ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Milano Bicocca, Gruppo Collegato di Parma

INFN/CCR-08/01
June 16, 2008

CCR-22/08/P

UNA INFRASTRUTTURA DI AUTENTICAZIONE E AUTORIZZAZIONE FLESSIBILE E SCALABILE PER UNA COMUNITA' SCIENTIFICA LOCALE

Roberto Alfieri, Roberto Covati

INFN-Sezione di Milano Bicocca, Gruppo Collegato di Parma
Viale G.P. Usberti n.7/A I-43100 Parma, Italy

Abstract

Viene descritto un modello scalabile di Autenticazione e Autorizzazione per l'accesso a tutte le risorse di calcolo e di rete per una ampia comunità locale di utenti, come può essere un Campus Scientifico. L'infrastruttura è stata implementata presso il Campus Universitario di Parma.

*Published by **SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

1 INTRODUZIONE

La crescita continua di risorse disponibili all'interno una LAN fornisce all'utente sempre nuovi strumenti il lavoro, ma, d'atra parte, ne complica l'attività se le Policy di Accesso non sono coordinate all'interno di una infrastruttura di Autenticazione e Autorizzazione (AA).
In questo documento viene descritto il progetto e l'implementazione di un modello di AA per gestire l'accesso, in modo flessibile, integrato e scalabile, alle principali risorse informatiche e di rete di una Comunità locale di utenti in ambito scientifico, come può essere ad esempio un Campus Universitario.
Le risorse integrate sono i principali strumenti di calcolo e di rete quali: accesso ai sistemi (Linux, Windows e MacOsX), alle applicazioni Web (Wiki, WebMail), alle risorse fisiche (stampanti, reti Wireless o Wired).
Gli utenti della Comunità possono provenire da diverse Organizzazioni, accomunate dalla condivisione delle risorse di LAN. Le Organizzazioni gestiscono l'Identità degli Utenti tramite gli Identity Server (IS) i quali contengono gli attributi di Identità, di ruolo e le credenziali di autenticazione (Username/Password e , se disponibile, il certificato X.509).
Il diagramma dei domini è riportato in Figura 1. Esempi di Domini Amministrativi sono l'Università, la Sezione INFN, e l'Unità CNR che afferiscono alla stessa LAN di Campus.

