simetrice

DC - proces de decriptare cu chei simetrice

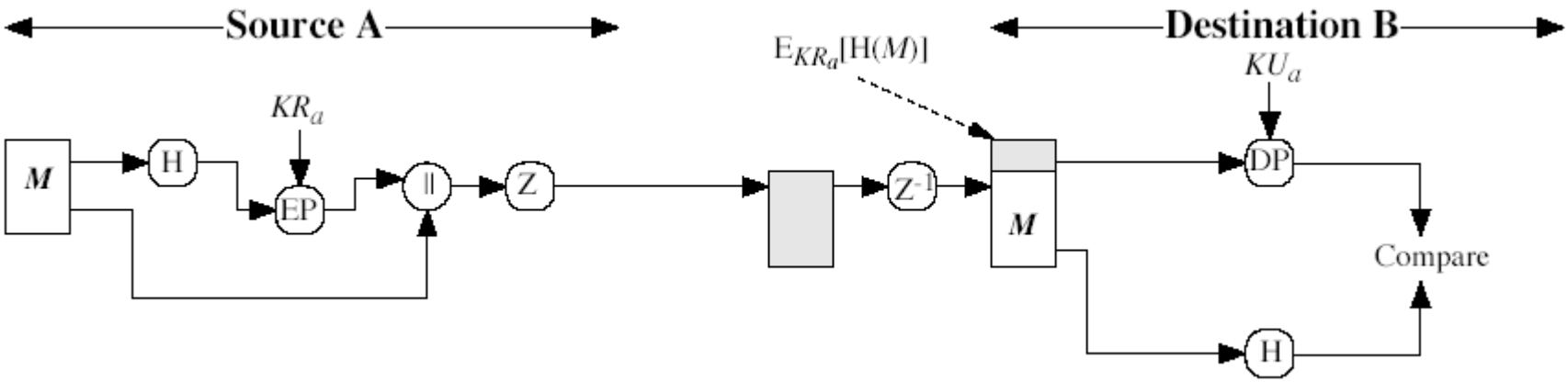
H – funcţie hash

|| - concatenare

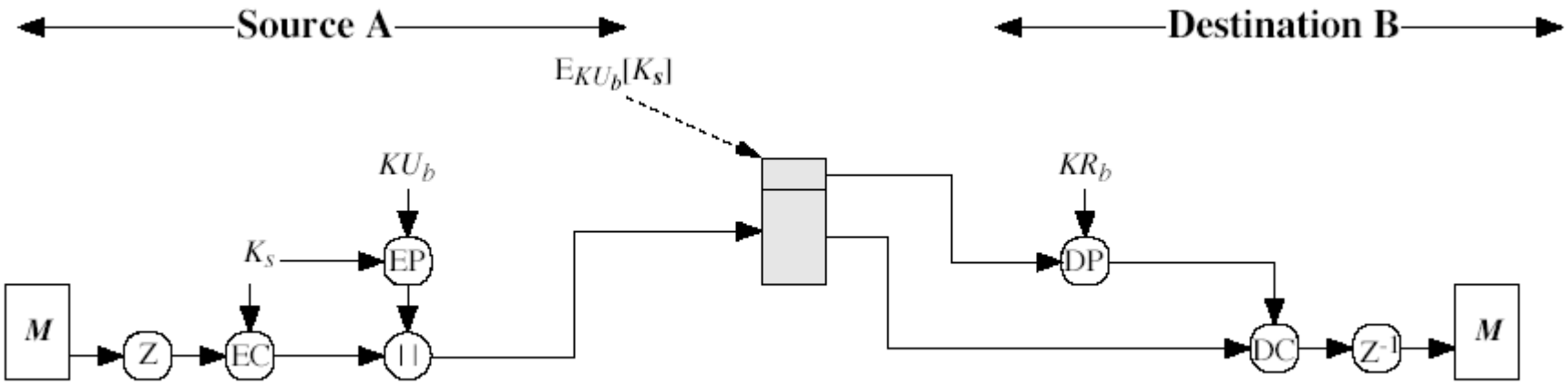
Z – compresie

R64 – conversie Radix 64

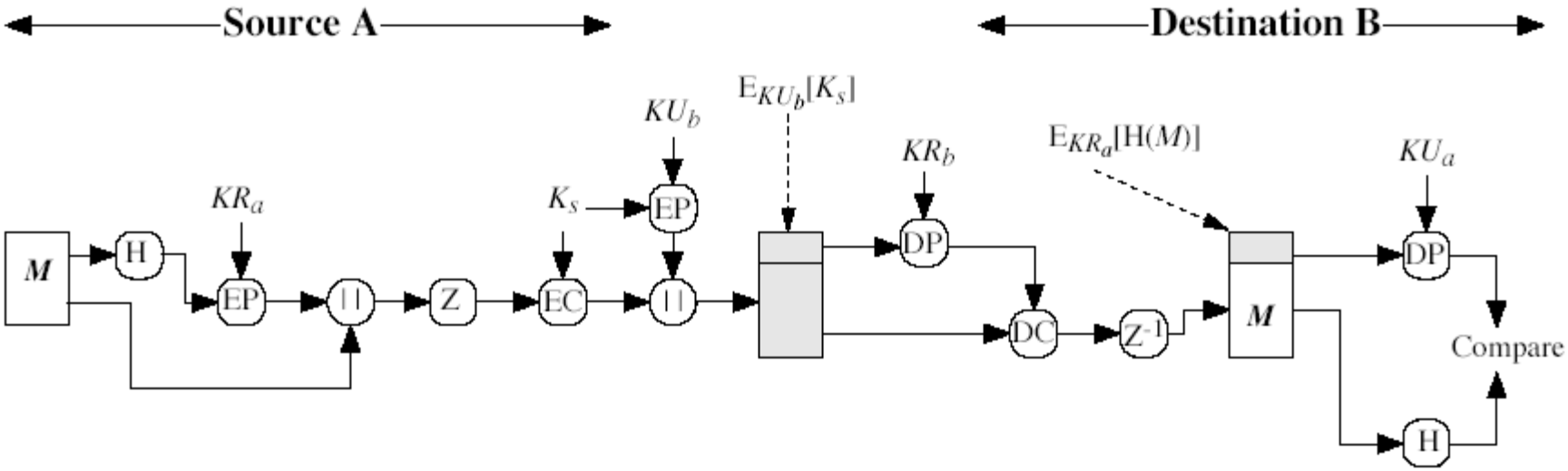
Autentificare



Confidenţialitate



Autentificare şi confidenţialitate



Compresie date

- Opţional, PGP poate comprima datele pentru a reduce durata procesărilor şi încărcarea reţelei
- Compresia datelor se aplică înainte de criptare
- Algoritmul de compresie: ZIP / UNZIP

Compatibilitate e-mail

- Mesajele semnate şi criptate sunt în format binar (pot conţine orice octet nu numai octeţi tipăribili)
- Sistemele de mesagerie electronică suportă numai mesaje text
- Conversie Radix 64:
  - 3 blocuri de 8-biţi → 4 blocuri de 6-biţi
  - creşte dimensiunea mesajelor cu 4/3 (x1,33)

