Esperienza di utilizzo della firma elettronica

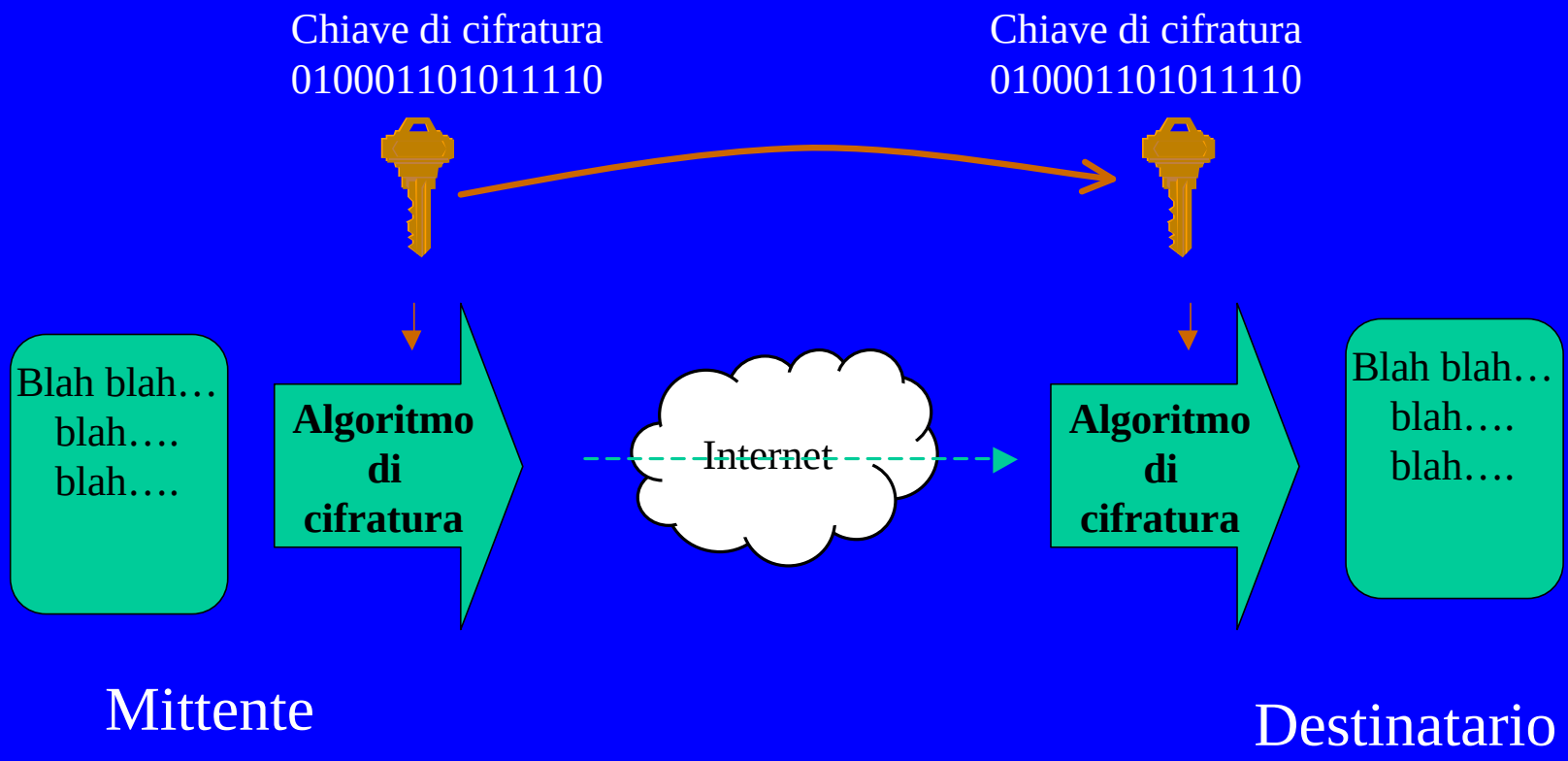
Francesco Gennai

Posta elettronica e crittografia

- Breve introduzione ai meccanismi che regolano la crittografia a chiave pubblica
- La certificazione: perchè è importante
- Descrizione di una Public Key Infrastructure (PKI)
- Comunicazioni sicure via posta elettronica

