



# 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



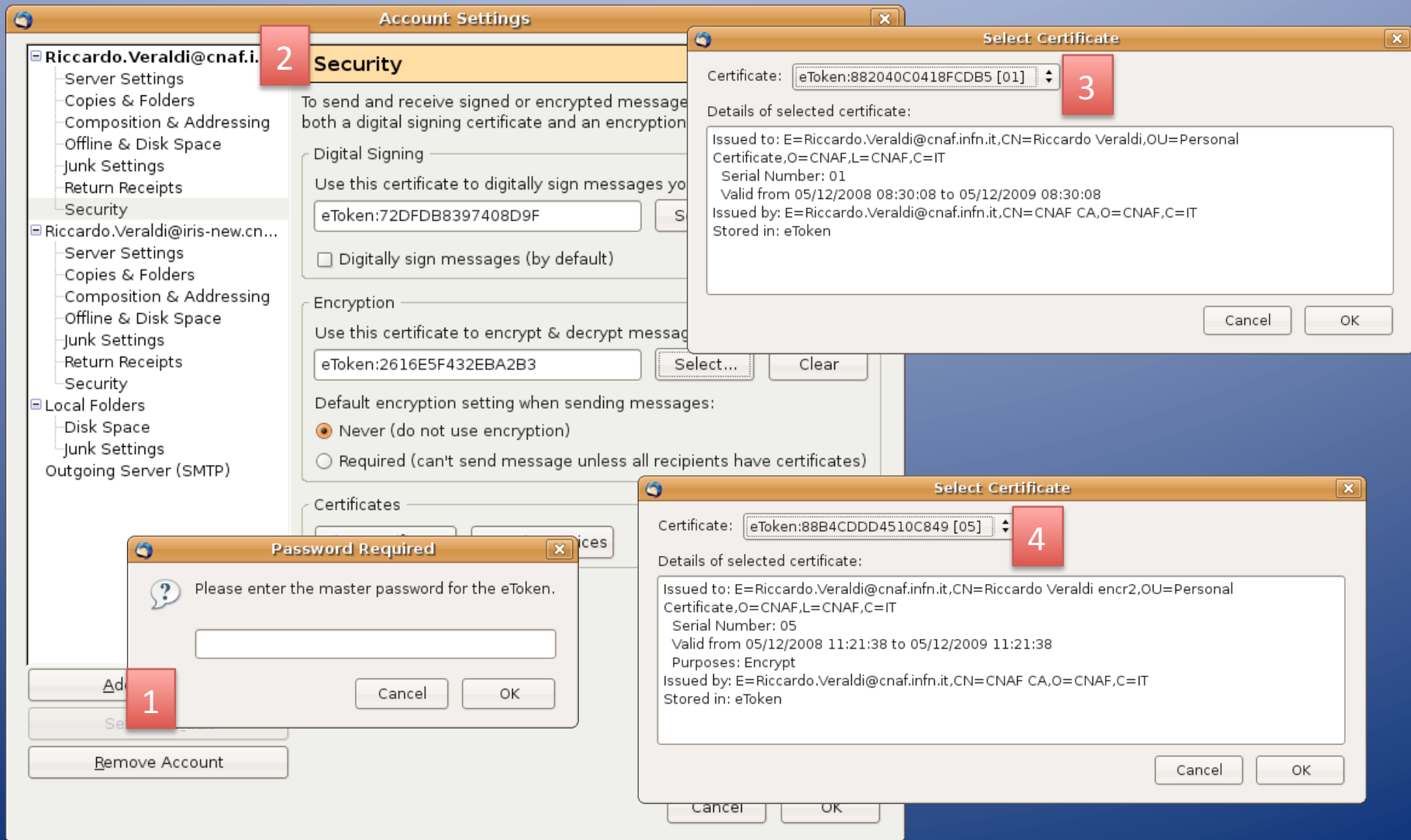


- 2 certificati per ogni utente
  - Digital Signing, KeyUsage
    - Rilasciato su eToken dall' INFN-CA
  - Encryption KeyUsage
    - L'utente richiede il certificato con le stesse modalità attualmente in vigore
      - La INFN CA rilascia il certificato all'utente che lo scarica sul proprio browser
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