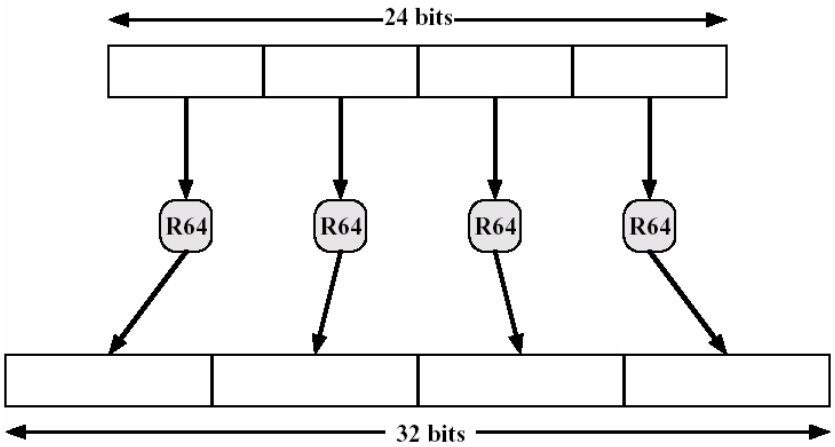


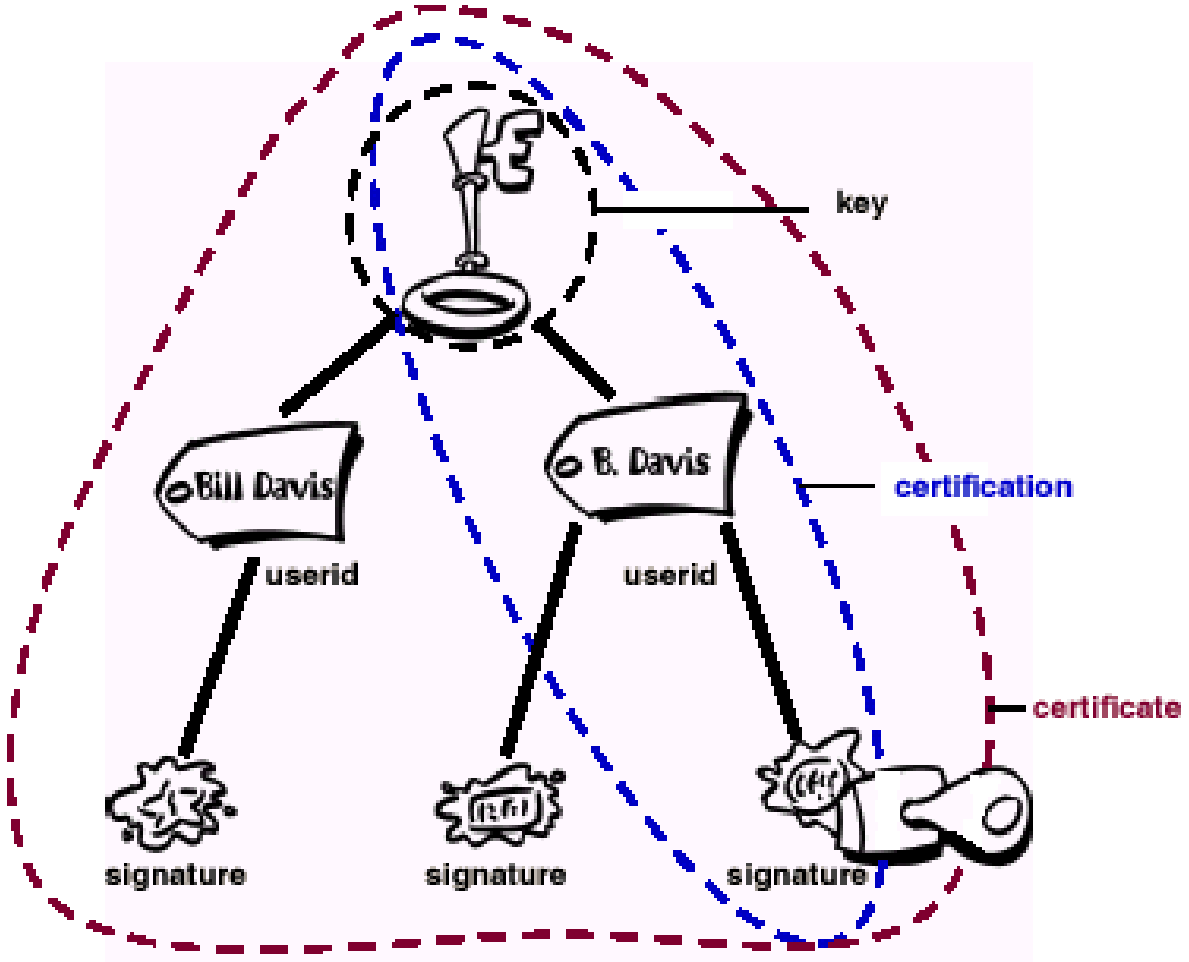
Tabela Radix-64

6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding	6 bit value	Character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

