Potenzialità di utilizzo di token USB per l'autenticazione multi-piattaforma

Come funziona un eToken

- Memorizza certificati x509
  - Il certificato e' protetto da PIN personale
  - La chiave privata non puo' essere esportata
- Puo' contenere piu' di 1 certificato utente
- Puo' contenere piu' di 1 certificato CA
- Supporto multi-piattaforma:
  - Windows (2k,XP,Vista)
  - Linux (RedHat, Fedora, Debian*, Ubuntu*)
  - Mac OS X

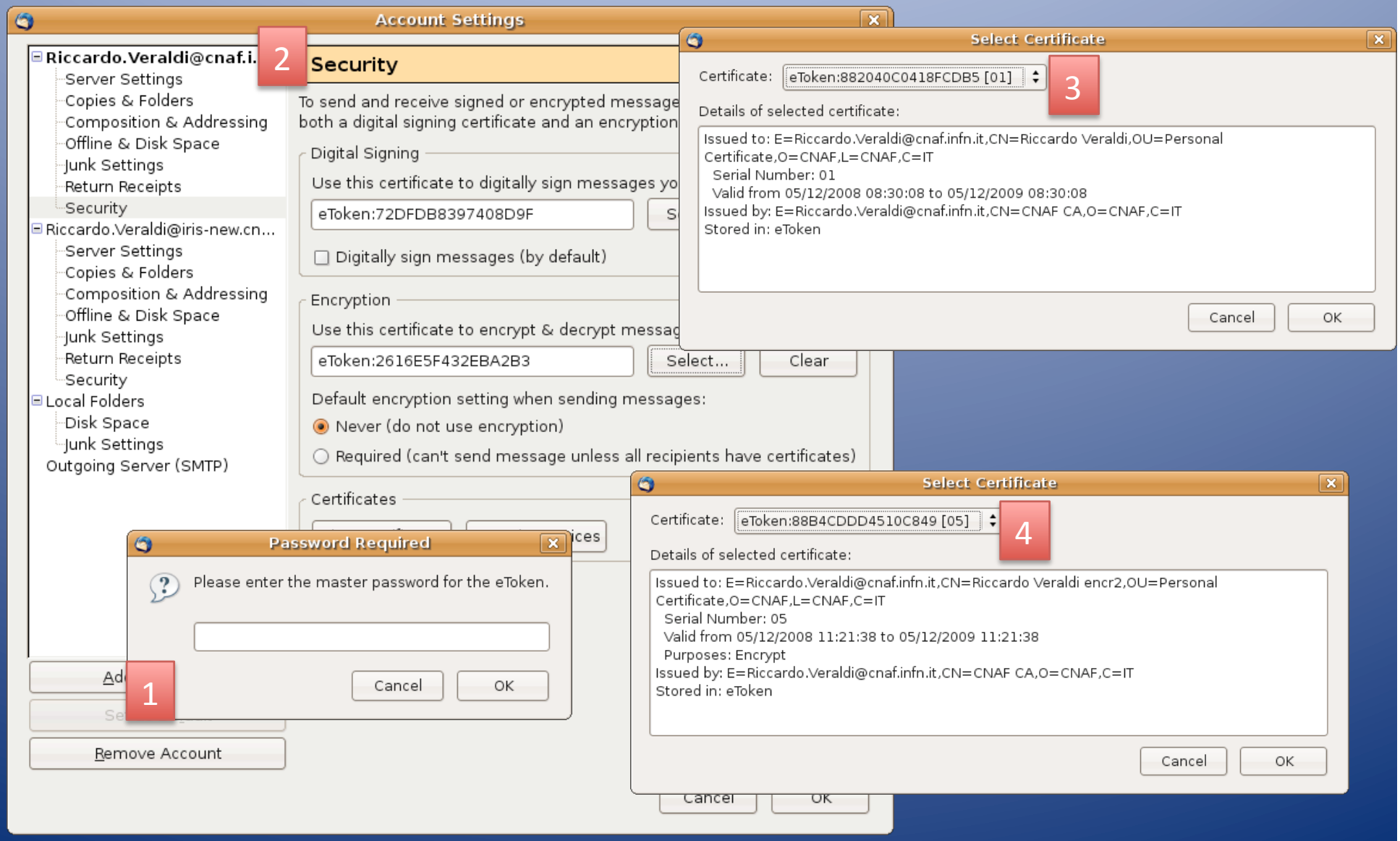
Distribuzione dei certificati utente

- 2 certificati per ogni utente
  - Digital Signing, KeyUsage
    - Rilasciato su eToken dall' INFN-CA
  - Encryption KeyUsage
    - L'utente richiede il certificato con le stesse modalita' attualmente in vigore
      - La INFN CA rislascia il certificato all'utente che lo scarica sul proprio browser
      - L'utente fa un backup del certificato (.p12) e lo memorizza in luogo sicuro
      - L'utenet carica il certificato su eToken
      - L'utente cancella il backup temporaneo (.p12)

