Scenari futuri di INFN-AAI

Workshop CCR-INFN GRID 2010

Santa Tecla – Acireale (CT)

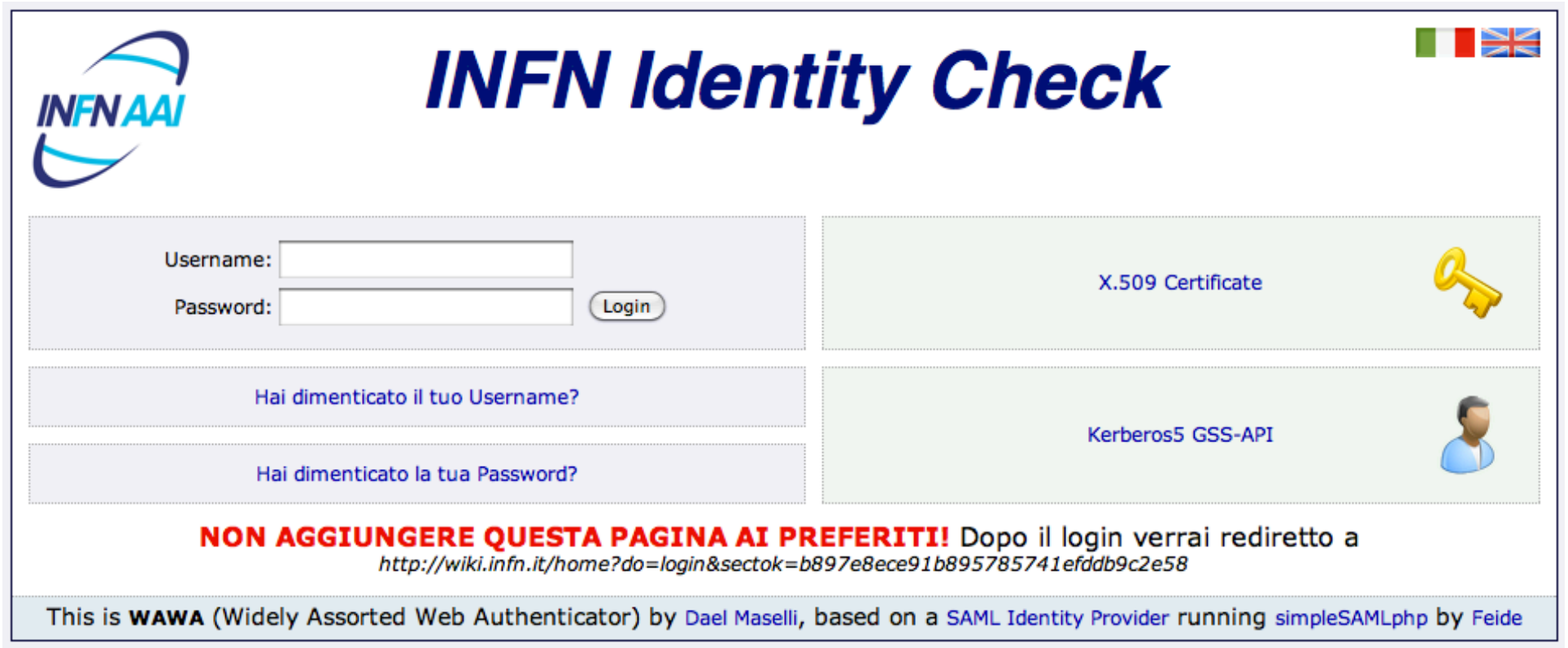
Enrico M.V. Fasanelli

INFN-AAI

INFN-AAI oggi

- Servizi di core
  - DB Oracle RAC
  - Core Master server LDAP
  - Core Slave server
  - Core KDC-slaves
  - GODiVA Application Servers
- Identity Provider SAML 2.0/Shibboleth 1.3
- Identity and Access Management System
  - GODiVA 0.9 (beta/rc1)

IdP SAML


INFN Identity Check
Username:
Password:
Login
X.509 Certificate
Hai dimenticato il tuo Username?
Kerberos5 GSS-API
Hai dimenticato la tua Password?
NON AGGIUNGERE QUESTA PAGINA AI PREFERITI! Dopo il login verrai rediretto a
http://wiki.infn.it/home?do=login&sectok=b897e8ece91b895785741efddb9c2e58
This is WAWA (Widely Assorted Web Authenticator) by Dael Maselli, based on a SAML Identity Provider running simpleSAMLphp by Feide

IdP SAML

- Applicazioni centralizzate fornite de DataWeb
- InDiCo http://agenda.infn.it/
- WIKI INFN http://wiki.infn.it/
- WEB INFN (via modulo joomla sviluppato da GARR-IDEM)
- Verificata la compatibilità con la federazione GARR-IDEM

Autorizzazione & Entitlements

- FreeRADIUS (sia 1 che 2) funziona correttamente usando INFN-AAI per:
  - Autenticazione, anche via krb5 plug-in del 389DS
  - Autorizzazione via verifica del possesso dell'entitlement **schacUserStatus = urn:mace:terena.org:schac:UserStatus:it:infn.it:networkaccess**

Cosa manca?