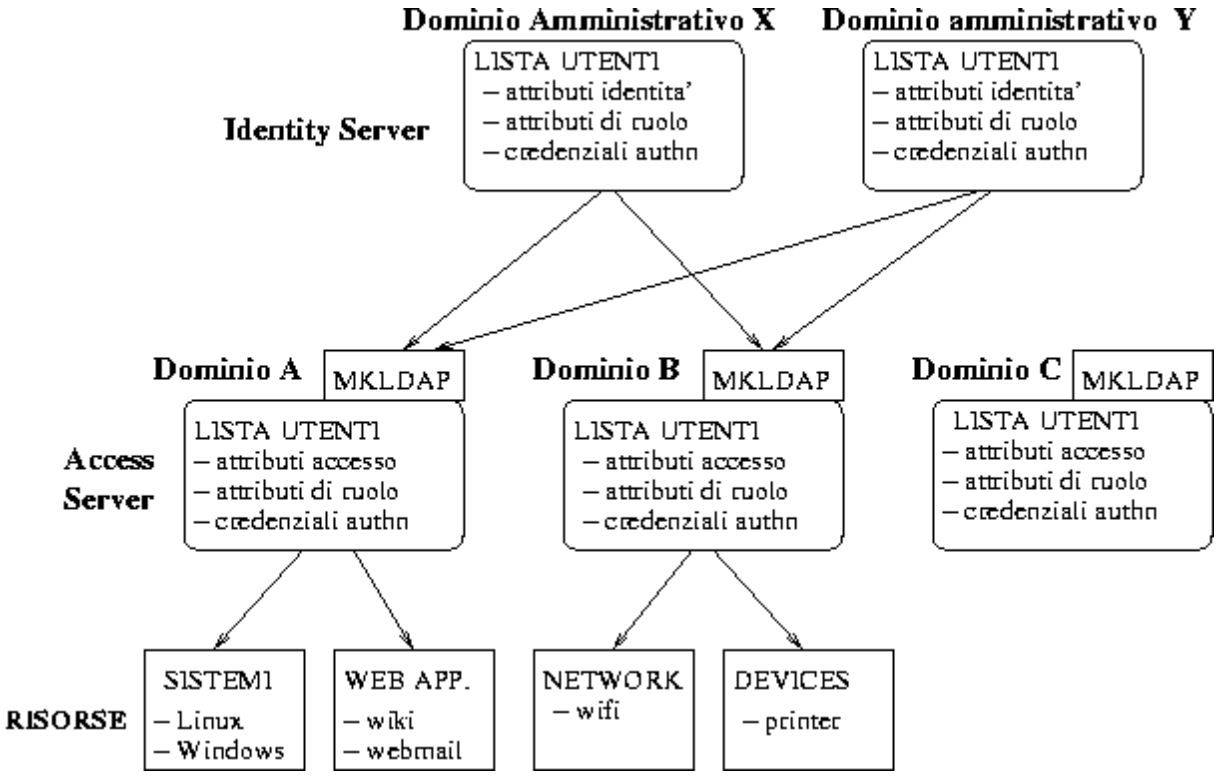

FIG. 1: Modello dei Domini

L'accesso alle risorse è regolato dagli Access Server (AS), anche questi basati su LDAP. Un AS applica le regole di accesso di un Dominio di Autorizzazione che sono specificate in un opportuno file di configurazione. Il programma “mkldap” applica le direttive del file di

configurazione (mkldap.conf) e aggiorna le informazioni dell'AS consultando periodicamente gli IS. Esempi di Domini di Autorizzazione sono: la sezione INFN, il Dipartimento Universitario, le aule Informatiche, gli utenti della Biblioteca, gli studenti di un Corso di Laurea.

2 L'IDENTITY SERVER

L'IS è un servizio in cui vengono registrate in modo univoco, autorevole e aggiornato le informazioni di Identità, Ruolo e alcune informazioni di Accesso (e.g. credenziali, UIDnumber) delle Entità di una Organizzazione, quale può essere ad esempio un Ente, una Università o una Azienda. Le Entità possono essere persone, unità organizzative o apparati (e.g. computer) strutturati all'interno dell'Organizzazione.

L'IS contiene quindi informazioni che sono alla base di qualunque Policy che lega risorse e utilizzatori all'interno delle Organizzazioni federate.

2.1 L'Identity Server dell'Ateneo di Parma

L'Università di Parma è una Organizzazione di circa 60000 persone tra Personale, Studenti e Ospiti che a vario titolo frequentano l'Ateneo e devono accedere alle sue risorse Informatiche.
L'Ateneo e' strutturato in Unità Organizzative quali Dipartimenti, Istituti, Facoltà e Uffici Amministrativi, che possono disporre di proprio personale e proprie risorse, ma che comunque devono interagire e collaborare con le altre Unità.
Il punto di partenza di qualsiasi Policy di AA che sia flessibile e scalabile è una Base di Dati autorevole e aggiornata che contenga le informazioni di Identità, gli attributi di ruolo e le credenziali di Autenticazione di tutti gli utenti dell'Ateneo (Identity Service).
Il Centro di Calcolo Elettronico[1)] dell'Ateneo di Parma nel 2003 ha attivato un Identity Service implementato mediante un Directory Server OpenLdap.
L'Entry dell'utente contiene informazioni di Accesso quali:

- Username, univoco all'interno dell'Ateneo.
- Password, nei vari formati (Posix e LM/NT); l'allineamento dei formati è garantito dall'utilizzo di uno script centralizzato per la creazione e la modifica.
- Certificati X.509 per autenticazione PKIX, anche se per ora non e' utilizzata.
- UIDnumber a 16 bit, univoco nell'IS.

