Installazione e configurazione

di un server Lightweight Directory Access Protocol

Loredana Martusciello, Francesco Gennai

loredana.martusciello@isti.cnr.it, francesco.gennai@isti.cnr.it

Introduzione

Il Lightweight Directory Access Protocol – **LDAP** (la versione corrente è LDAPv3, RFC3377) è un protocollo di rete che consente di interrogare e modificare un directory service. Un directory LDAP si conforma al modello X.500 e consiste, quindi, di un albero (Directory Information Tree – **DIT**) di **entry**, organizzate in una gerarchica, ognuna delle quali rappresenta un oggetto del mondo reale, come mostrato in figura 1.

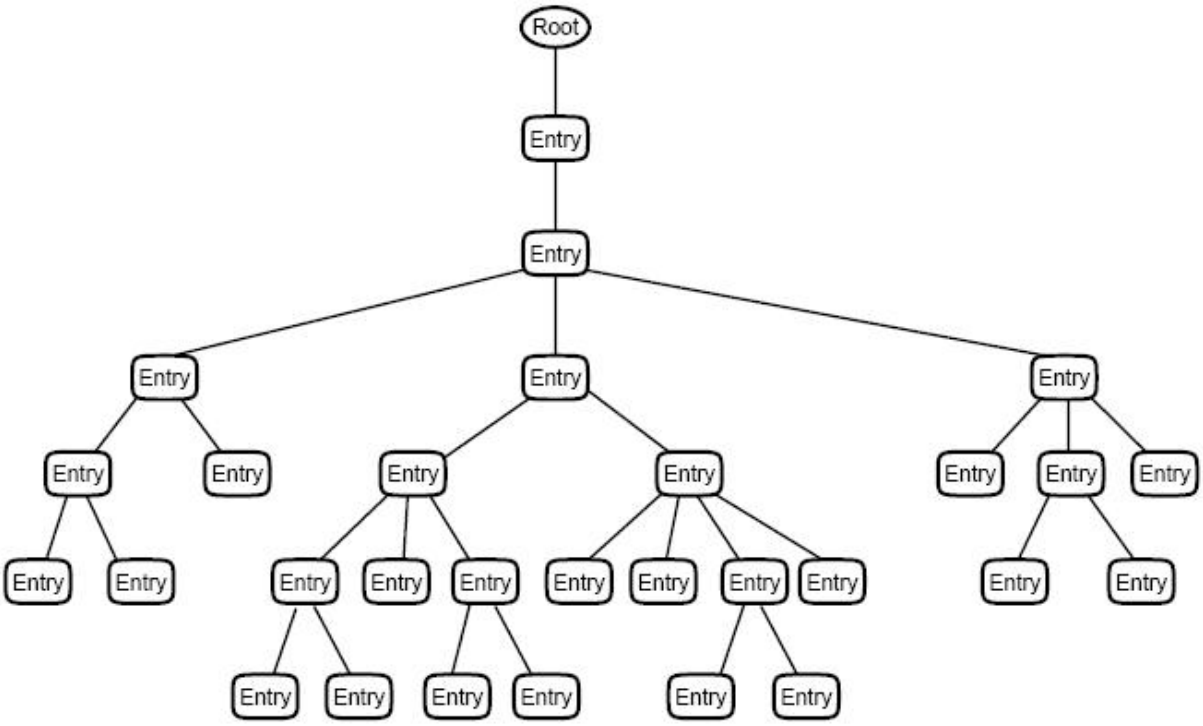

Figura1: la struttura gerarchica di un DIT

La posizione delle entry nella gerarchia dovrebbe essere basata sulle relazioni tra gli oggetti del mondo reale che rappresenta. Ad esempio, una entry che rappresenta una persona può essere posizionata al di sotto della entry che rappresenta l'organizzazione in cui la persona lavora. La struttura gerarchica determina il nome delle entry e, inoltre, permette una suddivisione del DIT in sottoalberi che possono essere distribuiti e replicati su server diversi.