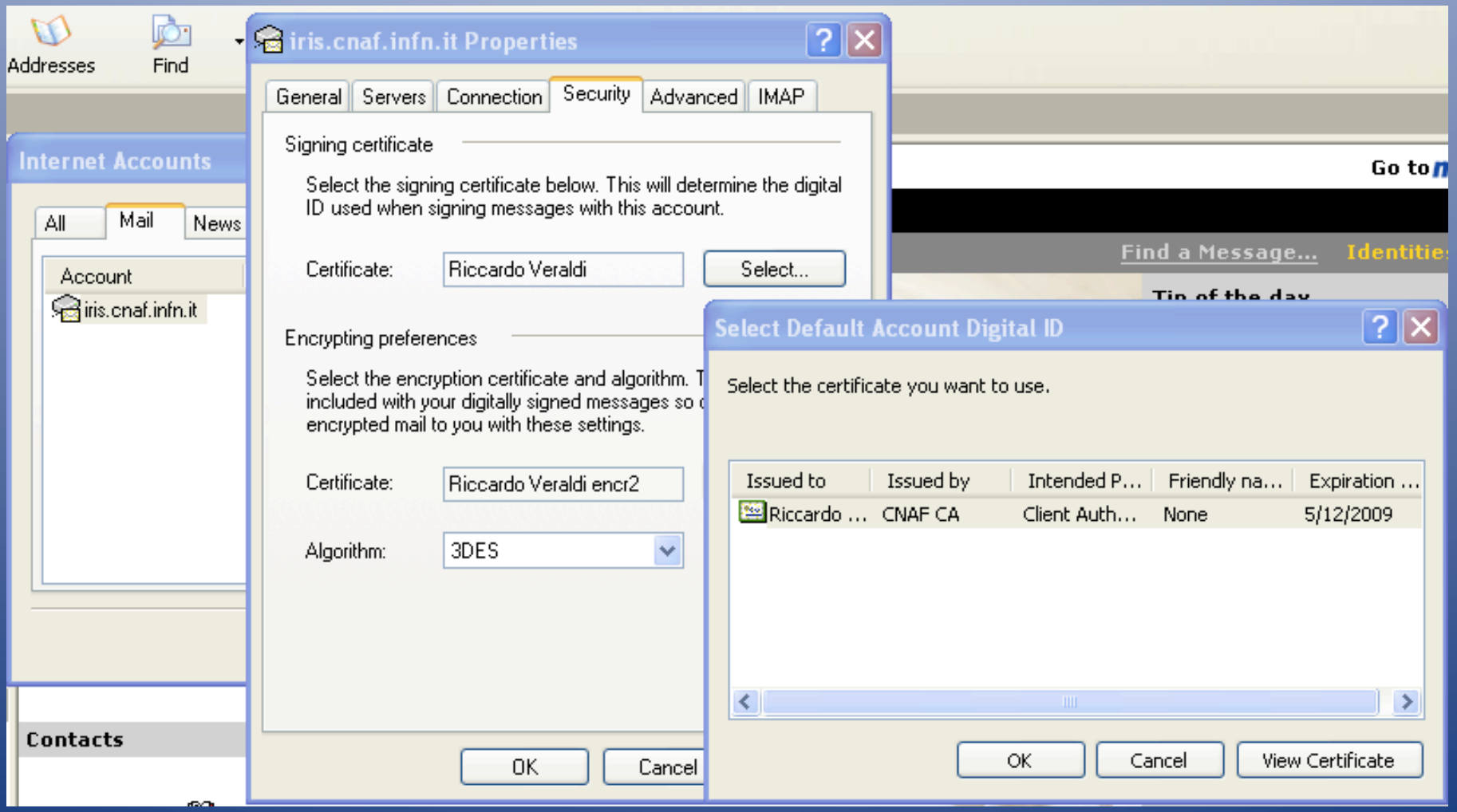
eToken: ambito di utilizzo

- Digital Signing
  - E-mail signing
    - Thunderbird
    - Outlook
- Encipherment
  - E-mail encryption
    - Thunderbird
    - Outlook
- TLS authentication
  - Mailing lists INFN wide (lists.infn.it)
  - Sendmail/postfix SMTP AUTH
  - Autenticazione IMAP
- TRIP (WiFi INFN wide)
  - INFN-dot1x, autenticazione EAP-TLS (802.1x)
  - INFN-Web captive portal
- GRID