- Un paio di moduli di GODiVA per la gestione dei Visitatori
  - E-mail di notifica dell'auto-registrazione
  - Gestione del bar-code per la certifica dell'anagrafica
- Porting del WorkFlow degli associati sul GODiVA-DB Oracle (DataWeb)

- Import e verifica dei dati, switch server di riferimento (DSDW→INFN-AAI LDAP)

Formazione

- I corsi sul passaggio da GOapp a GODiVA partiranno entro la fine di Giugno (nei prossimi giorni fisseremo le date)
- Inizialmente dedicati alle sedi che già usano GOapp ed alle sedi pilota
- Due corsi (forse anche tre) entro la fine di Luglio 2010.

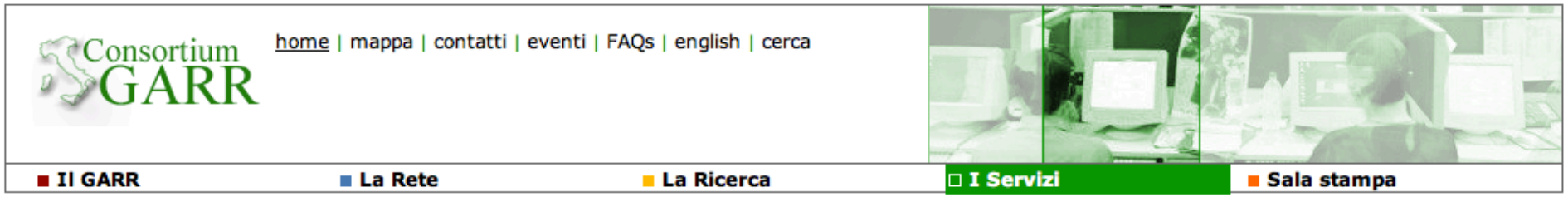
E dopo?

- Il passaggio dal Directory Server di Data Web (DSDW) alla INFN-AAI permetterà di agganciare tutti i servizi centralizzati (non solo quelli forniti da DW) alla INFN-AAI
- Per tutti i Dipendenti o Associati
- Per tutti gli Ospiti e Visitatori delle sedi che usano GOapp (e che passeranno a GODiVA)

GARR IDEM

- Federazione Italiana di Infrastrutture di Autenticazione ed Autorizzazione (AAI) che coinvolge gli enti della comunità scientifica ed accademica ed i fornitori di servizi e contenuti in rete.
- Verificata la compatibilità dell'IdP di INFN-AAI con il sistema usato da GARR-IDEM
- In fase di completamento la scrittura della documentazione richiesta da GARR-IDEM per la partecipazione al progetto

TERENA TCCS e-Science



E gli altri servizi?

- GODiVA 1.0 fornirà il supporto per poter assegnare all'utente tutti gli attributi LDAP necessari per l'utilizzo dei singoli servizi
  - Via template, fornito dai servizi di calcolo
- Qualunque servizio sia capace di utilizzare LDAP per ottenere informazioni relative all'autorizzazione, potrà essere agganciato alla INFN-AAI in modo nativo
- Per gli altri sarà necessario scrivere le interfacce opportune

UN ESEMPIO

Credenziali Kerberos5

```
kirjava:~ enrico$ klist
Kerberos 5 ticket cache: 'API:Initial default ccache'
Default principal: enrico@LE.INFN.IT

Valid Starting     Expires            Service Principal
05/19/10 00:49:05  05/19/10 10:49:04  krbtgt/LE.INFN.IT@LE.INFN.IT
```

Login su una UI GRID

```
kirjava:~ enrico$ ssh -K aaitest@gridui0.pi.infn.it
Last login: Wed May 19 00:26:50 2010 from ssire.mib.infn.it
```

Inoltro di credenziali Kerberos5

```
[aaitest@gridui0 ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_17332_IWOYe18689
Default principal: enrico@LE.INFN.IT

Valid starting     Expires            Service principal
05/19/10 00:50:52  05/19/10 10:49:04  krbtgt/LE.INFN.IT@LE.INFN.IT
```