La struttura di un directory LDAP generalmente riflette diversi vincoli di tipo politico, geografico e organizzativo. Oggi si tende ad utilizzare i nomi del Domain Name System (**DNS**) per strutturare il

primo livello della gerarchia (la root del DIT). Nel directory possono apparire entry che rappresentano persone, gruppi di persone, unità organizzative, stampanti, documenti, etc. La Figura 2 illustra una tipica entry rappresentante una persona.

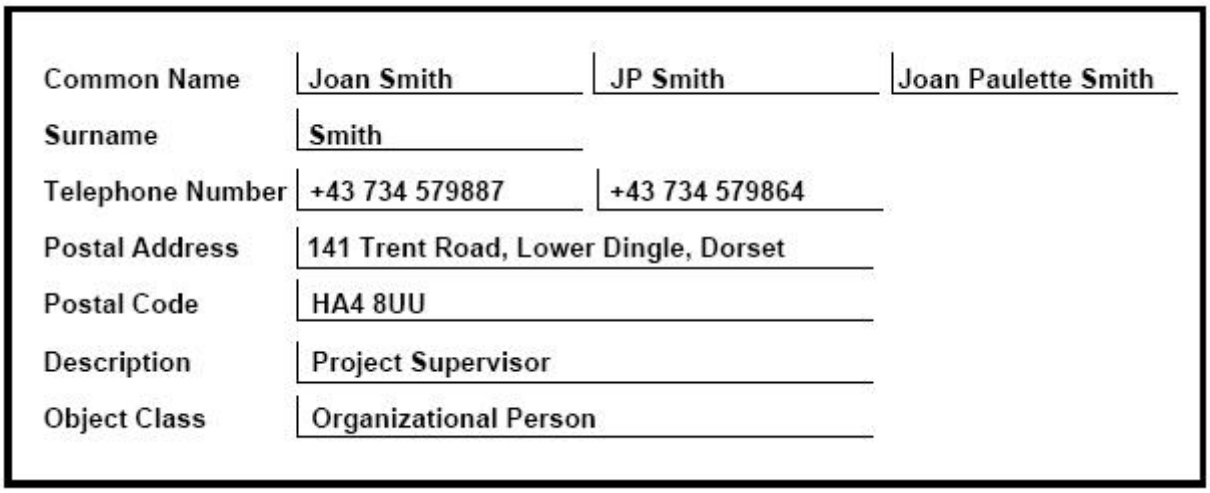

Figura 2: dn: cn=Joan Smith, dc=example, dc=com

Una entry consiste di un insieme di attributi, ogni attributo ha un nome (un attribute type o un attribute description) e uno o più valori. Ogni entry ha un identificatore unico: il Distinguished Name (**DN**) che consiste del Relative Distinguished Name (**RDN**), costituito da uno (o più di uno) degli attributi della entry, seguito dal DN della entry padre nella gerarchia. Il DN di una entry è costituito dalla concatenazione degli RDN delle entry che formano il percorso dalla root del DIT fino ad essa. Il DN è il nome della entry, non è né un attributo né parte della entry stessa. Nell'esempio in figura, "cn=Joan Smith" è lo RDN della entry, e "dc=example, dc=com" è il DN della entry padre, che in questo caso coincide con la root del DIT.

I nomi degli attributi sono tipicamente stringhe mnemoniche, come "cn" per common name, "dc" per domain component, "mail" per e-mail address.

Installazione e configurazione del server

La scelta del server LDAP da installare è caduta sull'**HP Enterprise Directory for eBusiness** V5.4-9, su piattaforma OpenVMS (Professional Workstation running OpenVMS Alpha V7.3-2), per la sua facilità di gestione e di installazione. Sulla stessa macchina è stato installato il software necessario come prerequisito per l'installazione del sistema (Multinet TCP/IP, DECnet Plus). L'HP Enterprise Directory implementa le versioni v2 e v3 di LDAP. E' gestito tramite due programmi richiamabili a linea di comando:

- **NCL** (Network Control Language) utilizzato per la gestione del server (stop/start, controllo delle connessioni)
- **DXIM** (HP X.500 Information Management) utilizzato per la gestione delle entry;

e comprende 2 componenti software:

- **DSA** (Directory System Agent) che si occupa di memorizzare le entry e gestire le connessioni;
- **DUA** (Directory User Agent) che è un client LDAP.