Gestiunea cheilor

- Modelul plasa de încredere (Web of Trust)
  - recomandări de la persoane de încredere
  - Self-Managing Security Architecture
- Inele de chei
  - Public Key Ring
  - Private Key Ring
- Distribuţie
  - floppy disk
  - e-mail (amprente de chei pentru validare)
  - servere de chei PGP

Certificat Digital PGP

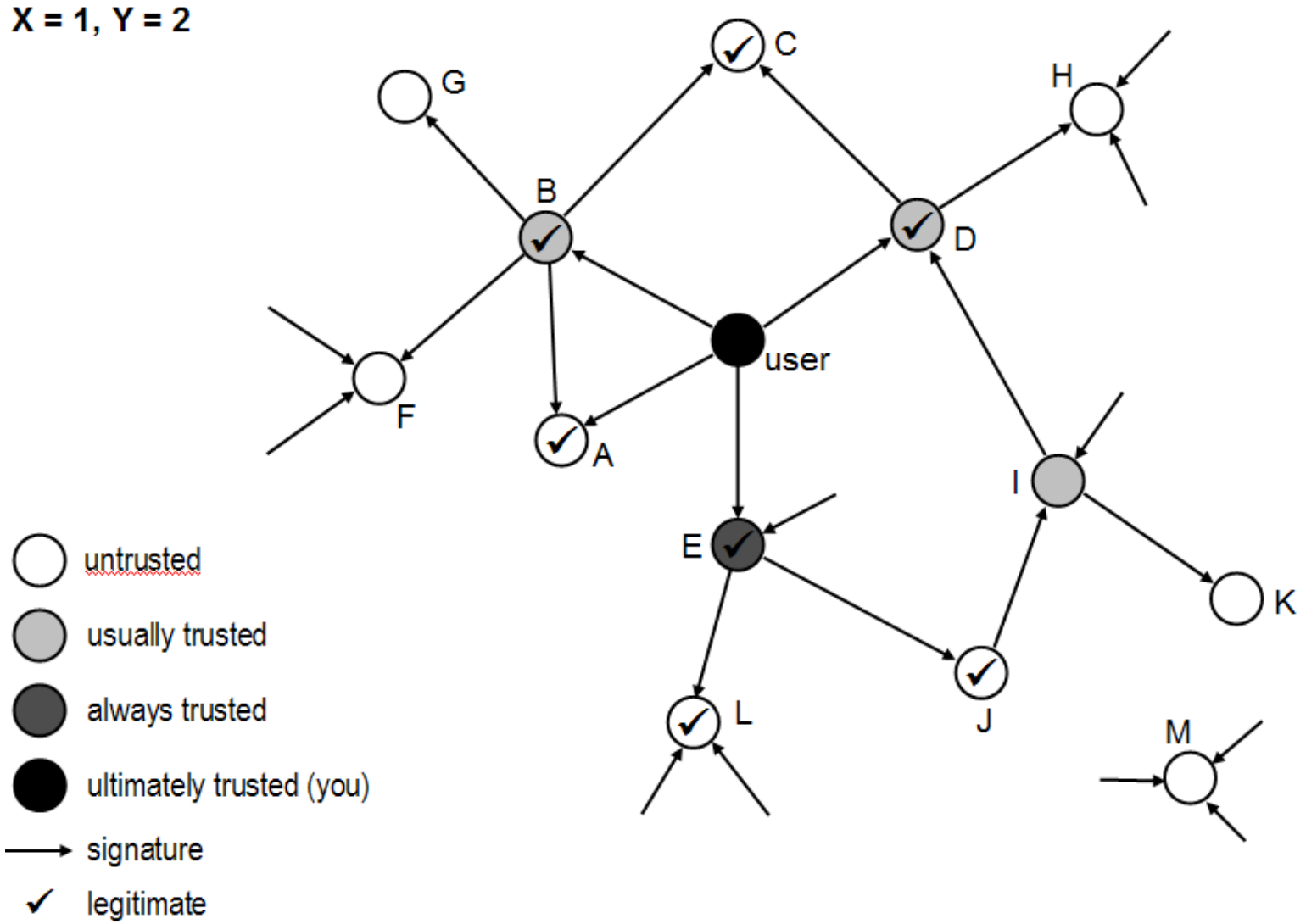


Nivele de încredere

- încrederea în proprietar (owner trust)
  - valoare asignată de către fiecare utilizator
  - valori posibile
    - *unknown user*
    - *usually not trusted*
    - *usually trusted (pondere 1/Y)*
    - *always trusted (pondere 1/X)*
    - *ultimately trusted (pondere 1)*
- încrederea în semnătură (signature trust)
  - valoare asignată de sistem
  - aceiaşi cu încrederea în proprietar dacă cheia publică folosită la semnarea recomandării se află în inelul de chei
- legitimitatea cheii (key legitimacy)

  TRUST = SUM (1/X) + SUM(1/Y)

Nivele de încredere (cont.)



Versiuni PGP

- Versiuni comerciale
  - PGP Corporation (www.pgp.com)
  - Versiunea 9.0
    - RSA+SHA sau DSA+SHA pt. autentificare
    - RSA sau ElGamal pt. schimbul de chei
    - AES, CAST, 3DES, IDEA, Twofish pt. criptare
    - certificate X.509 v.3
    - smart card-uri criptografice
- Versiuni free
  - www.pgpi.org
  - GnuPG (www.gnupg.org)
- PGPdisk
- PGPfone
- Librării criptografice (SDK)

S/MIME

- Secure / Multipurpose Internet Mail Extension
- Standard elaborat de RSA Security
- Adăugare facilităţi de securitate la formatul MIME