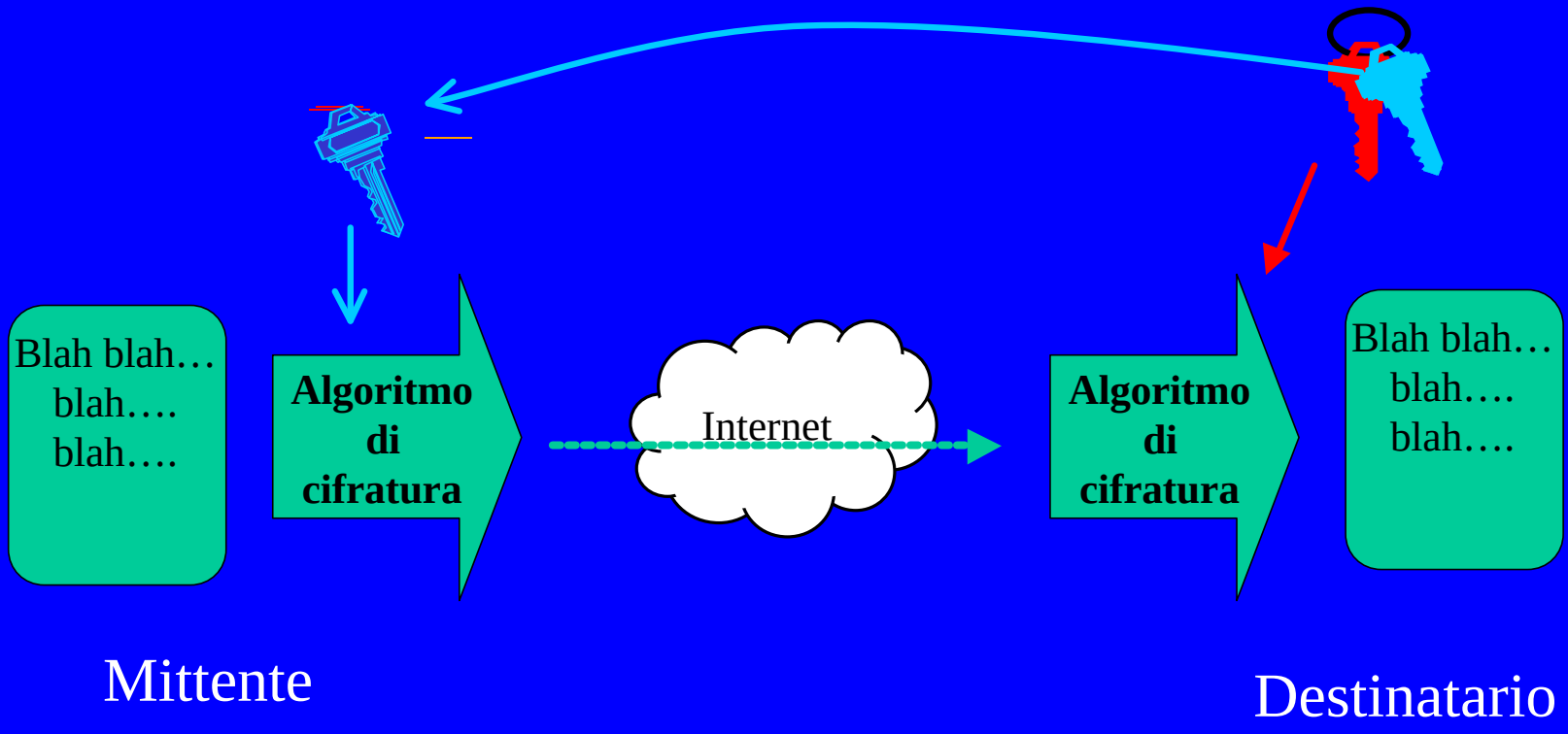
Posta elettronica e crittografia

Cifratura con chiave simmetrica



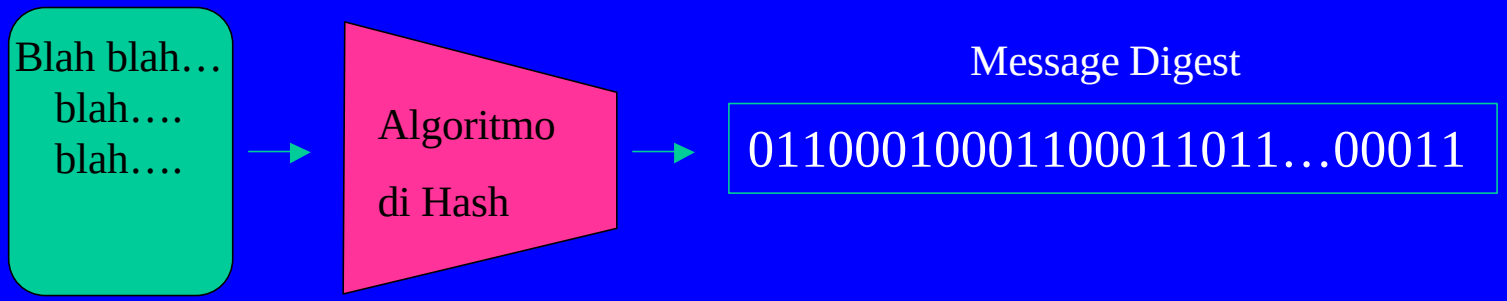
Posta elettronica e crittografia

Cifratura con chiave asimmetrica



Posta elettronica e crittografia

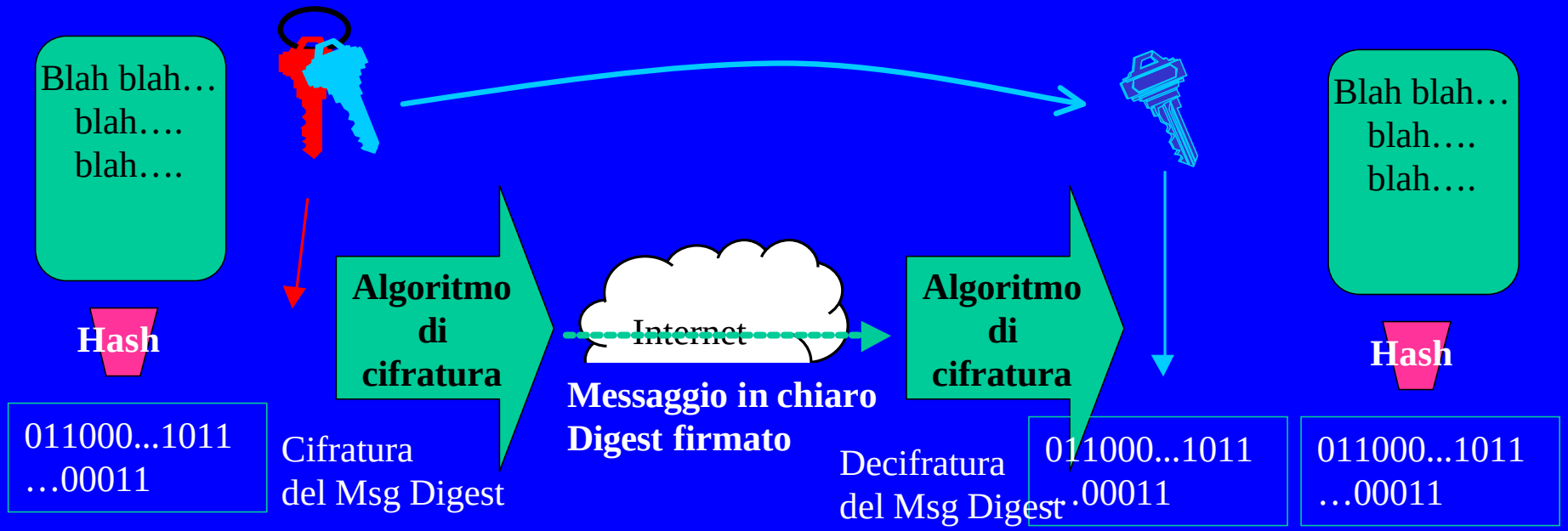
Firma digitale



Mittente

Posta elettronica e crittografia

Firma digitale



Posta elettronica e crittografia

- Certification Authority
  - garantisce l'appartenenza di una chiave pubblica ad un determinato soggetto. Come ? Mediante l'emissione di certificati
    - La Certification Authority rende nota la politica di sicurezza alla quale si dovrà rigorosamente attenere
  - gestisce il database dei certificati
  - gestisce la Certificate Revocation List (CRL)

Posta elettronica e crittografia

- La stessa Certification Authority (CA) possiede una coppia di chiavi
  - Un certificato è l'unione di dati che identificano in modo univoco un soggetto e della sua chiave pubblica
  - La Certification Authority firma con la propria chiave privata il certificato assegnandoli un numero di serie
  - Chiunque potrà verificare che una determinata chiave pubblica appartiene ad un determinato soggetto semplicemente applicando il processo di verifica firma con la chiave pubblica della CA.
    E' importante conoscere la "Policy" applicata dalla CA

Certificato X.509 (End Entity)

(parte 1/2)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: Email=pkp-ca@iat.cnr.it, CN=IAT PKP-CA, OU=IAT, O=CNR, C=IT
        Validity
            Not Before: Apr  3 22:34:26 2000 GMT
            Not After : Dec 31 22:34:26 2001 GMT
        Subject: C=IT, O=CNR, OU=IAT, CN=PKP-CA Staff 1/Email=mario.rossi@iat.cnr.it
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bd:12:33:ff:84:9c:2c:0a:7a:ad:19:90:ca:9a:
                    37:22:24:d0:0c:1a:e0:54:30:72:92:2d:4a:5e:02:
                    bd:0b:ed:72:80:25:a2:6a:5b:e3:d8:fb:bb:06:aa:
                    8e:d6:2d:68:56:45:18:1b:20:f9:a4:a6:c8:2a:0c:
                    62:d9:71:0c:0a:fe:20:3a:97:2b:1a:7c:45:b7:92:
                    09:75:e3:94:17:e9:14:86:02:4c:79:a0:b4:a6:41:
                    38:e4:83:3b:cf:33:14:c5:c9:f0:a9:d7:cd:9e:8f:
                    26:ab:dc:e6:26:c0:d8:b8:4f:ba:49:fd:54:a2:78:
                    f0:dd:ff:36:26:8e:38:08:bb
                Exponent: 65537 (0x10001)
```

Certificato X.509 (End Entity)

(parte 2/2)

```
X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Comment:
                PKP user certificate. Certificato emesso nell'ambito di una sperimentazione
                fra Istituti CNR. Informazioni sul progetto e CPS della CA sono reperibili
                alla URL https://pkp-ca.iat.cnr.it
            X509v3 Subject Key Identifier:
                D7:0D:CF:E9:D8:5F:D3:BB:1D:32:24:89:83:44:4B:6A:85:B5:98:7C
            X509v3 Authority Key Identifier:
                keyid:3F:45:7B:0E:9F:E8:9A:D3:3F:08:D3:F9:97:37:2B:9E:0F:62:FA:CE
                DirName:/Email=pkp-ca@iat.cnr.it/CN=IAT PKP-CA/OU=IAT/O=CNR/C=IT
                serial:00