- 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



**1** Add Account

**2** Security

**3** Certificate: eToken:882040C0418FCDB5 [01]

**4** Certificate: eToken:88B4CDDD4510C849 [05]

**1** Password Required

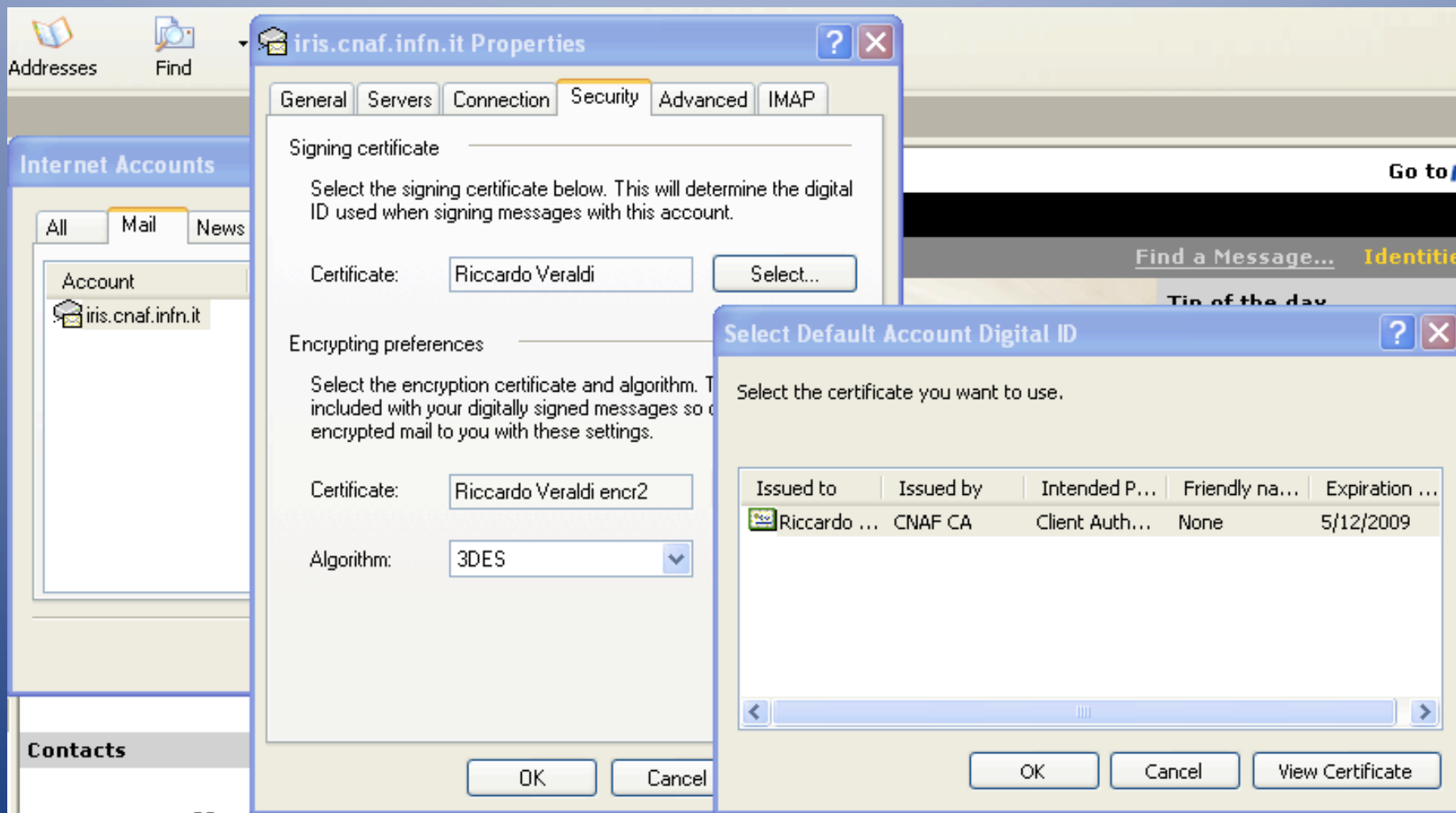
Please enter the master password for the eToken.