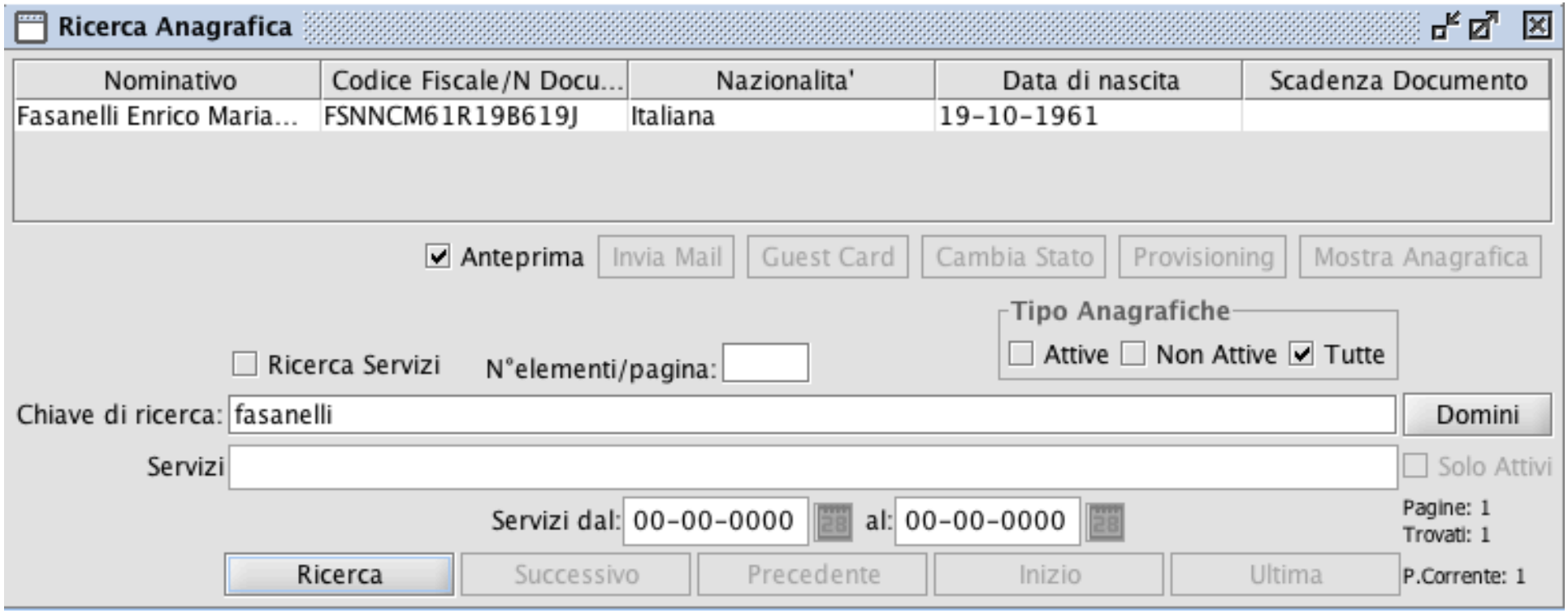
E’ solo una demo…

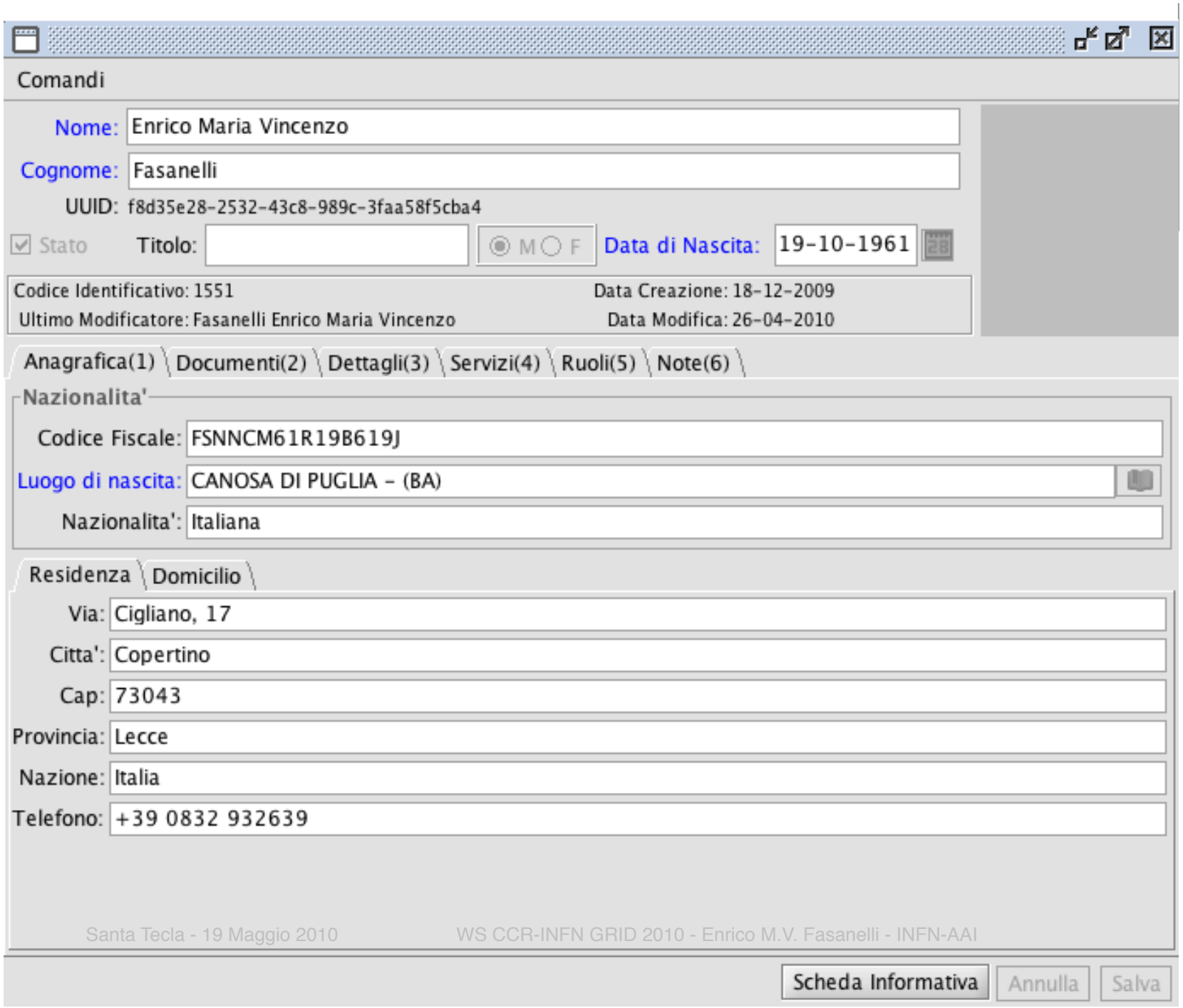
```
[aaitest@gridui0 ~]$ cat .k5login
enrico@LE.INFN.IT
carbone@MIB.INFN.IT
```