Inoltre sono incluse informazioni specifiche relative ai ruoli degli utenti dell'Ateneo, quali la la struttura di appartenenza, la posizione con tutti i dati relativi. Per questo l'Università di Parma ha creato uno Schema Ldap specifico, registrato con Object Identificator (OID) numero 1.3.6.1.4.14657.
Alcune ObjectClass significative sono:

```
objectclass ( 1.3.6.1.4.14657.1.1.2.2
 NAME 'personaUniPR'
 SUP LDAPaccountUniPR
 MUST ( categoria $ uPortalDefLayout )
 MAY ( c $ isManager $ title $ codiceFiscale $ dataNascita $
       luogoNascita $ localityName ) )
objectclass ( 1.3.6.1.4.14657.1.1.2.3
```

```
      NAME 'studenteUniPR'
      SUP personaUniPR
      MUST ( matricola )
      MAY ( facolta $ corsolaurea $ anno $ datafine $ tipo $
            annocorso $ codcomune $ provincia $ cittadinanza $
            matricolainiziale $ annoPrimaImm $ codcomnascita )  )
objectclass ( 1.3.6.1.4.14657.1.1.2.4
      NAME 'ospiteUniPR'
      DESC 'Ospite Università'
      SUP personaUniPR
      MUST ( ownerDN )
      MAY ( qualifica )  )
objectclass ( 1.3.6.1.4.14657.1.1.2.6
      NAME 'docentiUniPR'
      DESC 'docenti e ricercatori UniPR'
      SUP dipendenteUniPR
      MAY ( ruolo $ confermato )  )
objectclass ( 1.3.6.1.4.14657.1.1.2.7
      NAME 'staffUniPR'
      DESC 'tecnici amministrativi UniPR'
      SUP dipendenteUniPR
      MAY ( livello $ area )   )
objectclass ( 1.3.6.1.4.14657.1.1.2.12
        NAME 'dottorandoUniPR'
        DESC 'Dottorando Università'
        SUP personaUniPR
        MUST ( ownerDN $ codiceDottorato $ cicloDottorato $ nomeDottorato )
        MAY ( qualifica ) )
```

I dati degli utenti sono organizzati in un Directory Information Tree (DIT) con la seguente struttura:

```
dc=unipr,dc=it
     + ou=People
       + ou=Personale
         + cn=...
         + cn=...
       + ou=Studenti
         + cn=...
         + cn=...
       + ou=Ospiti
       + ou=Borse e Dottorandi
       + ou=SSIS
       + ou=Erasmus
   + ou=Strutture
```

2.2 L'IS come Server di Accesso

L'IS dell'Università di Parma può essere utilizzato direttamente come AS Ldap per l'autenticazione degli utenti. In effetti esistono diversi servizi che attualmente si autenticano in questo modo. I principali sono l'autenticatore del portale Wifi e il CAS.

- **Autenticatore WIFI.** Il sistema di accesso per le reti Wireless di Ateneo e' basato su di una piattaforma proprietaria (HP ProCurve[2)]) la quale consente, tra l'alto, l'accesso tramite un Captive Portal dotato di un autenticatore con backend LDAP (o Radius). L'autenticatore svolge anche una parte di autorizzazione attraverso un attributo LDAP il cui valore consente di attribuire agli utenti profili personalizzati.

- **CAS**[3] (Central Authentication Server): e' un servizio sviluppato dall'Università di Yale che consente di concentrare in un unico punto l'autenticazione di tutte le Applicazione Web dell'Organizzazione. Al momento dell'autenticazione il client viene dirottato sul server CAS con un canale cifrato HTTPS e dopo l'autenticazione con credenziali standard (password Posix e a breve Certificati X.509) ritorna sull'applicazione con un Token utilizzabile per autenticazioni successive (Single Sign On).

I limiti di questo tipo di utilizzo stanno nella scalabilità limitata e nella scarsa flessibilità nella definizione delle Policy di accesso (Autorizzazione).

3 L'ACCESS SERVER

L'introduzione dell'AS consente di decentrare l'Access Management separandolo dall'Identity Management. Gli AS aprono periodicamente un canale cifrato verso gli IS, aggiornano i dati, quindi chiudono il canale. L'AS gestisce in modo autonomo il dominio locale di autorizzazione, dipendendo dall'IS centrale solo per l'aggiornamento. Inoltre la distribuzione dei dati rende scalabile il modello.

Un AS contiene uno o più Domini di Autorizzazione. L'amministratore dell'AS può creare e aggiornare un nuovo Dominio mediante il programma MkLdap.

L'AS è un server Linux su cui deve essere installato, oltre a MkLdap, un Directory Server come openLDAP e Samba (per le eventuali risorse Windows).