- Servicii similare PGP (autentificare, confidenţialitate, etc.)
- IETF RFC 5751, 5750

RFC 822

- Defineşte formatul mesajelor text ce pot fi transmise prin e-mail
- Structura unui mesaj RFC 822:
  - antet (e.g., from: …, to: …, cc: …)
  - corp (textul mesajului)

```
Date: Tue, 03 Dec 2005 10:30:15 (EST)
From: "Ion Bica" <ibica@mta.ro>
Subject: Test
To: afriend@abc.ro

This is a test.
```

MIME

- RFC 822 are o serie de limitări
  - nu poate transmite obiecte binare
  - nu oferă suport multilingvistic
  - unele servere SMTP nu acceptă mesaje peste o anumită dimensiune
  - probleme de conversie la nivelul gateway-urilor
- MIME a fost gândit pentru a elimina aceste neajunsuri
  - defineşte noi tipuri de câmpuri pentru antetul mesajelor
  - defineşte o serie de formate de conţinut (standardizarea reprezentării conţinutului multimedia)
  - defineşte reguli de codificare a datelor astfel încât conţinutul mesajelor să nu fie modificat de sistemul de mesagerie
  - IETF RFC 2045,…,2049

MIME (cont.)

- MIME-Version (1.0)
- Content-Type
  - descrie tipul de date din cadrul corpului mesajului
  - pe baza acestui câmp, receptorul poate selecta metoda corespunzătoare pentru afişarea conţinutului respectiv
- Content-Transfer-Encoding
  - Specifică transformarea folosită pentru a reprezenta corpul mesajului
- Content-ID
- Content-Description
  - descrie obiectul din cadrul corpului mesajului
  - util atunci când conţinutului este indescifrabil (date audio)