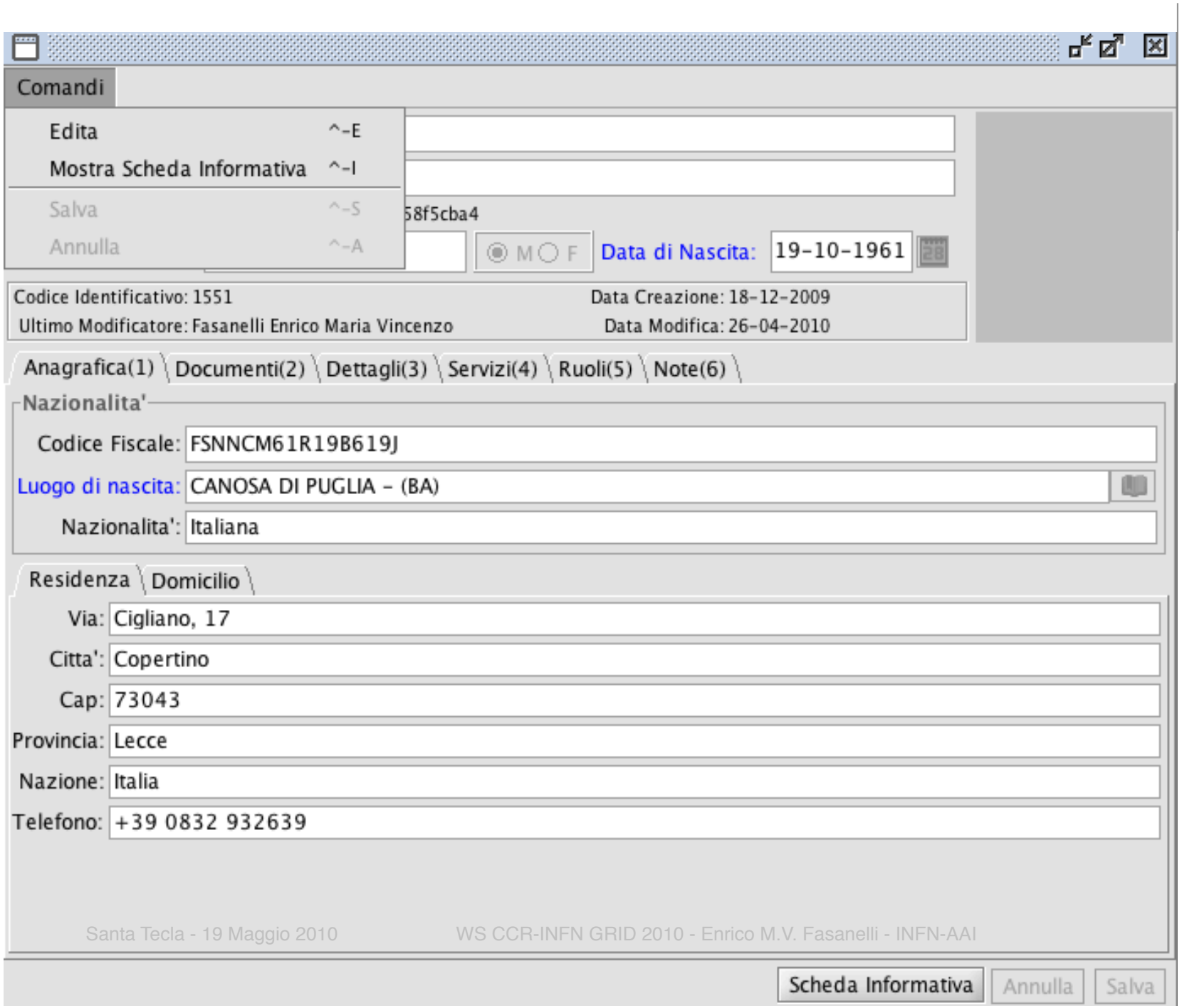
…ma ottengo l'Autorizzazione

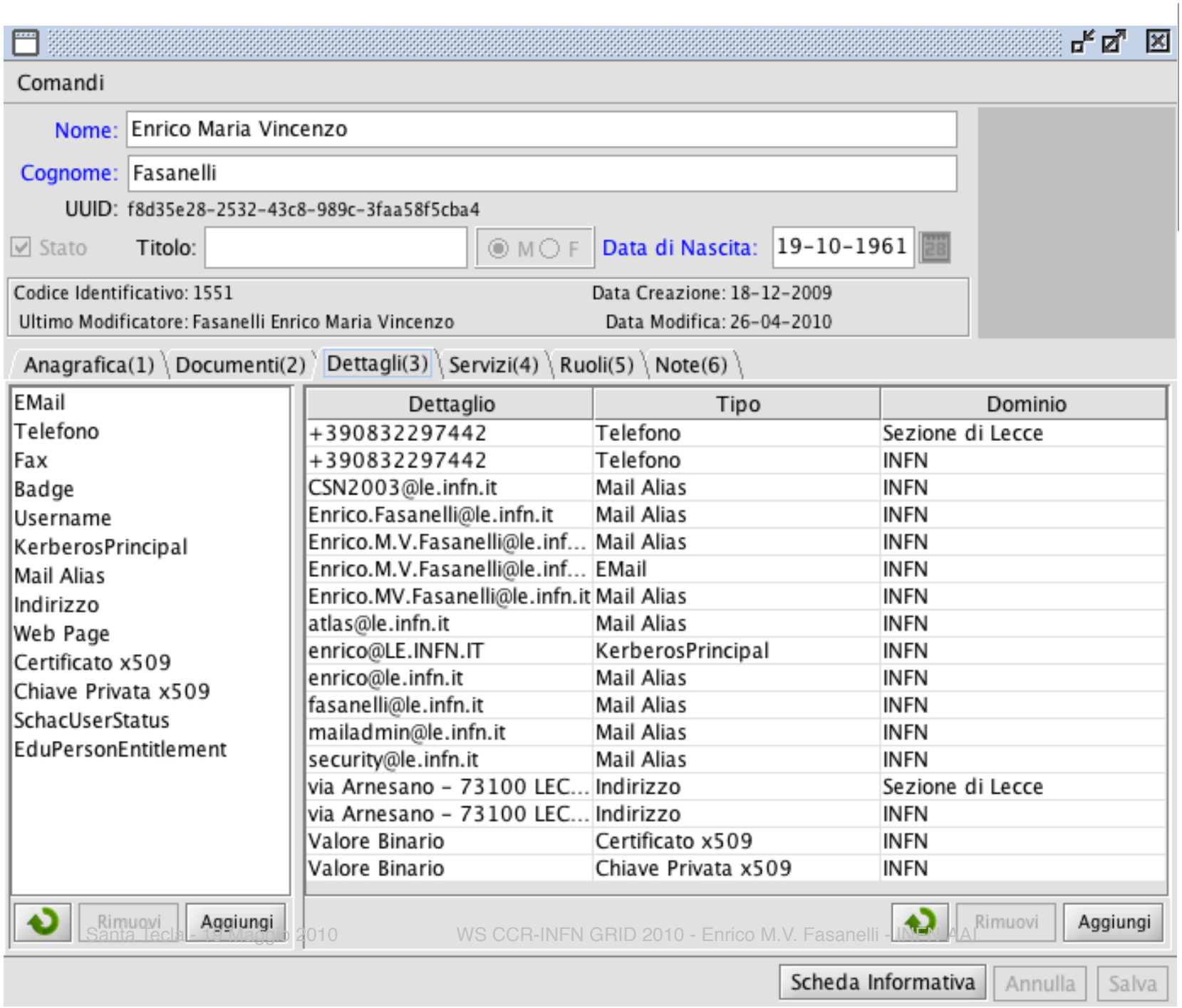
```
[aaitest@gridui0 ~]$ ./getcrt -vo gridit

Proxy file doesn't exist or has bad permissions

Enter GRID pass phrase:
Your identity: /C=IT/O=INFN/OU=Personal Certificate/L=Lecce/CN=Enrico M. V. Fasanelli
Creating temporary proxy ..................................................................
.............. Done
Contacting  voms-01.pd.infn.it:15008 [/C=IT/O=INFN/OU=Host/L=Padova/CN=voms-01.pd.infn.it] "gridit"
Done
Creating proxy ............................................... Done
Your proxy is valid until Wed May 19 12:53:11 2010
[aaitest@gridui0 ~]$
```