Il DIT dell' AS e dei Domini ha la seguente struttura:

```
<AS_baseDN>           (es: dc=fis,dc=unipr,dc=it)
     + ou=Dominio1    (es: ou=fisica)
     + ou=Dominio2    (es: ou=calcolo)
     + ou=Dominio3    (es: ou=grid)
     + ou=Dominio4    (es: ou=infn)
     + cn=browser
<DominioX_baseDN>      (es: ou=fisica,dc=fis,dc=unipr,dc=it)
     + ou=Users
       + ou=Personale
         + uid=..
       + ou=Studenti
         + uid=..
       + ou=Ospiti
       + ou=SSIS
       + ou=Erasmus
       + ou=locali
       + uid=nobody
       + uid=root
     + ou=Computers
       + uid=...
       + uid=...
     + ou=Groups
       + cn=Studenti
       + cn=personale
       + cn=Ospiti
       + cn=SSIS
       + cn=Borse e Dottorati
       + cn=Erasmus
```

```
    + cn=locali
    + cn=...
  + ou=Mounts
    + ou=auto.master
     + ou=auto.\/home
  + sambaDomainName=xxxx
```

L'inserimento negli AS di utenti provenienti da diversi Domini Amministrativi pone il problema dell'identificazione univoca degli utenti stessi. L'indirizzo email, che fa oramai parte degli attributi di identità di tutti i Domini Amministrativi, costituisce Identificativo naturale per questo scopo. Esistono però anche attributi di accesso, come l'UIDnumber, che possono richiedere univocità in tutti gli AS della comunità. La soluzione adottata per questo problema consiste nell'inserimento dell'UIDnumber nell'IS con numerazioni a 16 bit (< 65536). Questo numero viene poi utilizzato per generare nell'AS un nuovo UIDnumber ottenuto sommando UIDnumber originale ad un prefisso identificativo dell'IS, multiplo di 10^6.

3.1 Lo script Mkldap

Il programma MkLdap si occupa della creazione del DIT e delle eventuali Home Directory degli utenti, compresa la gestione della Quota dello spazio disco.