Cancel OK

Cancel OK

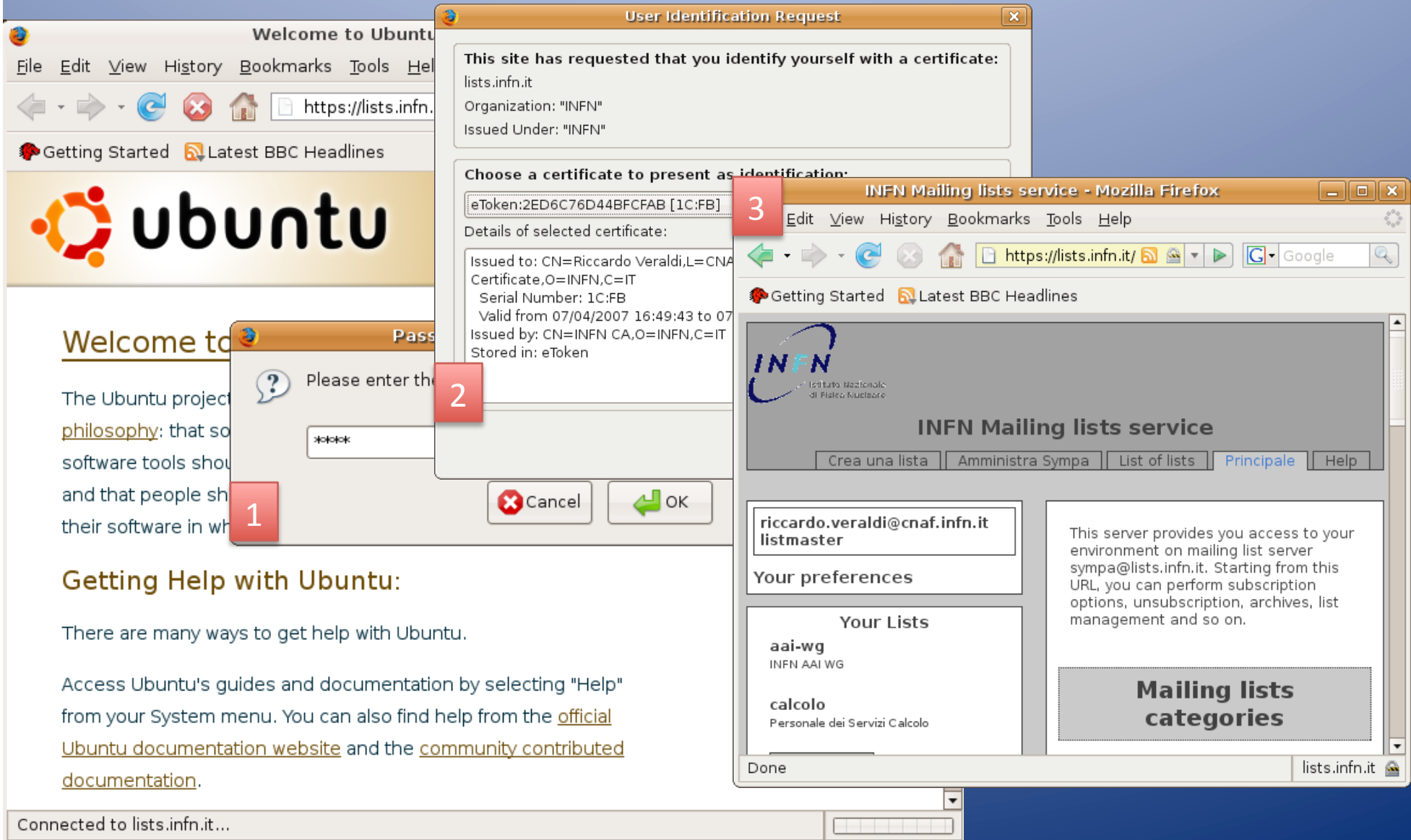
Cancel OK

Cancel OK

The screenshot displays the Outlook Express interface with the 'iris.cnaf.infn.it Properties' dialog box open to the 'Security' tab. The 'Signing certificate' section shows 'Riccardo Veraldi' selected. The 'Encrypting preferences' section shows 'Riccardo Veraldi encr2' selected for the certificate and '3DES' for the algorithm. A 'Select Default Account Digital ID' dialog box is also open, showing a table of certificates.