Uso di GODiVA




Comandi
Nome: Enrico Maria Vincenzo
Cognome: Fasanelli
UUID: f8d35e28-2532-43c8-989c-3faa58f5cba4
Stato
Titolo:
M F
Data di Nascita: 19-10-1961
Codice Identificativo: 1551
Data Creazione: 18-12-2009
Ultimo Modificatore: Fasanelli Enrico Maria Vincenzo
Data Modifica: 26-04-2010
Anagrafica(1)
Documenti(2)
Dettagli(3)
Servizi(4)
Ruoli(5)
Note(6)
Nazionalita'
Codice Fiscale: FSNNCM61R19B619J
Luogo di nascita: CANOSA DI PUGLIA - (BA)
Nazionalita': Italiana
Residenza
Domicilio
Via: Cigliano, 17
Citta': Copertino
Cap: 73043
Provincia: Lecce
Nazione: Italia
Telefono: +39 0832 932639
Scheda Informativa
Annulla
Salva


Comandi
Edita ^-E
Mostra Scheda Informativa ^-I
Salva ^-S
Annulla ^-A
58f5cba4
M F
Data di Nascita: 19-10-1961
Codice Identificativo: 1551
Data Creazione: 18-12-2009
Ultimo Modificatore: Fasanelli Enrico Maria Vincenzo
Data Modifica: 26-04-2010
Anagrafica(1) Documenti(2) Dettagli(3) Servizi(4) Ruoli(5) Note(6)
Nazionalita'
Codice Fiscale: FSNNCM61R19B619J
Luogo di nascita: CANOSA DI PUGLIA - (BA)
Nazionalita': Italiana
Residenza Domicilio
Via: Cigliano, 17
Citta': Copertino
Cap: 73043
Provincia: Lecce
Nazione: Italia
Telefono: +39 0832 932639
Scheda Informativa
Annulla
Salva


Comandi
Nome: Enrico Maria Vincenzo
Cognome: Fasanelli
UUID: f8d35e28-2532-43c8-989c-3faa58f5cba4
Stato
Titolo:
M F
Data di Nascita: 19-10-1961
Codice Identificativo: 1551
Data Creazione: 18-12-2009
Ultimo Modificatore: Fasanelli Enrico Maria Vincenzo
Data Modifica: 26-04-2010
Anagrafica(1)
Documenti(2)
Dettagli(3)
Servizi(4)
Ruoli(5)
Note(6)
EMail
Telefono
Fax
Badge
Username
KerberosPrincipal
Mail Alias
Indirizzo
Web Page
Certificato x509
Chiave Privata x509
SchacUserStatus
EduPersonEntitlement
Dettaglio
Tipo
Dominio
+390832297442 Telefono Sezione di Lecce
+390832297442 Telefono INFN
CSN2003@le.infn.it Mail Alias INFN
Enrico.Fasanelli@le.infn.it Mail Alias INFN
Enrico.M.V.Fasanelli@le.inf... Mail Alias INFN
Enrico.M.V.Fasanelli@le.inf... EMail INFN
Enrico.MV.Fasanelli@le.infn.it Mail Alias INFN
atlas@le.infn.it Mail Alias INFN
enrico@LE.INFN.IT KerberosPrincipal INFN
enrico@le.infn.it Mail Alias INFN
fasanelli@le.infn.it Mail Alias INFN
mailadmin@le.infn.it Mail Alias INFN
security@le.infn.it Mail Alias INFN
via Arnesano - 73100 LEC... Indirizzo Sezione di Lecce
via Arnesano - 73100 LEC... Indirizzo INFN
Valore Binario Certificato x509 INFN
Valore Binario Chiave Privata x509 INFN
Rimuovi
Aggiungi
Rimuovi
Aggiungi
Scheda Informativa
Annulla
Salva