            X509v3 Subject Alternative Name:
                email:anna.vaccarelli@iat.cnr.it
            X509v3 Issuer Alternative Name:
                <EMPTY>

    Signature Algorithm: md5WithRSAEncryption
        0b:1e:9c:18:9a:ba:a6:cf:e1:d5:9f:6f:9a:f1:1d:e4:82:e6:
        ba:91:77:e4:68:26:19:2a:15:df:f0:eb:7f:37:b3:27:9e:a4:
        d2:9f:7d:dc:cb:78:e5:d5:ed:1e:45:a0:ef:74:96:e5:58:a4:
        50:a0:f6:0e:d7:79:7f:ae:8e:8c:04:cf:5e:0e:b5:7c:68:2a:
        .. . . .. . . . ….. . .. .. …
        …. . . . … . . . ..
        7d:77:ed:83:3b:a7:f0:f7:49:d6:14:dd:3b:db:aa:c2:e3:ab:
        b0:de:29:f4:0f:52:5d:44:ca:02:30:0b:f9:4d:3e:bb:eb:9f:
        b7:58:91:f8
```

Certificato X.509 (Certification Authority)

(parte 1/2)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: Email=pkp-ca@iat.cnr.it, CN=IAT PKP-CA, OU=IAT, O=CNR, C=IT
        Validity
            Not Before: Apr  3 21:54:36 2000 GMT
            Not After : Dec 31 21:54:36 2001 GMT
        Subject: Email=pkp-ca@iat.cnr.it, CN=IAT PKP-CA, OU=IAT, O=CNR, C=IT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ca:25:a7:43:62:4d:75:8f:71:d4:88:aa:30:4f:
                    d9:6c:37:1d:2f:e2:bf:f9:53:36:ad:40:be:9a:ad:
                    14:e2:c2:90:ee:6a:a6:4c:43:09:1d:ab:5d:53:3c:
                    4c:e2:2c:78:35:1f:39:e7:3d:04:d9:b1:12:a5:5f:
                    92:05:90:9a:df:02:52:1e:57:7b:b4:13:4e:12:7f:
                    51:d2:c8:08:19:aa:f1:27:71:7b:f2:48:f5:aa:cd:
                    68:6c:cd:25:8b:5a:5d:af:ce:b6:97:db:4c:4b:29:
                    ae:5f:e2:05:b3:e2:46:92:2b:51:cd:50:a9:67:47:
                    c6:17:bf:c4:da:ff:2a:0e:2d:a6:8f:89:05:ea:f0:
                    90:4d:14:9e:41:1e:5c:05:a4:26:1b:02:0f:02:95:
                    a4:bd:94:73:4c:1b:61:f3:29:7a:01:04:16:0e:2a:
                    24:3d:47:bf:28:95:15:5e:bb:53:d0:97:69:ab:5b:
                    c2:ca:20:9e:5a:54:01:da:f5:7c:65:76:31:93:52:
                    27:3a:aa:8a:31:41:3c:0a:af:3e:3c:62:08:bd:e8:
                    10:8d:63:e3:52:c6:d9:aa:40:f3:15:67:15:4f:09:
                    a4:e3:e8:58:f0:fc:89:a5:86:0b:56:39:6f:a7:22:
                    f7:ec:8f:e3:40:84:21:39:91:04:bb:e6:57:6c:d1:
                    0e:65
                Exponent: 65537 (0x10001)
```

Certificato X.509 (Certification Authority)

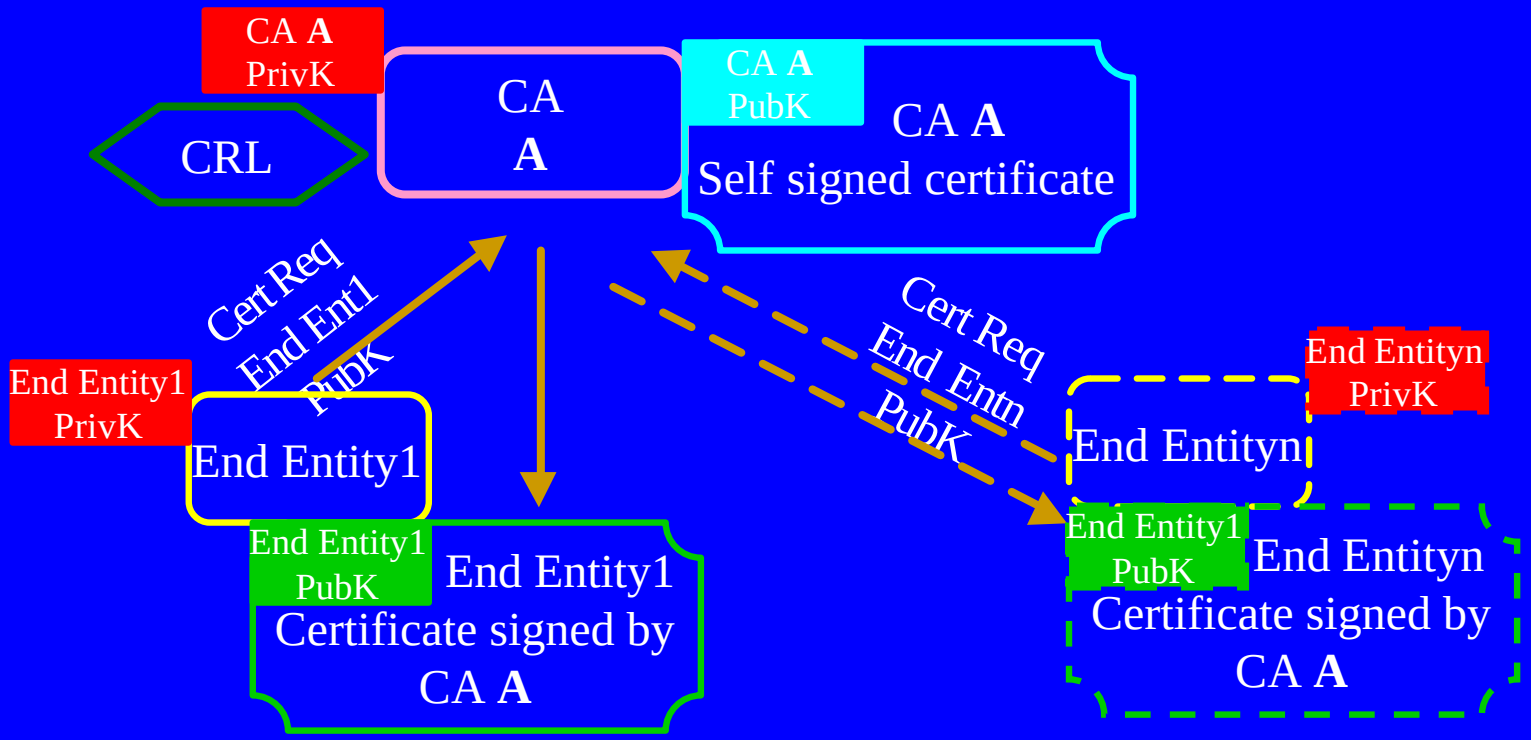
(parte 2/2)

```
X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Key Identifier:
                3F:45:7B:0E:9F:E8:9A:D3:3F:08:D3:F9:97:37:2B:9E:0F:62:FA:CE
            X509v3 Authority Key Identifier:
                keyid:3F:45:7B:0E:9F:E8:9A:D3:3F:08:D3:F9:97:37:2B:9E:0F:62:FA:CE
                DirName:/Email=pkp-ca@iat.cnr.it/CN=IAT PKP-CA/OU=IAT/O=CNR/C=IT
                serial:00

            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Subject Alternative Name:
                <EMPTY>

            X509v3 Issuer Alternative Name:
                <EMPTY>

    Signature Algorithm: md5WithRSAEncryption
        29:8f:9b:60:86:d2:17:78:72:b4:6e:a1:f4:6a:d8:f0:3e:9f:
        df:38:82:47:11:31:2e:9c:36:49:9b:39:b5:e0:ef:59:c5:7c:
        fc:9c:f9:1b:4e:8f:35:ad:71:3a:c0:d4:37:16:dd:f0:a8:b0:
        62:b9:09:5b:9b:00:b3:41:be:f1:9c:72:9b:00:6f:a9:dc:2c:
        92:0a:7f:48:43:2a:03:1e:49:fd:2f:15:c3:7c:b6:a2:c9:0e:
        ……..  . . .. …… .. . . . ..
         … . …. . .. ……..     ….. .
        9d:e3:d9:4c:70:d5:e0:c3:a1:8d:c1:a8:d5:be:bc:14:c0:9a:
        99:8e:a1:11:c1:b6:96:3e:a8:eb:0c:ae:8b:f1:0b:6b:88:3a:
        14:6a:0e:6d:71:7c:af:1e:94:67:1a:fc:2d:67:3b:81:ab:3b:
        ea:d4:92:24:3b:3c:9a:93:9a:6c:cd:2f:c1:7f:fd:2f:ba:f3:
        bf:22:12:14
```