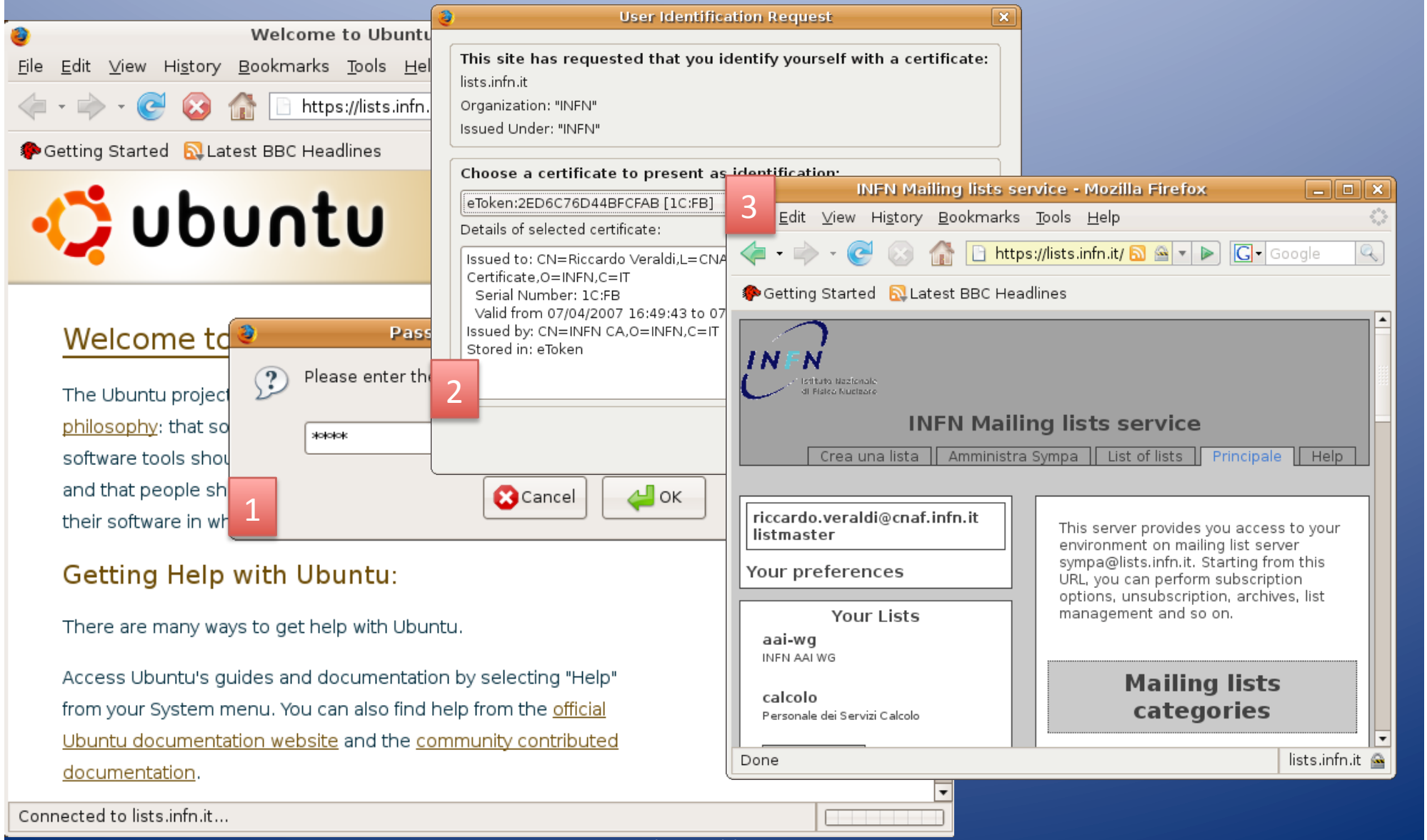
eToken e Thunderbird



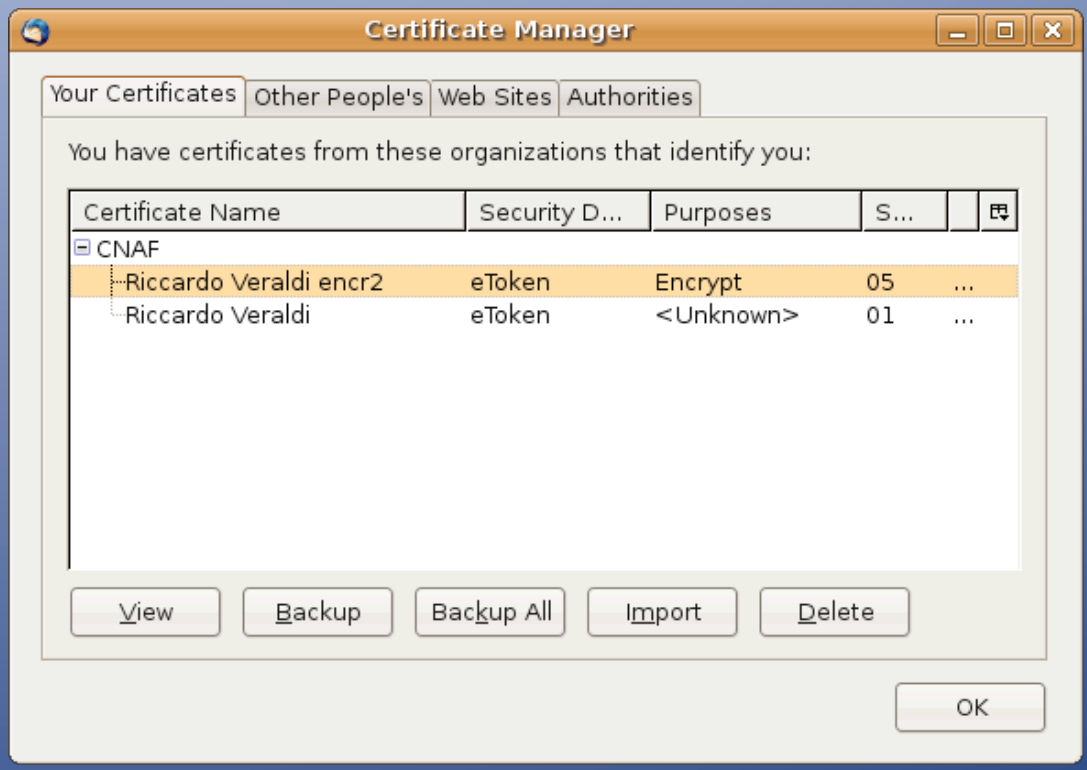
eToken e Outlook Express



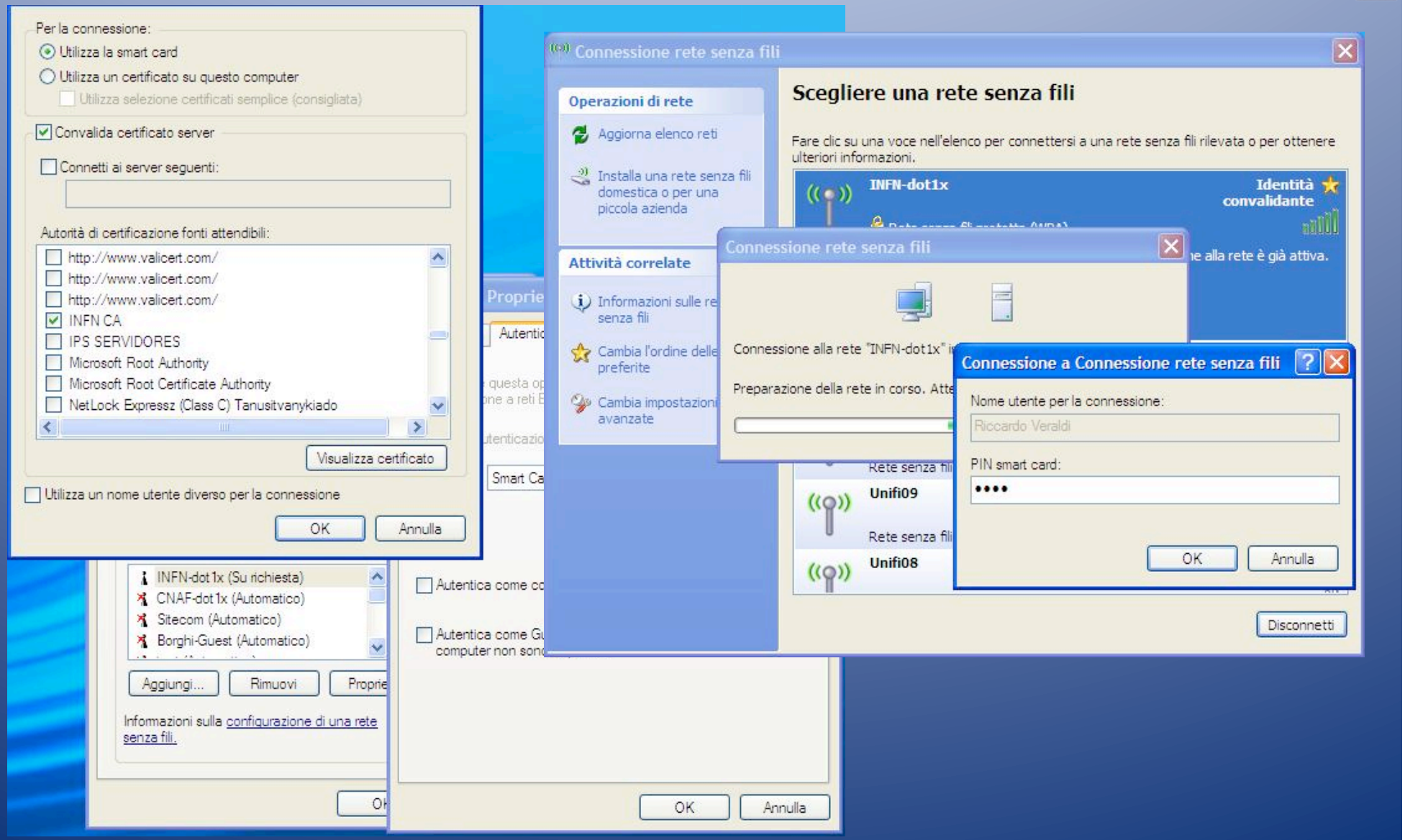
Accesso alle mailing list



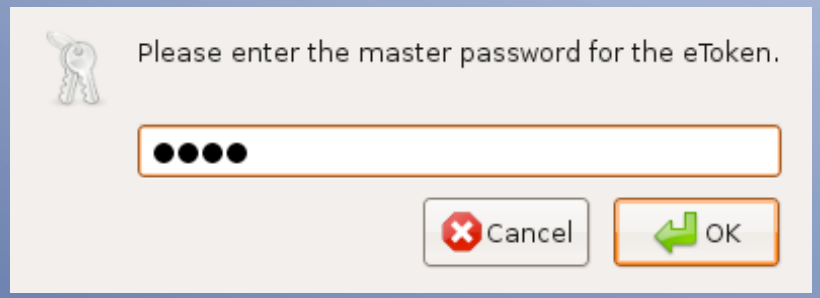
x509 SMTP AUTH

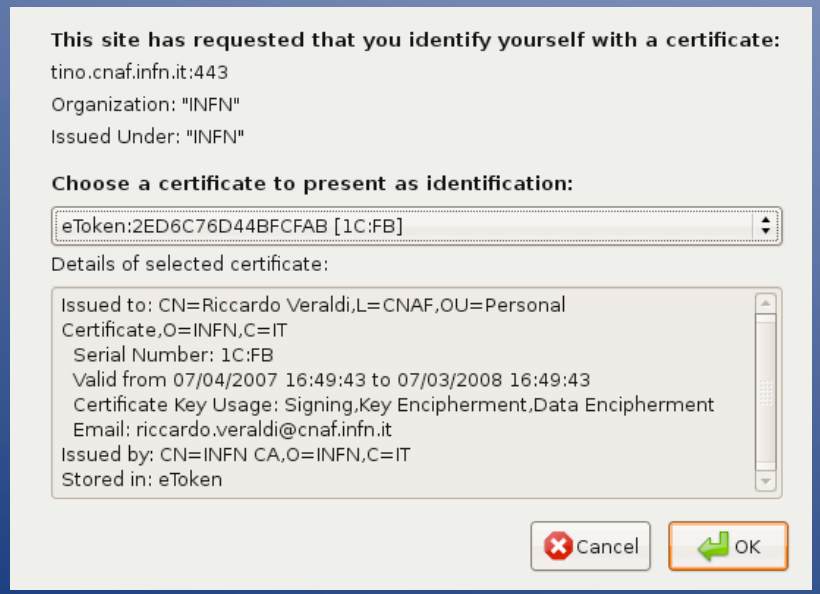


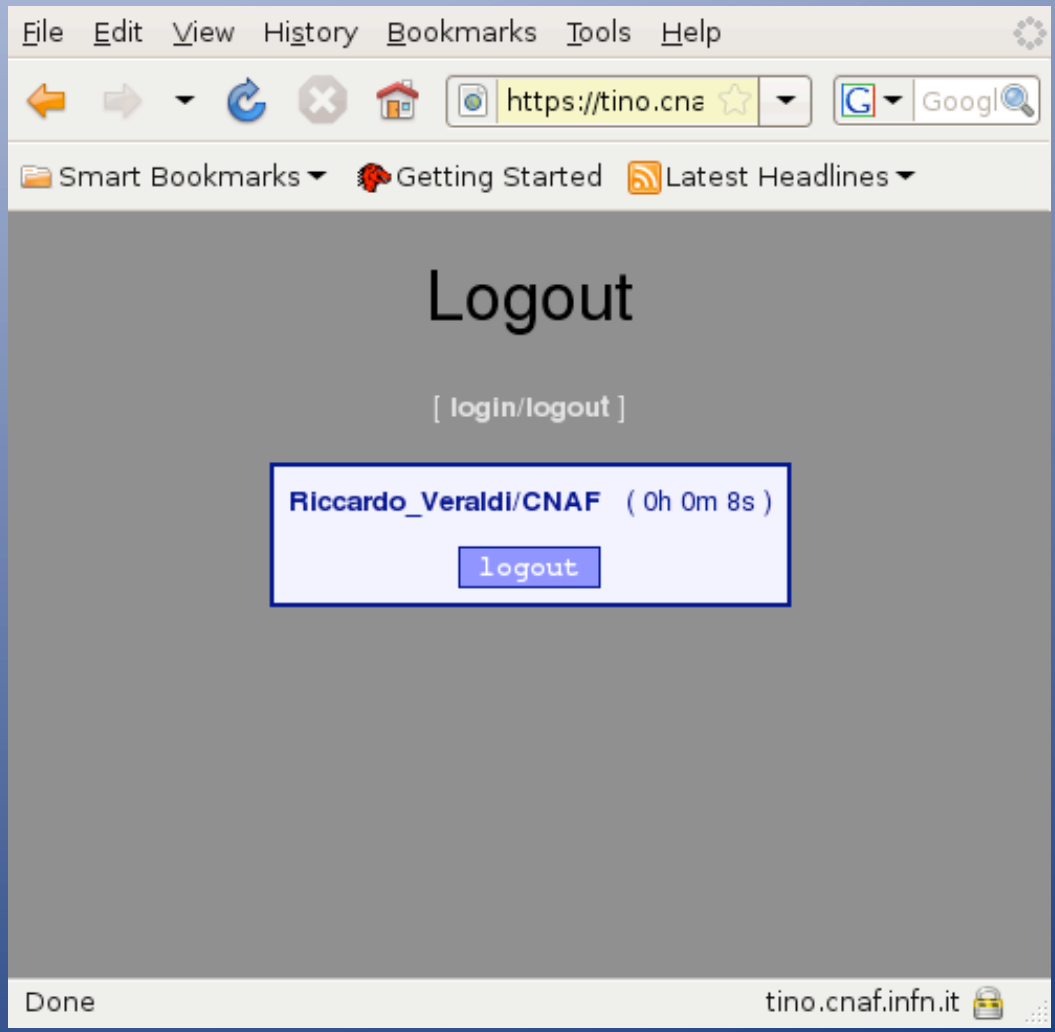
INFN-dot1x EAP-TLS (windows)



INFN-Web authentication