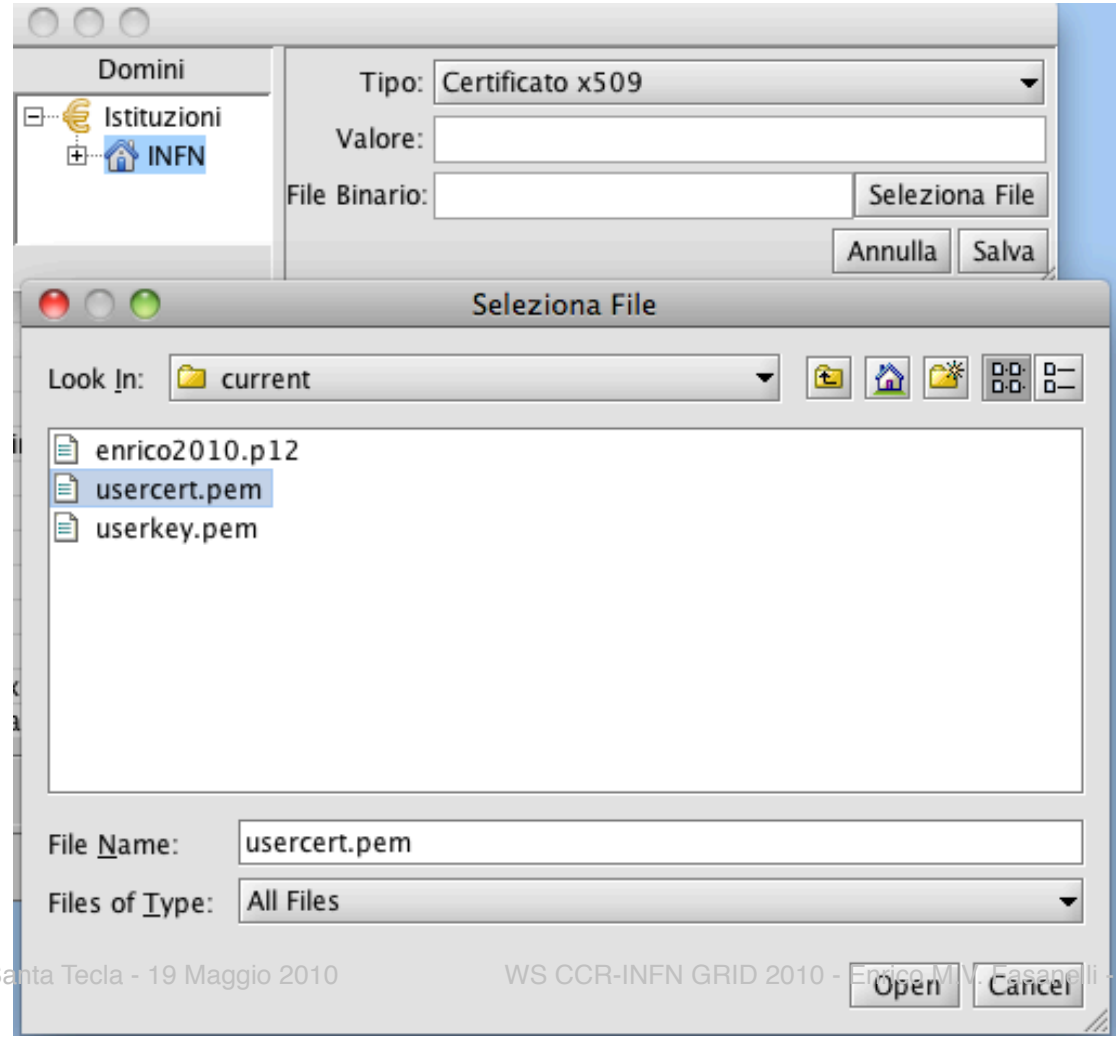
ACI al lavoro - 1

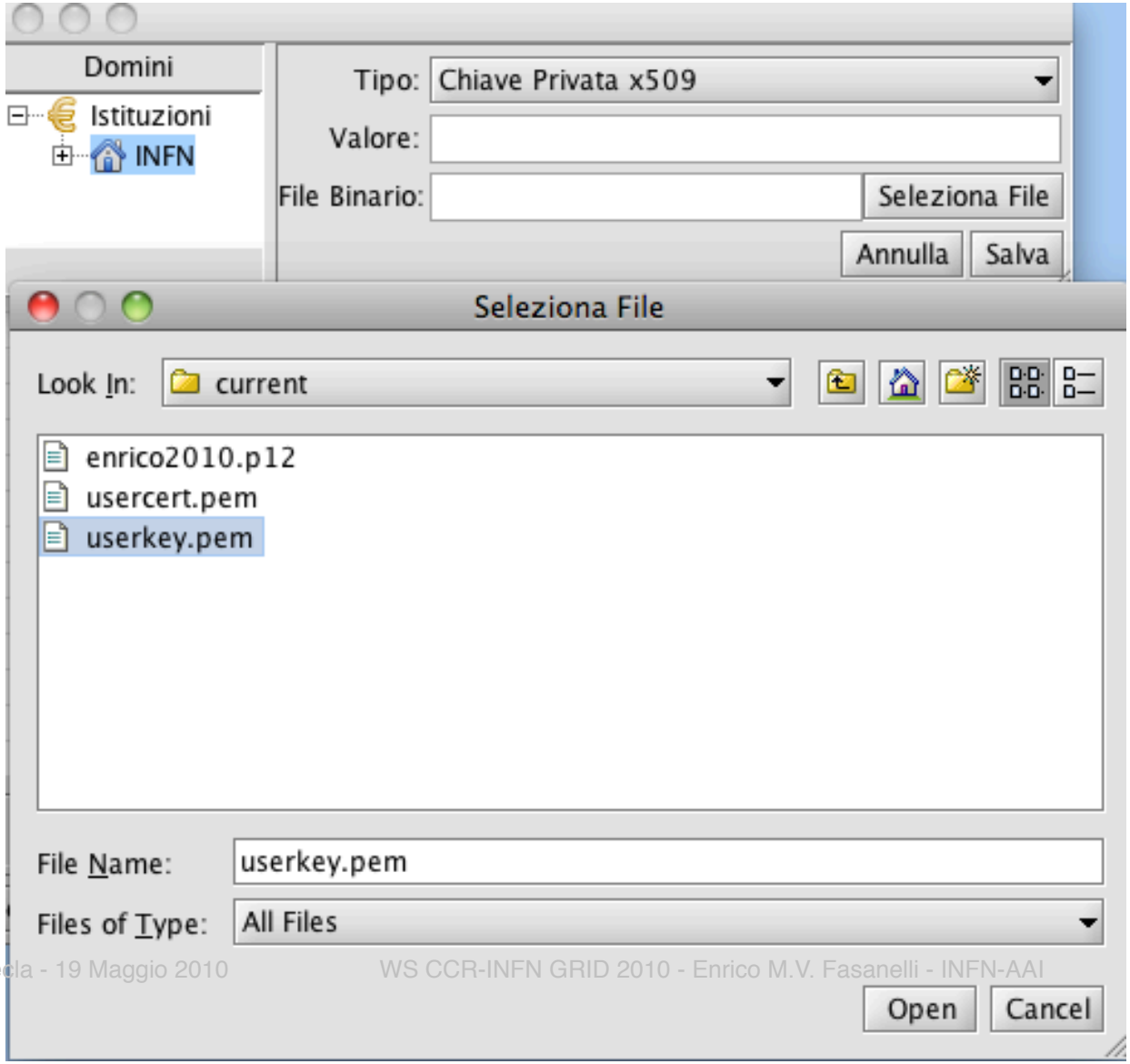
```
[aaitest@gridui0 ~]$ ldapsearch -YGSSAPI -ZZZ -h aaidevds.lnf.infn.it -b ou=People,dc=infn,dc=it '(uid
=enrico)' userCertificate
SASL/GSSAPI authentication started
SASL username: enrico@LE.INFN.IT
SASL SSF: 56
SASL installing layers
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=infn,dc=it> with scope subtree
# filter: (uid=enrico)
# requesting: userCertificate
#

# f8d35e28-2532-43c8-989c-3faa58f5cba4, People, infn.it
dn: infnUUID=f8d35e28-2532-43c8-989c-3faa58f5cba4,ou=People,dc=infn,dc=it
userCertificate:: QmFnIEF0dHJpYnV0ZXMKICAgIGZyaWVuZGx5TmFtZTogRW5yaWNvIE0uIFYu
 IEZhc2FuZWxsaQogICAgbG9jYWxlZXlJRDogODkgQUYgMTcgODcgODggRDkgMTAgRDMgRUEgM0EgR
 jMgQTEgMDUgQUIgRTkgNTIgMDcgMjYgRUYgODIgCnN1YmplY3Q9L0M9SVQvTz1JTkZOL09VPVBlcn
```

ACI al lavoro - 2

```
[aaitest@gridui0 ~]$ ldapsearch -YGSSAPI -ZZZ -h aaidevds.lnf.infn.it -b ou=People,dc=infn,dc=it '(uid
=carbone)' \*
SASL/GSSAPI authentication started
SASL username: enrico@LE.INFN.IT
SASL SSF: 56
SASL installing layers
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=infn,dc=it> with scope subtree
# filter: (uid=carbone)
# requesting: *
#

# 9ba5d1be-29cc-44e5-a437-83eb1bf3f727, People, infn.it
dn: infnUUID=9ba5d1be-29cc-44e5-a437-83eb1bf3f727,ou=People,dc=infn,dc=it