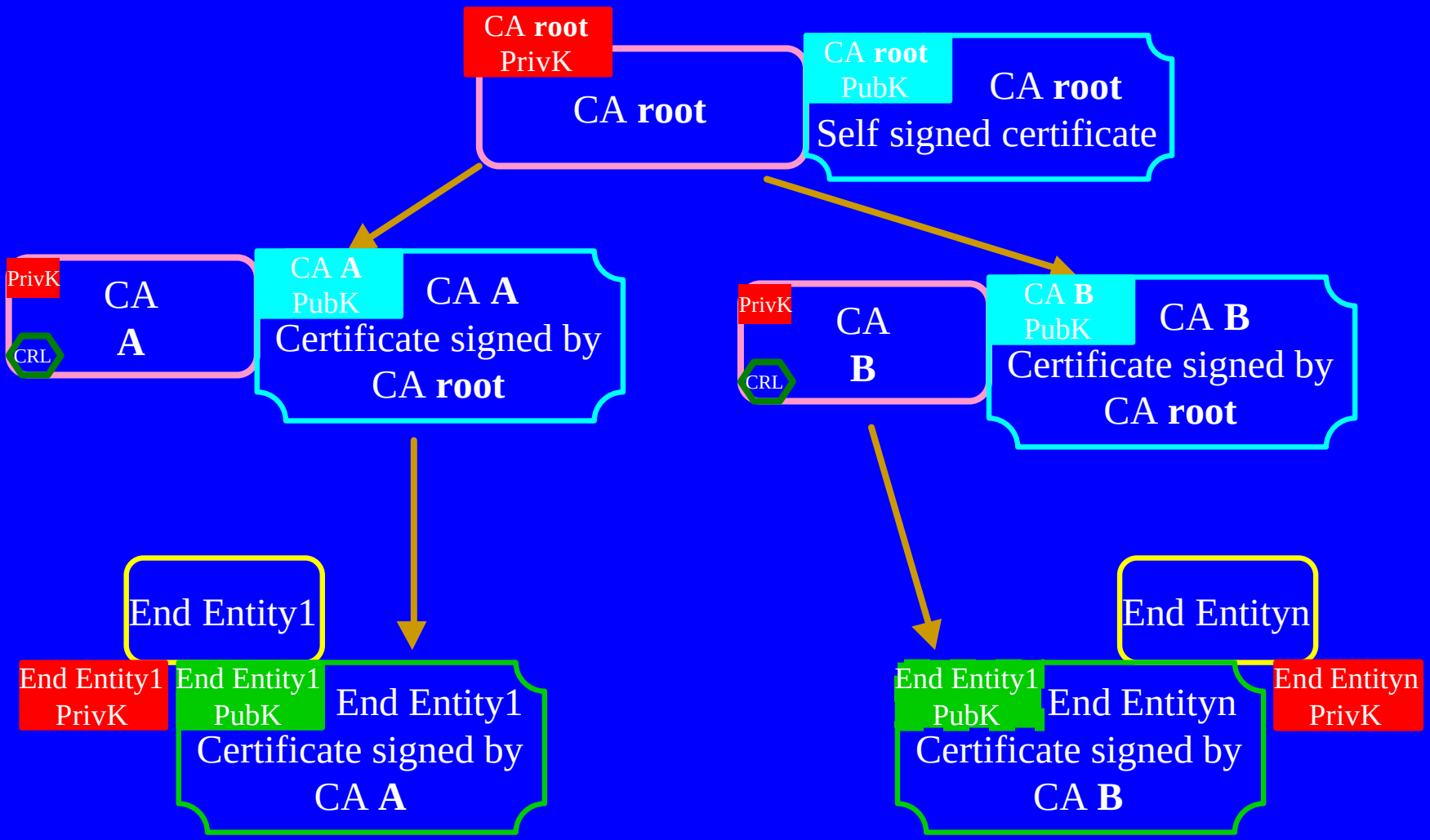
Certificate Revocation List

```
Certificate Revocation List (CRL):
        Version 1 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: /O=OpenCA/C=IT
        Last Update: Jun 19 13:57:27 2000 GMT
        Next Update: Jul 20 13:57:27 2000 GMT
Revoked Certificates:
    Serial Number: 02
        Revocation Date: Jun 19 13:25:55 2000 GMT
    Serial Number: 03
        Revocation Date: Jun 19 13:27:38 2000 GMT
    Serial Number: 04
        Revocation Date: Jun 19 13:55:39 2000 GMT
    Serial Number: 05
        Revocation Date: Jun 19 13:57:20 2000 GMT
    Signature Algorithm: md5WithRSAEncryption
        57:4b:cb:04:da:be:8e:7f:53:0b:26:8f:e2:f5:ca:67:a8:d1:
        ab:2e:8e:62:59:65:7e:f4:12:49:0d:20:fd:b5:ed:58:88:55:
        08:a1:ad:43:3d:6b:03:83:78:c2:11:a4:54:65:74:5b:1b:58:
        cd:b1:e7:05:58:fd:50:f8:8e:cb:16:e1:b9:6d:10:11:30:e3:
        25:5a:35:bb:f6:39:64:cc:bb:fa:36:54:15:f0:f6:bb:6b:39:
        e4:e7:d3:db:0b:4d:59:d3:35:d1:aa:f8:7b:6a:b5:3b:50:a8:
        8e:06:a9:4a:c8:08:2c:6d:9b:82:89:d1:aa:e2:a0:09:17:6d:
        52:8c:61:73:38:f9:ed:ec:79:9e:42:11:31:8a:5d:ff:54:5e:
        4d:30:a0:8f:38:65:ad:47:22:45:51:70:d6:6b:c4:3c:b4:ad:
        9b:2c:f6:af:4b:bb:b7:b5:2e:f9:df:5d:93:ec:a5:dc:73:18:
        37:46:44:2f:e1:83:1f:fa:d2:9a:b4:d6:40:85:6e:20:62:b5:
        68:db:4f:af:3b:0b:e1:85:c4:1e:13:1f:6f:c0:15:db:cc:2f:
        fa:83:48:48:2f:f3:22:c4:e6:8f:d4:65:16:e9:0f:72:94:74:
        03:2e:66:74:0e:b2:90:47:51:a5:96:56:0e:ff:60:4e:f8:94:
        7a:27:77:e9
```