MIME (cont.)

```
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Date: Sun, 21 Mar 1993 23:56:48 -0800 (PST)
Subject: Sample message
MIME-Version: 1.0
Content-type: multipart/mixed; boundary="simple boundary"

This is the preamble. It is to be ignored, though it is a handy place for
composition agents to include an explanatory note to non-MIME conformant
readers.

--simple boundary

This is implicitly typed plain US-ASCII text. It does NOT end with a
linebreak.
--simple boundary

Content-type: text/plain; charset=us-ascii
This is explicitly typed plain US-ASCII text. It DOES end with a linebreak.

--simple boundary--

This is the epilogue. It is also to be ignored.
```

S/MIME

- **enveloped data** (application/pkcs7-mime; smime-type = enveloped-data)
  - conţinut criptat
- **signed data** (application/pkcs7-mime; smime-type = signed-data)
  - semnătură digitală standard (“hash and sign”)
  - conţinutul + semnătura sunt codificate base64
  - conţinutul nu poate fi interpretat de programe ce nu sunt compatibile S/MIME
- **clear-signed data** (multipart/signed)
  - semnătură digitală standard (“hash and sign”)
  - numai semnătura este codificată base64
  - conţinutul poate fi interpretat de programe ce nu sunt compatibile S/MIME; acestea nu vor putea însă să verifice semnătura
- **signed and enveloped data**