GRID – certificato proxy

```
veraldi@u710:~$ ./mkproxy --out=proxy.pem
Starting Aladdin eToken PRO proxy generation
Found X.509 certificate on eToken:
  label: A7FB01211D3FD63F
  id:    353830384138453838374131453936 46
Your identity: /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Riccardo Veraldi
Certificate serial number: 1CFB
Generating a 512 bit RSA private key
..++++++++++++
.....++++++++++++
writing new private key to 'proxykey.P11381'
-----
engine "pkcs11" set.
Signature ok
subject=/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Riccardo Veraldi/CN=proxy
Getting CA Private Key
PKCS#11 token PIN:
Your proxy is valid until: Sun Jun 29 10:41:00 CEST 2008
```

Durata cert proxy

VO requirement:

- ALICE: 3 giorni
- ATLAS: 4 giorni
- CMS: 8 giorni
- LHCB: 7 giorni
- CDF: 7 giorni

GRID – sottomissione job

```
testbed6> voms-proxy-init  --voms infngrid --cert proxy.pem --key proxy.pem
Creating temporary proxy to /tmp/tmp_x509up_u502_21251 ......++++++++++++
.++++++++++++
Done
Contacting  voms.cnaf.infn.it:15000 [/C=IT/O=INFN/OU=Host/L=CNAF/CN=voms.cnaf.infn.it] "infngrid" Done
Creating proxy to /tmp/x509up_u502 ..............++++++++++++
.......................++++++++++++
Done
Your proxy is valid until Fri May 30 22:43:20 2008
```

```
testbed6> globus-job-run ce05-lcg.cr.cnaf.infn.it ./xpi 100
pi=
3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803
    48253421170679821480865132823066470938446095505822317253594081284811174502841027019385211055596446229489549303819644288109756659334461284756482337867826
```

50 eToken

- 50 Beta testers
- Volontari ?