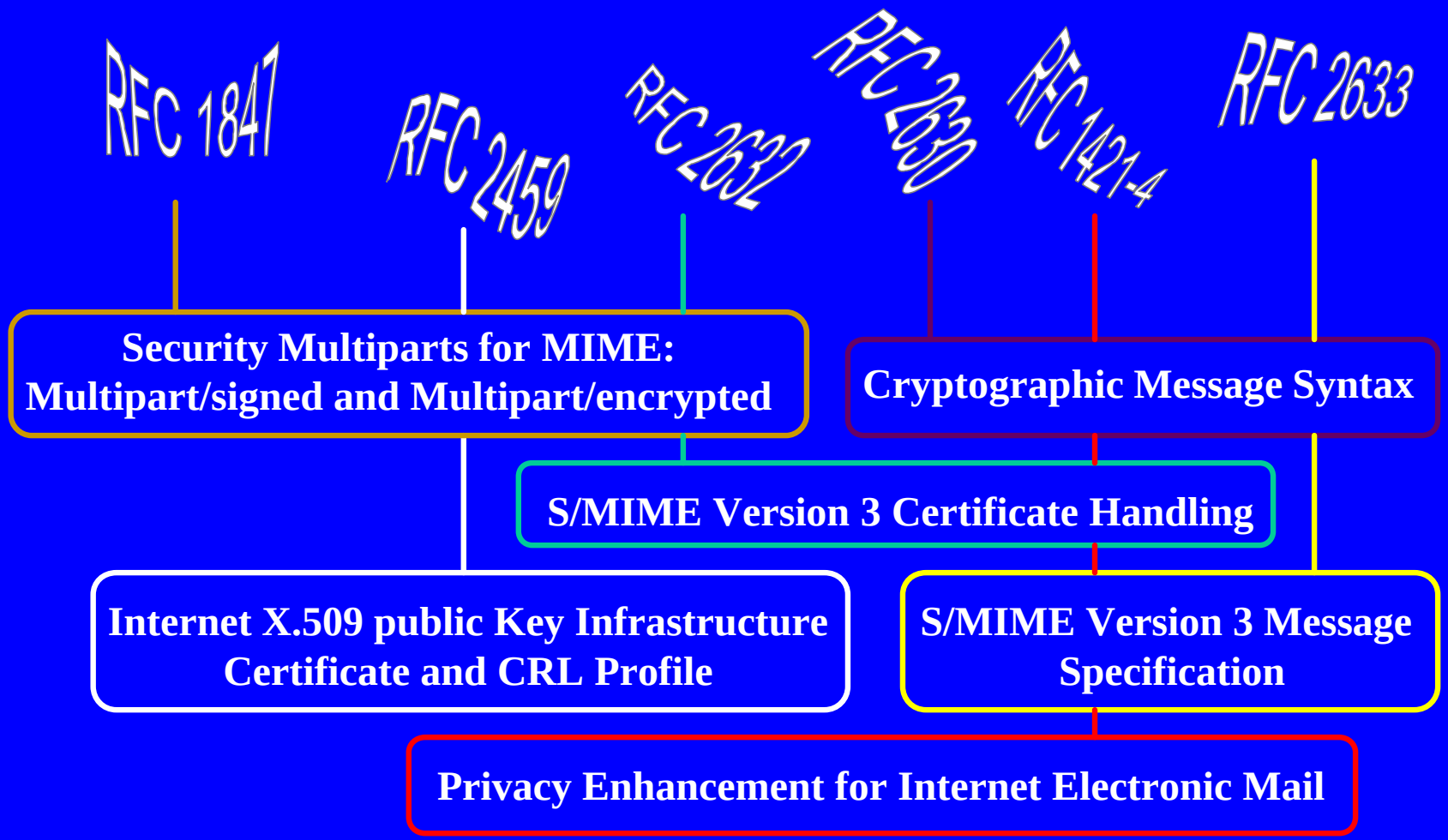
Public Key Infrastructure



Public Key Infrastructure



Messaggi di posta elettronica e crittografia



Messaggi di posta elettronica e crittografia

- RFC 1847 + RFC 2630 + RFC 2633 = struttura messaggio

Criptato: composto da un'unica parte
application/pkcs7-mime; smime-type=enveloped-data

Firmato: composto da un'unica parte
application/pkcs7-mime; smime-type=signed-data
oppure
composto da due parti
multipart/signed; protocol="application/pkcs7-signature";
micalg=sha-1 | md5
I parte: normale MIME content-type
II parte: application/pkcs7-signature

Firmato e criptato: una qualsiasi combinazione dei due precedenti casi

Messaggi di posta elettronica e crittografia

RFC 1847

Intestazione e indirizzi

To:
From:
cc:
Subject:

Corpo del messaggio

Content-type: Multipart/signed; protocol="..."; micalg="...."

Content-type: text/plain, image/gif, etc..

Content-type: application/pkcs7-signature
Content-transfer-encoding: base64

MULTIPART/SIGNED

```
Content-type: multipart/signed; protocol="application/pkcs7-signature";
 micalg=sha1; boundary=------------ms775C52C7DD5A1C12484764F0

This is a cryptographically signed message in MIME format.

--------------ms775C52C7DD5A1C12484764F0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Saluti da Antonio

--------------ms775C52C7DD5A1C12484764F0
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIGogYJKoZIhvcNAQcCoIIGkzCCBo8CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCC
BKAwggScMIIDhKADAgECAgECMA0GCSqGSIb3DQEBBAUAMGsxJzAlBgkqhkiG9w0BCQEWGHBr
aS1yYUBwa2ktcmEuaWF0LmNuci5pdDEPMA0GA1UEAxMGUEtJLVJBMRQwEgYDVQQLEwtQS0kt
UkEgVW5pdDEMMAoGA1UEChMDSUFUMQswCQYDVQQGEwJJVDAeFw0wMDA5MDExODA5MDBaFw0w
……. .. … …… . ……. . .. . . .. . . . . . . . ..
…….  … ……. . . . .. . . .
AQEBBQAEgYCKfsck4CKgnnJqx5HisiSGFBuSnZAjMiz6uGVscetkyhfoJY/+BZmRYKAIfigr
+QSxE9VIIeeqEGMM9z5b3o77kNxViqy3WM2QPzsGLB7rYXyuV1nxTxZQzR+DrnRgqswmP0tT
1KRpBTsL9sLD4ulIObUY2j36on69xsAxGsLWfw==
--------------ms775C52C7DD5A1C12484764F0--
```

Messaggi di posta elettronica e crittografia

RFC 2633

Intestazione e indirizzi

To:
From:
cc:
Subject:

Corpo del messaggio

Content-type: application/pkcs-mime; smime-type=signed-data;
Content-transfer-encoding: base64