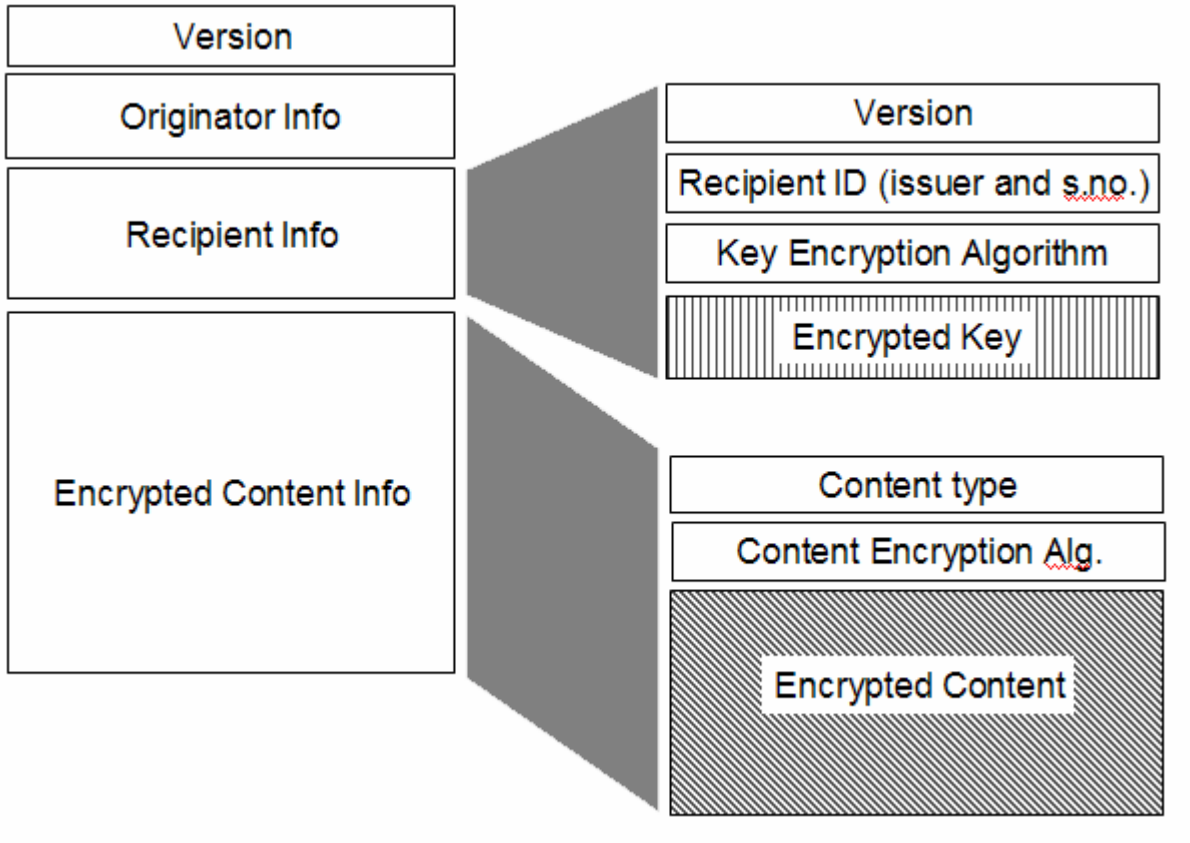
Algoritmi criptografici

- Funcţie hash
  - must: SHA-1
  - should (receiver): MD5
- Semnătură digitală
  - must: DSS
  - should: RSA
- Anvelopare cheie de sesiune
  - must: Diffie-Hellman
  - should: RSA
- Criptare date
  - sender:
    - should: 3DES, RC2/40
  - receiver:
    - must: 3DES
    - should: RC2/40

Securizare MIME

- Conţinutul ce urmează a fi transmis este procesat conform regulilor MIME rezultând un obiect MIME
- Obiectul MIME este procesat de S/MIME pentru a produce un obiect PKCS #7
- Obiectul PKCS #7 este tratat ca şi conţinut obişnuit (binar) şi este încapsulat într-un nou obiect MIME