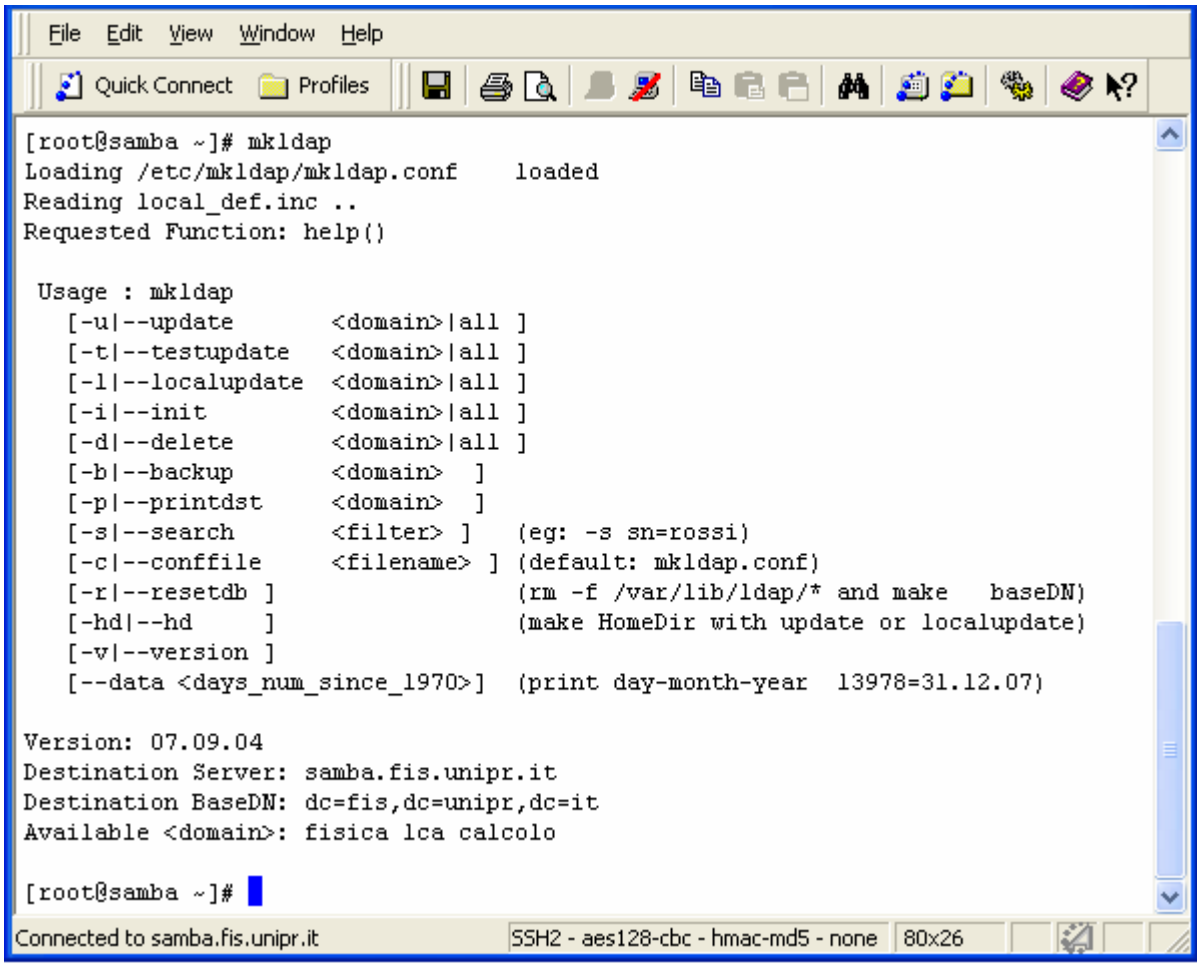

FIG. 2: Interfaccia di mkldap

La gestione dei servizi Windows è realizzata con Samba, il cui schema è l'unico aggiuntivo rispetto agli schema standard di openLDAP.
MkLdap è un programma scritto in PHP che svolge tutte le funzioni per la gestione di un AS mediante una interfaccia a linea di comando, come si vede in Figura 2.
La funzione **init** consente all'amministratore di creare un nuovo Dominio, mentre la funzione **update** che dovrà essere schedulata periodicamente, contatta gli IS e allinea il Dominio sulla base delle direttive del file di configurazione **mkldap.conf.**
Alcuni utenti o attributi non presenti sul IS possono essere definiti localmente (nel file **local_def.inc**) e aggiornati con la funzione **localupdate**.
Nel file di configurazione vengono specificate le direttive per includere, o inibire singoli utenti o gruppi definiti in base agli attributi di identità o di ruolo.
La regola **ldapadd** seleziona per inserimento tutti gli utenti individuati dal filtro specificato.
La regola **ldapban** esclude gli utenti selezionati dall'inserimento.
La regola **groupadd** definisce un nuovo gruppo e la lista degli utenti che lo compongono.
Si veda come esempio la Figura 3.