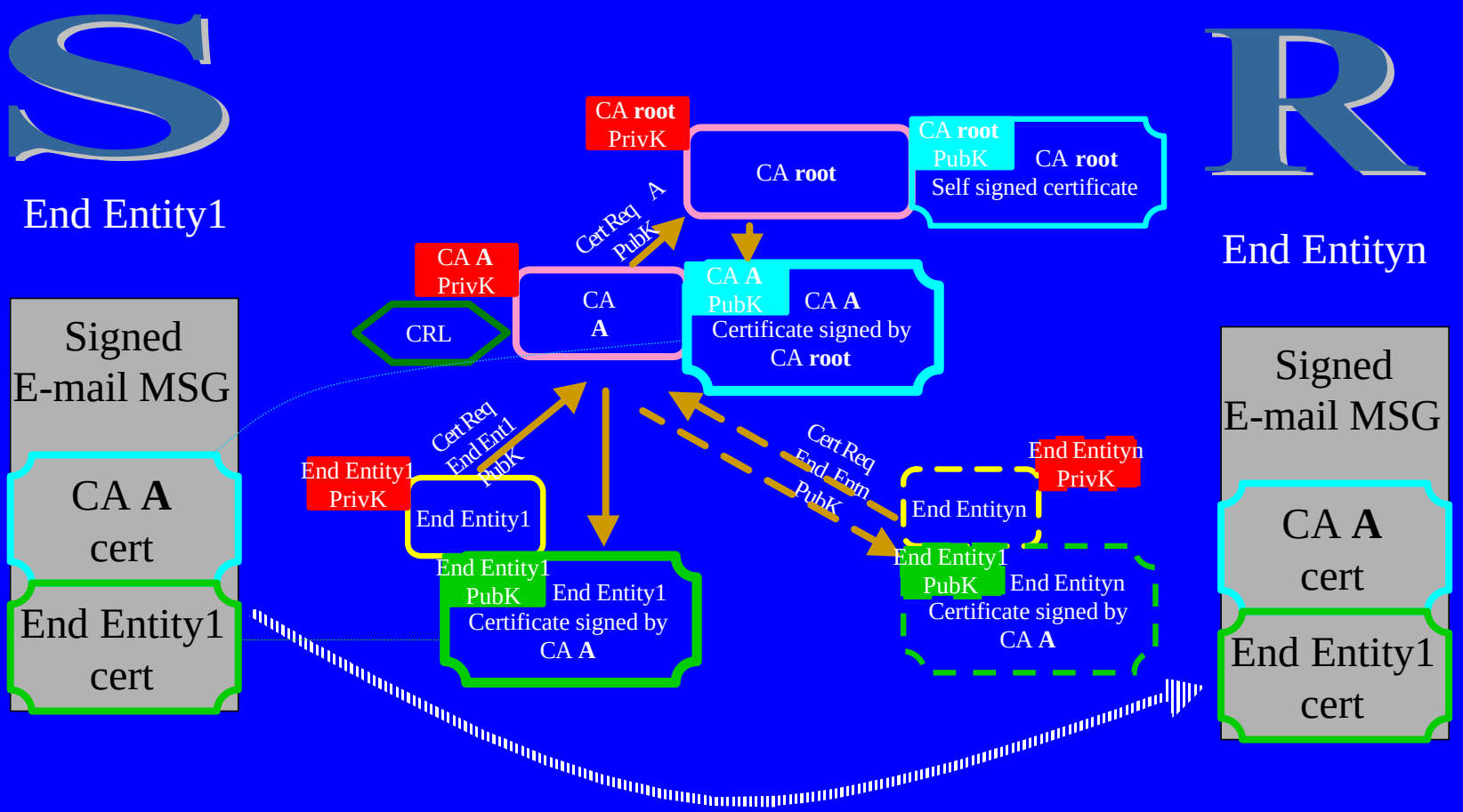
Application/pkcs-mime

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

ZSBmcmEgSUFUL1JBIGVkIElTUC4gSW5mb3JtYXppb25pIHN1bCBwcm9nZXR0byBlIENQUyBk
ZWxsYSBDQSBzb25vIHJlcGVyaWJpbGkgYWxsYSBVUkwgaHR0cDovL3BraS1yYS5pYXQuY25y
Lml0MB0GA1UdDgQWBBSOjXEKaKccTQtTUFi5OwWNxGFr5TCBlQYDVR0jBIGNMIGKgBQLF6fS
1Pti2lhmMn5C/WD8J4UoRaFvpG0wazEnMCUGCSqGSIb3DQEJARYYcGtpLXJhQHBraS1yYS5p
YXQuY25yLml0MQ8wDQYDVQQDEwZQS0ktUkExFDASBgNVBAsTC1BLSS1SQSBVbml0MQwwCgYD
……. .. … …… . ……. . .. . . .. . . . . . . ..
…….  … ……. . . . .. . . .
GkgYWxsYSBVUkwgaHkOppIfex5HisiSGFBuSnZAjMiz6uGVscetkyhfoJY/+BZmRYKAIfigr
+DQSBzb25vIHJlcGVjxViqy3WM2QPzsGLB7rBwcm9nZpYXyuV1nxTxZQzR+DrnRgqswmP0tT
TUFi5OwWNxGFr5TCBlQYoRaFvpG0waz==
```

Messaggi di posta elettronica e crittografia

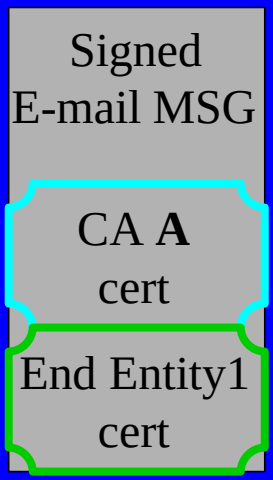
- Estensioni al nome file (parametro name del content-type):
  - multipart/signed
    - application/pkcs7-signature; name=smime.p7s
  - application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
  - application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m

Posta elettronica e PKI



Il mittente

End Entity1



- Include qualsiasi certificato che ritiene utile alla operazione di verifica del “Recipient”.
- Include almeno una catena di certificati sino a quello della CA (escluso) che ritiene possa essere affidabile (trusted) per il “Recipient”.
- L’indirizzo “From:” dovrebbe essere identico a quello eventualmente presente nel corrispondente certificato.

Il ricevente

- Riconosce un qualsiasi numero di certificati inclusi nel messaggio. In particolare gestisce una “catena di certificati”.
- Accede al certificato della CA ritenuta “affidabile”.
- Verifica che il from del messaggio corrisponda all’indirizzo eventualmente presente nel certificato.
- Accede alla CRL per riconoscere eventuali certificati revocati.

Condizioni di verifica

LA VERIFICA FALLISCE SE:

- Indirizzo del from non corrisponde ad uno degli indirizzi presenti nel certificato
- Non esiste un valido percorso fino ad una CA affidabile
- Impossibile accedere ad una CRL