Criptare date

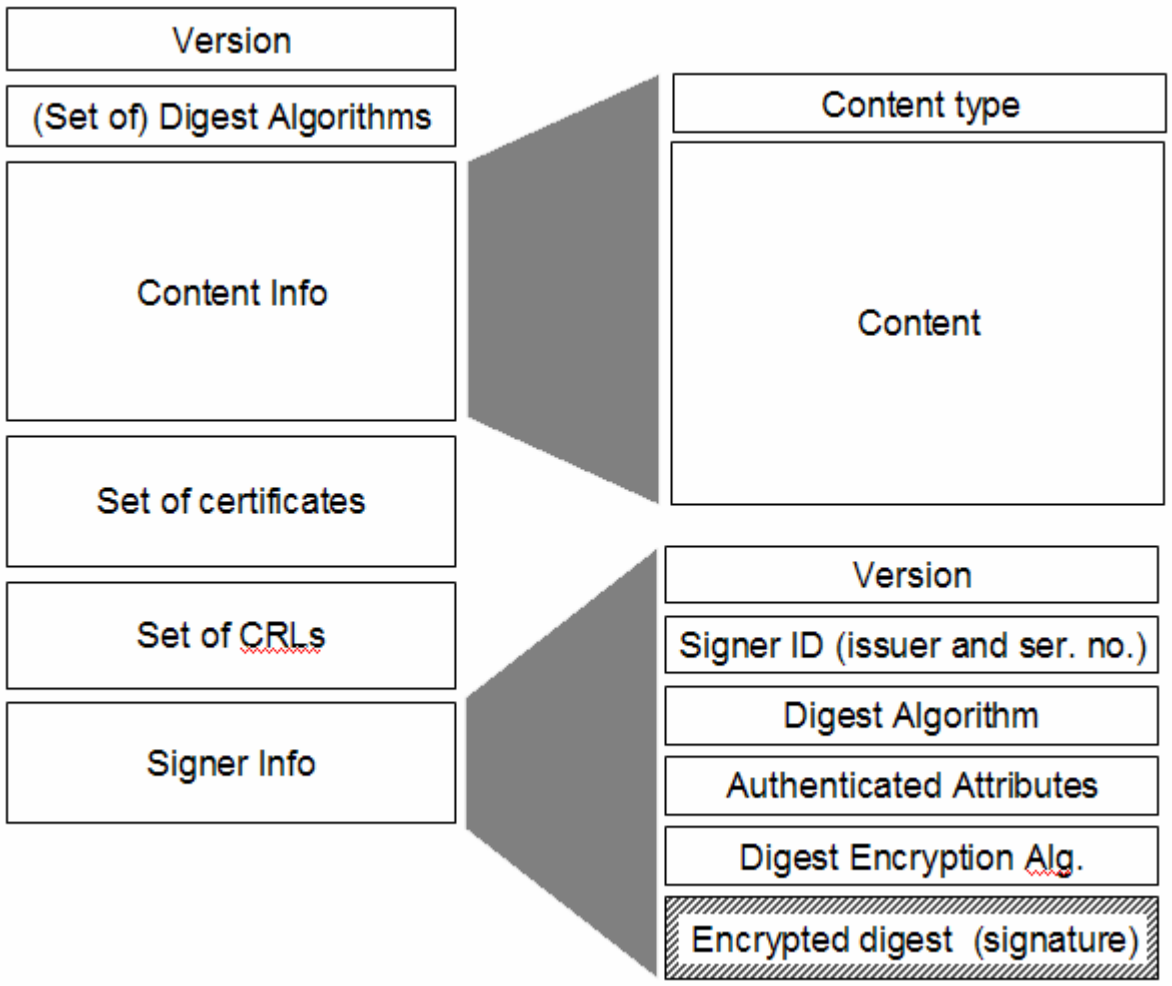


Criptare date (cont)

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

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGf
HfYT67n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6j
H7756tbB9Hf8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT
6ghyHhHUujpfyF40GhIGfHfQbnj756YT64V
```

Semnare date



Semnare date (cont.)

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

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAMYICNDCCAjA
CAQEwgdAwgbwxCzAJBgNVBAYTAkRFMRAwDgYDVQQIEwdIYW1idXJnMRAwDgYDVQQHEwdIYW1idX
JnMTowOAYDVQQKEzFUQyBUcnVzdENlbnRlciBmb3IgU2VjdXJpdHkgaW4gRGF0YSBOZXR3b3Jrc
YBHbWJIMSIwIAYDVQQLExlUQyBUcnVzdENlbnRlciBDbGFzcyAyIENBMSkwJwYJKoZIhvcNAQkB
FhpjZXJ0aWZpY2F0ZUB0cnVzdGNlbnRlci5kZQIPAPBiAAAAAqdEw5SzrwZ8MAkGBSsOAwIaBQC
ggbowGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMDUxMjAzMDIxMz
A3WjAjBgkqhkiG9w0BCQQxFgQU/ItNf+rqvXbwVlG/Ewy8O3r8cbMwWwYJKoZIhvcNAQkPMU4wT
DAKBggqhkiG9w0DBzAOBggqhkiG9w0DAgICAIAwDQYIKoZIhvcNAwICAUAwBwYFKw4DAgcwDQYI
KoZIhvcNAwICASgwBwYFKw4DAh0wDQYJKoZIhvcNAQEBBQAEgYBN76JiXrLSwOlTCQFZlrO0MAH
sfsJcxLOxYcGiuDTm3y2Vo2y+tfZZLUG032n32ouT1he8KaecphMT3nezUaBAVif74rel4fP/wr
ACFa69Wyk7q0NsVZ7sCta5Pg6H4o/LC+oEsr4VGxYYvl28VJ30eJtyBHfYzqfLJ2IMsEY1cQAAA
AAAA==
```

Semnare date (cont.)

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

--boundary42
Content-Type: text/plain

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

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

Configurare S/MIME

- Clienţi de e-mail compatibili S/MIME v3!
- Toate setările se fac la nivelul clienţilor
- Banner-ele şi disclaimer-ele adăugate automat de către serverele de mail sau antivirus invalidează semnăturile digitale!

Atacuri împotriva PGP și S/MIME

- **EFAIL (Mai 2018) !!!**
  - exfiltrare conținut mesaj criptat
  - presupune interceptarea și modificarea mesajului criptat
  - Direct exfiltration attack
  - CBC/CFB gadget attack
  - mai multe detalii la: https://efail.de/