infnUUID: 9ba5d1be-29cc-44e5-a437-83eb1bf3f727

# search result
search: 5
result: 0 Success

# numResponses: 2
# numEntries: 1
```

```
[aaitest@gridui0 ~]$ klist -fa
Ticket cache: FILE:/tmp/krb5cc_17332_MmgxOF2438
Default principal: enrico@LE.INFN.IT

Valid starting     Expires            Service principal
05/19/10 00:50:52  05/19/10 10:49:04  krbtgt/LE.INFN.IT@LE.INFN.IT
        Flags: FfT
        Addresses: (none)
05/19/10 05:51:52  05/19/10 10:49:04  krbtgt/INFN.IT@LE.INFN.IT
        Flags: FfT
        Addresses: (none)
05/19/10 05:51:52  05/19/10 10:49:04  krbtgt/LNF.INFN.IT@INFN.IT
        Flags: FfT
        Addresses: (none)
05/19/10 05:51:52  05/19/10 10:49:04  ldap/aaidevds.lnf.infn.it@LNF.INFN.IT
        Flags: FfT
        Addresses: (none)
```


Domini
Istituzioni
INFN
Tipo:
Certificato x509
Valore:
File Binario:
Seleziona File
Annulla
Salva
Seleziona File
Look In:
current
enrico2010.p12
usercert.pem
userkey.pem
File Name:
usercert.pem
Files of Type:
All Files
Open
Cancel


Domini
Istituzioni
INFN
Tipo:
Chiave Privata x509
Valore:
File Binario:
Seleziona File
Annulla
Salva
Seleziona File
Look In:
current
enrico2010.p12
usercert.pem
userkey.pem
File Name:
userkey.pem
Files of Type:
All Files
Open
Cancel