- La CRL non è valida
- La CRL è scaduta
- Il certificato è scaduto
- Il certificato è stato revocato

OpenSSL

- Librerie per lo sviluppo di applicativi crittografici
- Applicativi per la manipolazione/generazione/conversione di vari oggetti appartenenti ad una PKI (certificate manipulation, basic CRL manipulation, basic CA management, signing, encrypting, decrypting, verifying, etc…)
- Pubblico dominio.
- Ultima release: 0.9.6
  - http://www.openssl.org

Il processo di verifica di OpenSSL

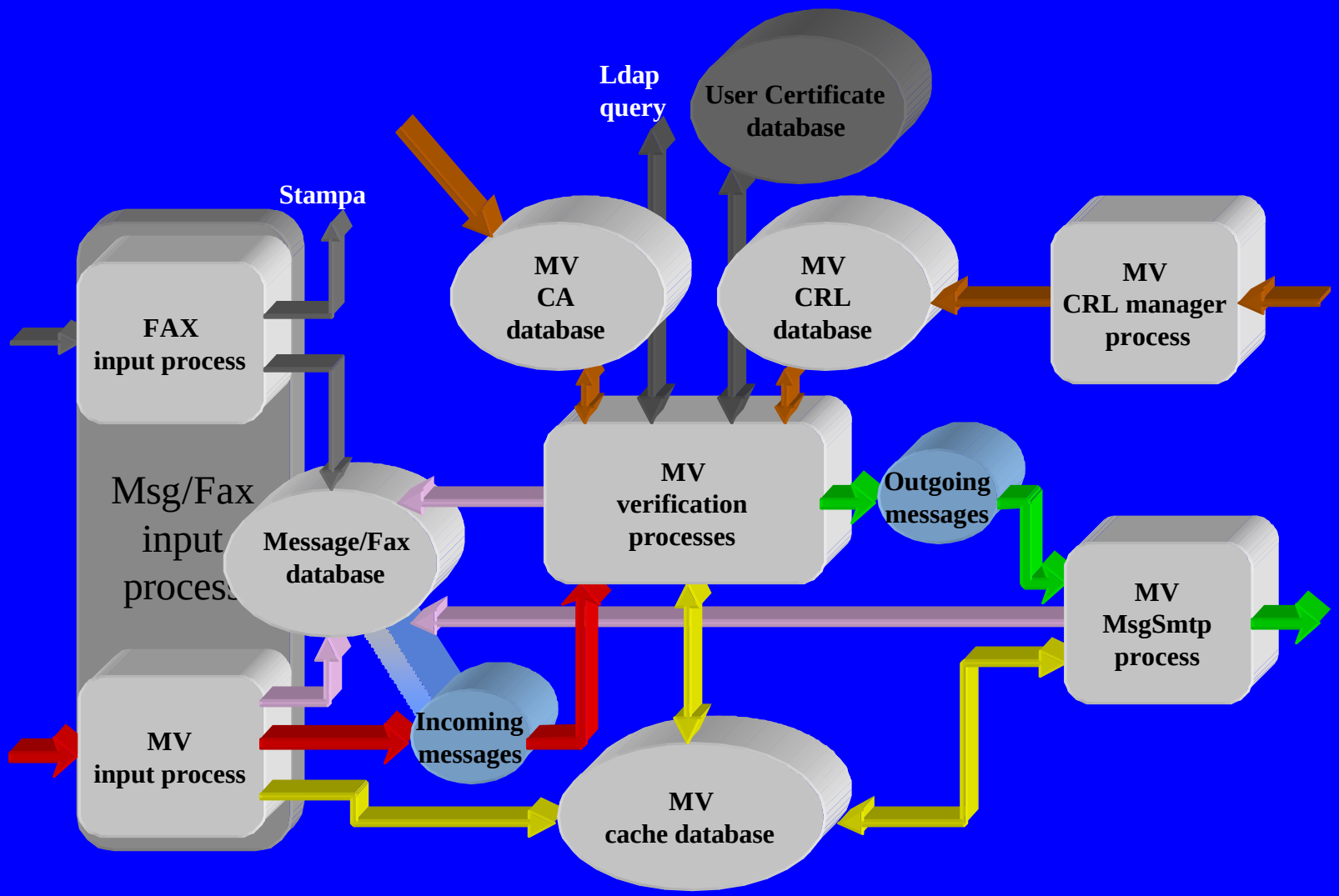
- Costruzione catena certificati: Authority e Subject Key Identifier
- Controllo KeyUsage
- Selezione certificato per la root CA (trusted)
- Verifica consistenza certificati intermedi (CA:TRUE)
- Verifica validità certificati della catena e relativa firma

Il sistema Message Verify

Sistema Message Verify

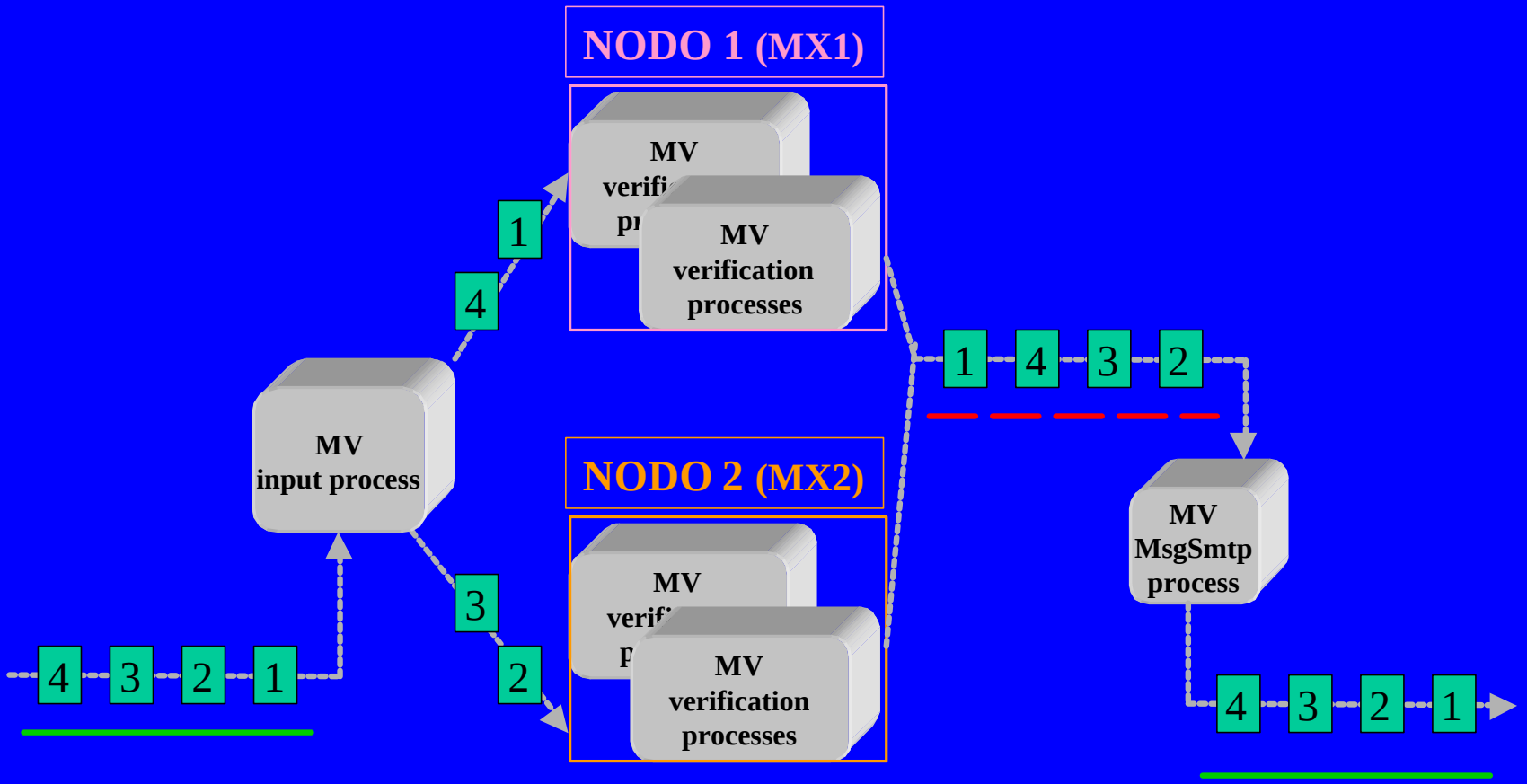
- Sviluppato per permettere la verifica firma automatica di un flusso di messaggi destinati a ulterirori elaborazioni automatiche.
  - Contesto di sviluppo e sperimentazione:
    - Registartion Authority italiana riceve circa 25000 fax per mese
    - Sperimentazione per utilizzo messaggi firmati in sostituzione fax
    - Certification Authority basata su OpenCA (http://www.openca.org)
    - Certificati distribuiti ad un sottoinsieme di “Maintainer” che partecipano alla sperimentazione

MsgVerify system overview



MsgVerify

messages path



MsgVerify system options

- Autoforwarding
  - trasmissione messaggio verificato al NIC Destination Address
- Deliver Method
  - P = Preview Mode
  - S = Skip CA
  - A = Skip all CA
  - U = Unconditioned continuation
- Intervals and timeouts
- E-mail addresses

MsgVerify Headers

- X-MVcertissuer: <Distinguished Name dell'issuer>
- X-MVcertsubject: <Distinguished Name del subject>
- X-MVglobalid: <codiceverifica-globalid>
  - codiceverifica: S = verifica completata con successo
W = verifica completata con assenza di CRL
  - globalid: identificativo (protocollo) univocamente assegnato dal Processo Input Messaggi/Fax

MsgVerify Headers