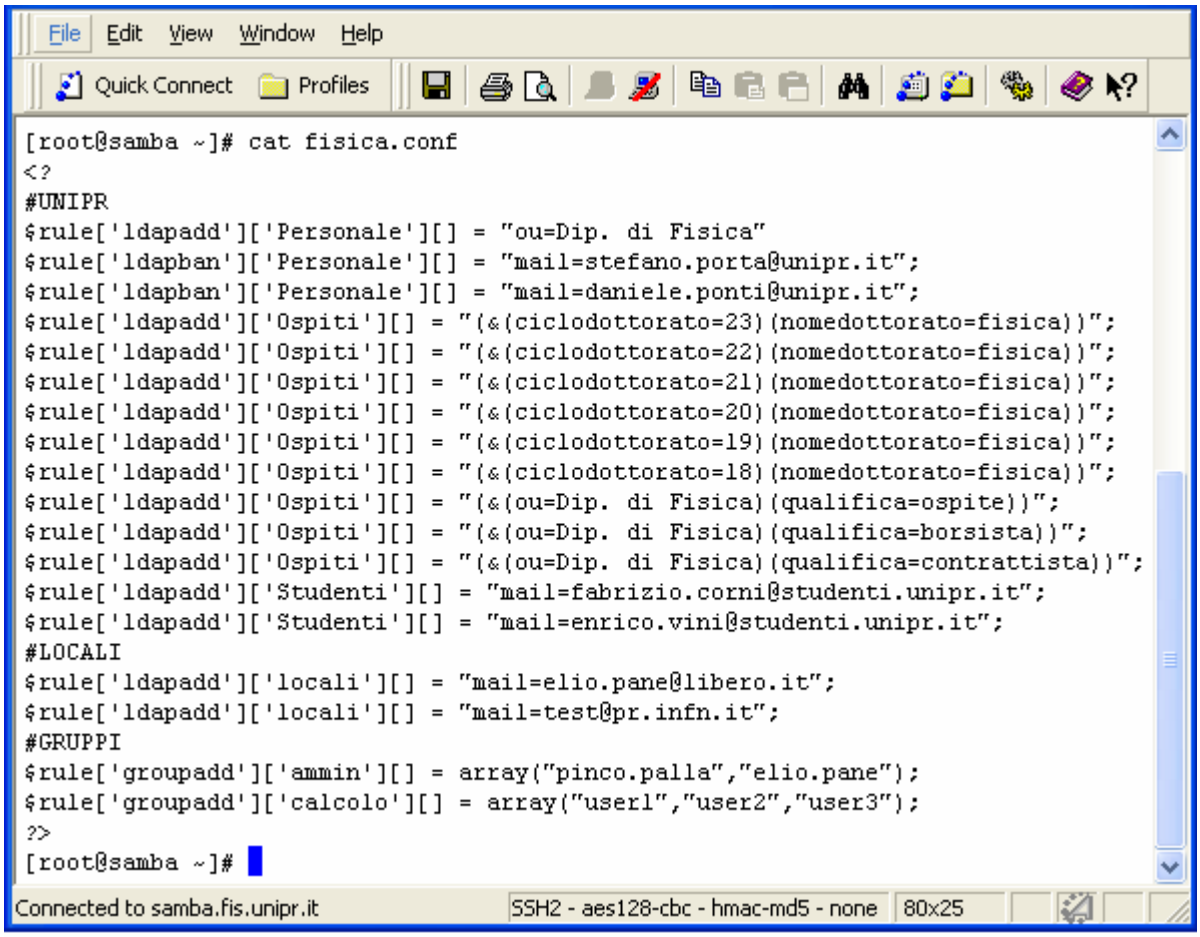

FIG. 3: Il file di configurazione di mkldap

Se necessario i domini di Autorizzazione possono essere cancellati e ricostruiti nel giro di pochi secondi, partendo dal file di configurazione. Questo consente di muovere agevolmente un Dominio da un AS all'altro, oppure di attivare repliche dei dati senza ricorrere ai servizi del Directory Server.

3.2 Gli Access Server del Dipartimento di Fisica

I 3 AS attualmente in funzione gestiscono 7 Domini di Autorizzazione, coprendo tutte attività di servizio e di ricerca del Dipartimento di Fisica/INFN e gran parte delle attività didattiche della Facoltà di Scienze. I domini sono:

- **fisica**: Personale strutturato e ospiti del Dipartimento di Fisica
- **infn:** Afferenti al gruppo Collegato INFN di Parma.
- **calcolo**: Utenti del sistema di Calcolo Dipartimentale
- **grid**: Utenti locali della Farm Grid
- **biblioteca:** Utenti delle risorse informatiche della biblioteca del Dipartimento di Fisica.
- **didattica**: Utenti (studenti e docenti) delle risorse per la Didattica del Dipartimento di Fisica.
- **scienze:** Utenti (studenti e docenti) delle risorse per la Didattica della Facoltà di Scienze.

Gli utenti di questi domini accedono in modo autenticato con le stesse credenziali a tutte le risorse disponibili, tra cui:

- I sistemi Linux, Windows e Mac OS X (server dipartimentali, aule informatiche, PC personali, PC ad accesso pubblico, farm di calcolo, farm Grid)
- Le code di stampa in modo autenticato e contabilizzato
- Le applicazioni Web, quali i Wiki (personali o di gruppo), WebMail, ecc.
- L'accesso alla rete (Wireless o, se necessario, Wired)

4 CONCLUSIONI

Dall'estate 2007 sono attivi 3 AS con 7 Domini gestendo le Policy di accesso di tutti gli afferenti al Dipartimento di Fisica, all'INFN e tutti gli studenti della Facoltà di Scienze.
Sono in corso contatti per estendere l'infrastruttura ad altre strutture dell'Ateneo.

5 BIBLIOGRAFIA

(1) Centro di Calcolo Elettronico (CCE) dell'Ateneo di Parma - http://www.cce.unipr.it
(2) HP Procurve - http://www.hp.com/rnd/products/wireless/700wlseries/overview.htm
(3) CAS - http://www.ja-sig.org/products/cas/