Issued to	Issued by	Intended P...	Friendly na...	Expiration ...
Riccardo ...	CNAF CA	Client Auth...	None	5/12/2009

The screenshot illustrates the process of accessing the INFN mailing lists service. It shows a Firefox browser window displaying the service's main page, which includes navigation links like 'Crea una lista', 'Amministra Sympa', and 'List of lists'. A 'User Identification Request' dialog box is overlaid on the browser, asking for a certificate to identify the user. The dialog provides details about the selected certificate, such as the issuer (CN=INFN CA) and validity period. A password prompt is also visible, with a red box highlighting the input field. The browser's status bar at the bottom shows 'Connected to lists.infn.it...'

# x509 SMTP AUTH



**SMTP Server**

Settings

Description: CNAF SMTP AUTH

Server Name: iris.cnaf.infn.it

Port: 587 Default: 25

Security and Authentication

Use name and password

User Name:

Use secure connection:

No  TLS, if available  TLS  SSL

Cancel OK

**Certificate Manager**

Your Certificates Other People's Web Sites Authorities

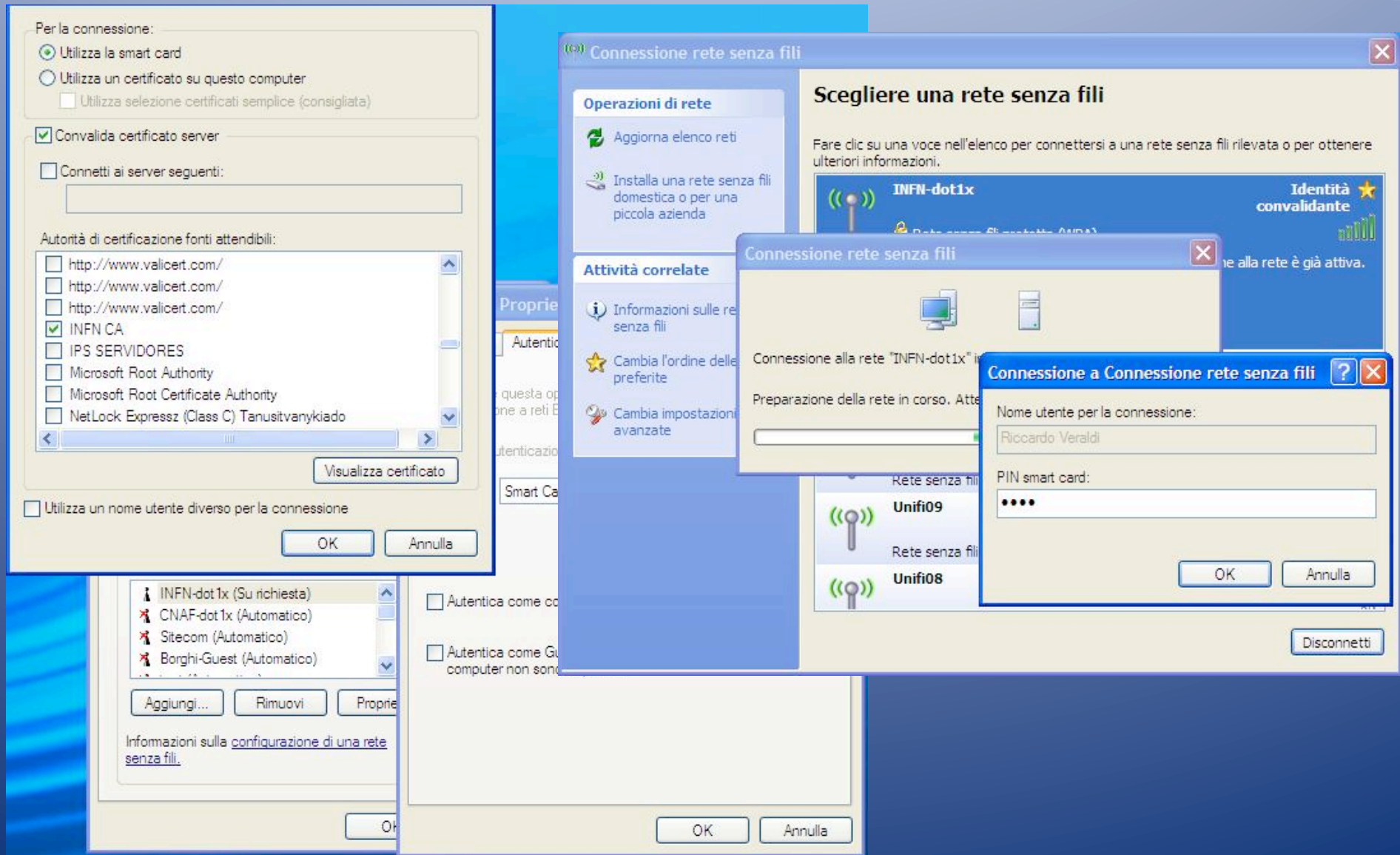
You have certificates from these organizations that identify you:

Certificate Name	Security D...	Purposes	S...		
[-] CNAF					
Riccardo Veraldi encr2	eToken	Encrypt	05	...	
Riccardo Veraldi	eToken	<Unknown>	01	...	

View Backup Backup All Import Delete

OK




The screenshot displays several overlapping Windows XP network configuration windows:

- Per la connessione:** A dialog box with options:
  - Utilizza la smart card
  - Utilizza un certificato su questo computer
  - Utilizza selezione certificati semplice (consigliata)
  - Convalida certificato server
  - Connetti ai server seguenti:
  - A list of trusted certification authorities, with **INFN CA** selected.
  - Utilizza un nome utente diverso per la connessione
- Connessione rete senza fili:** A window titled "Scegliere una rete senza fili" showing a list of available networks:
  - INFN-dot1x** (Selected)
  - Unifi09
  - Unifi08
- Connessione a Connessione rete senza fili:** A dialog box for authentication:
  - Nome utente per la connessione: Riccardo Veraldi
  - PIN smart card: [masked]
- Connessione rete senza fili (Info):** A smaller window showing "Connessione alla rete 'INFN-dot1x' in corso. Preparazione della rete in corso. Attendi." and a "Disconnetti" button.
- Background Windows:**
  - Network list window showing "INFN-dot1x (Su richiesta)", "CNAF-dot1x (Automatico)", "Sitecom (Automatico)", and "Borghi-Guest (Automatico)".
  - Properties window for "Connessione rete senza fili" with "Autentica come computer non sono..." checked.



 Please enter the master password for the eToken.

●●●●

**This site has requested that you identify yourself with a certificate:**  
tino.cnaf.infn.it:443  
Organization: "INFN"  
Issued Under: "INFN"

**Choose a certificate to present as identification:**

eToken:2ED6C76D44BF0CFAB [1C:FB]

Details of selected certificate:

Issued to: CN=Riccardo Veraldi,L=CNAF,OU=Personal  
Certificate,O=INFN,C=IT  
Serial Number: 1C:FB  
Valid from 07/04/2007 16:49:43 to 07/03/2008 16:49:43  
Certificate Key Usage: Signing,Key Encipherment,Data Encipherment  
Email: riccardo.veraldi@cnaf.infn.it  
Issued by: CN=INFN CA,O=INFN,C=IT  
Stored in: eToken

File Edit View History Bookmarks Tools Help

https://tino.cna

Smart Bookmarks Getting Started Latest Headlines

## Logout

[ login/logout ]

**Riccardo\_Veraldi/CNAF ( 0h 0m 8s )**

Done tino.cnaf.infn.it

# GRID – certificato proxy



```
veraldi@u710:~$ ./mkproxy --out=proxy.pem
Starting Aladdin eToken PRO proxy generation
Found X.509 certificate on eToken:
  label: A7FB01211D3FD63F
  id: 35383038413845383837413145393646
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



```
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
482534211706798214808651328230664709384460955058223172535940812848111745028410270193
85211055596446229489549303819644288109756659334461284756482337867826
```

# 50 eToken



- 50 Beta testers
- Volontari ?