```
X-MVcertissuer: /C=DE/ST=Hamburg/L=Hamburg/O=TC TrustCenter for Security in
 Data Networks GmbH/OU=TC TrustCenter Class 1
 CA/Email=certificate@trustcenter.de

X-MVcertsubject: /C=DE/ST=NRW/L=K\xC8oln/CN=Manon Goo/Email=manon@manon.de

X-MVglobalid: W-200009016390
```

MsgVerify performances

- Cluster OpenVMS: 2 nodi Alphaserver 800 (500 Mhz)

  Test effettuato sull'invio di 2000 messaggi firmati

	6 Jobs (3 x Nodo)	1 Job	2 Jobs (1 x Nodo)
processo verifica	45min	2h 6min	59min
processo delivery	1h 16min	2h 6min	1h 4min
Totale	1h 16min	2h 6min	1h 4min

MsgVerify notifications

- Success notification message format
  - Subject: MV-RE-S: <subject from the received message>
  - Altre informazioni saranno nel message body
    - From:
    - Subject:
    - Global ID:
    - Message ID:
    - Previous Message ID:
    - Number of retries:
    - Cert issuer:
    - Cert subject:

MsgVerify notifications

- Error notification message format
  - Subject: MV-RE-W: <subject from the received message>
    WAITING - saranno fatti altri tentativi
    MV-RE-F: <subject from the received message>
    FINAL - nessun tentativo sarà ripetuto
    MV-RE-I: <subject from the received message>
    INFORMATIONAL
  - Altre informazioni saranno nel message body
    - From:
    - Subject:
    - Global ID:
    - Errortype:
    - Number of retries:
    - Cert issuer:
    - Cert subject:

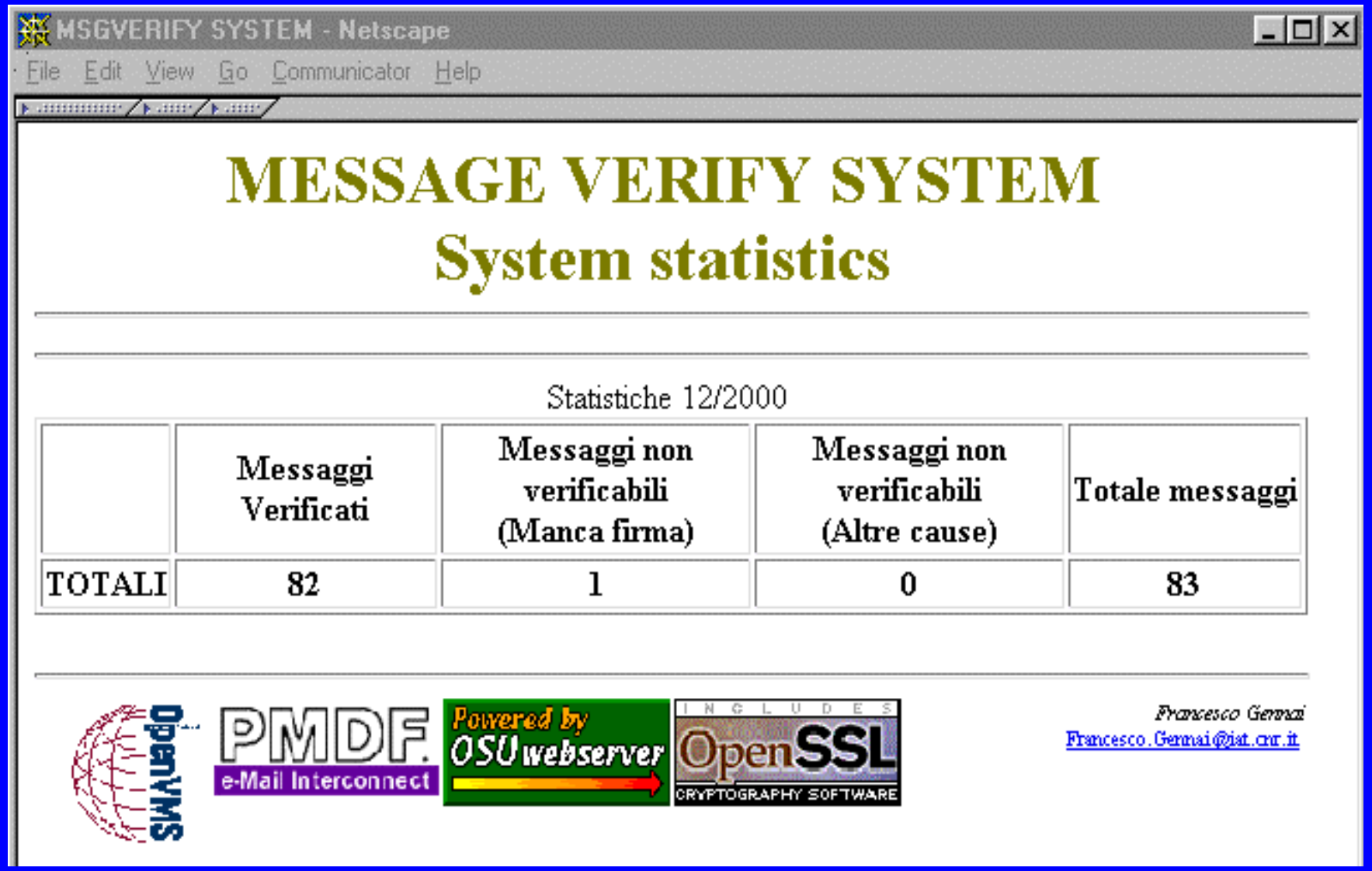
MsgVerify ErrorType

- ErrorType:
  - 0
  - 1
  - 3

  } FATAL ERROR
- ErrorType:
  - 2

  WARNING


MSGVERIFY SYSTEM - Netscape
File Edit View Go Communicator Help
MESSAGE VERIFY SYSTEM
Normal Login
PRIVILEGED USER
Privileged Login
Selezione Messaggi/Fax
Add or replace a CA's certificate
CA's certificate database management
Display CRL MANAGER log files
System configuration
System Monitor
OpenVMS
PMDF e-Mail Interconnect
Powered by OSU webserver
INCLUDES OpenSSL CRYPTOGRAPHY SOFTWARE
Francesco Gennai
Francesco.Gennai@iat.cnr.it


MSGVERIFY SYSTEM - Netscape
File Edit View Go Communicator Help
MESSAGE VERIFY SYSTEM
System statistics
Statistiche 12/2000
Messaggi Verificati
Messaggi non verificabili (Manca firma)
Messaggi non verificabili (Altre cause)
Totale messaggi
TOTALI
82
1
0
83
OpenVMS
PMDF
e-Mail Interconnect
Powered by
OSU webserver
INCLUDES
OpenSSL
CRYPTOGRAPHY SOFTWARE
Francesco Gennai
Francesco.Gennai@iat.cnr.it

Integrazione con altri servizi

- Controllo accesso a servizi basati su posta elettronica
  - servizi automatici via e-mail
  - liste di distribuzione

FINE