Una volta installato il server LDAP, sono state effettuare le operazioni necessarie alla sua configurazione:

- Esecuzione della utility di configurazione del DSA da un account con i privilegi *SYSPRV* e *OPER*:

```
$ @SYS$STARTUP:DXD$DSA_CONFIGURE
```

- Creazione del DSA e del naming context:

```
$ RUN SYS$SYSTEM:NCL
NCL> CREATE DSA
NCL> ENABLE DSA
NCL> CREATE DSA NAMING CONTEXT "dc=it/dc=cnr"
NCL>show dsa naming context * all attrib
Node 0 DSA Naming Context "/dc=it/dc=cnr"
at 2005-05-06-15:31:31.815+02:00Iinf
Identifiers
    Name                                = "/dc=it/dc=cnr"
NCL> EXIT
```

- Configurazione delle applicazioni di default:

```
$ @SYS$STARTUP:DXD$DUA_CONFIGURE.COM
```

- Creazione della entry relativa all'istituto:

```
$ dxim/interface=character_cell
   (C) Copyright 1992-2004 Hewlett-Packard Development Company,
   L.P.
   dxim> create /dc=IT/dc=CNR attri objectclass=domain
   dxim> show entry "/dc=it/dc=cnr"
       /dc=it/dc=cnr
```

```
        Domain Component = cnr
        Object Class   = domain
dxim> create /dc=IT/dc=CNR/dc=isti attri objectclass=domain
dxim> show entry /dc=it/dc=cnr/dc=isti
       /dc=it/dc=CNR/dc=isti
         Domain Component = isti
         Object Class   = domain
```

Definizione della struttura del DIT, estensione dello schema

Come si può notare nella creazione del naming context, nella strutturazione del DIT relativo al personale dell'ISTI, è stato scelto di utilizzare il meccanismo descritto nello RFC2247 (Using Domains in LDAP/X.500 Distinguished Names) che fornisce un automatismo per ottenere un DN per ogni domain name in Internet. Per cui la root è stata definita utilizzando l'attributo **dc** (domain component), in modo da avere **dc=isti, dc=cnr, dc=it**.

Per facilitare la ricerca, si è poi suddiviso il DIT in sottoalberi, corrispondenti ai diversi laboratori e aventi come figli le unità di personale. Quindi, subito "al di sotto" della root nella gerarchia, sono presenti le **ou** (organizational unit) relative ai laboratori, ad esempio:

```
dxim>  show entry /dc=it/dc=CNR/dc=isti/OU=RET
    /dc=it/dc=CNR/dc=isti/OU=RET
      Organizational Unit = RET
      Object Class   = OrganizationalUnit
      Description    = Network Systems and Internet Services
```

I contenuti delle entry nel DIT sono governati da uno **schema** che definisce il tipo degli attributi che le entry possono contenere. La definizione di un attributo include una sintassi: la maggior parte dei valori non-binari in LDAPv3 utilizza la sintassi di stringa UTF-8 (8-bit Unicode Transformation Format). Ad esempio, un attributo "mail" può contenere il valore user@example.com; un attributo "jpegPhoto" può contenere una o più fotografie in formato binario JPEG/JFIF. La definizione degli attributi specifica anche come fare le operazioni di search e di compare sull'attributo (se è case-sensitive e se è supportato il substring-matching), se l'attributo è single-valued o multi-valued, etc. Ogni entry deve avere almeno un attributo *objectClass* che descrive il tipo di oggetto rappresentato

dalla entry. Le **object class** sono definite all'interno dello schema e contengono l'elenco degli attributi che le entry possono o devono contenere, oltre ad altre informazioni di controllo.

Avendo come fonte dei dati il database del personale, è stato deciso a quali attributi far corrispondere i dati in esso presenti, escludendo quelli strettamente personali e non caricati nel DIT. Per la definizione dello schema, sono state utilizzate le object class standard: **domain** e **organizationalUnit**, rispettivamente per la definizione della root del DIT e delle unità organizzative corrispondenti ai laboratori. Per la definizione delle entry relative al personale è stata creata una object class personalizzata, estensione della classe standard InetOrgPerson.

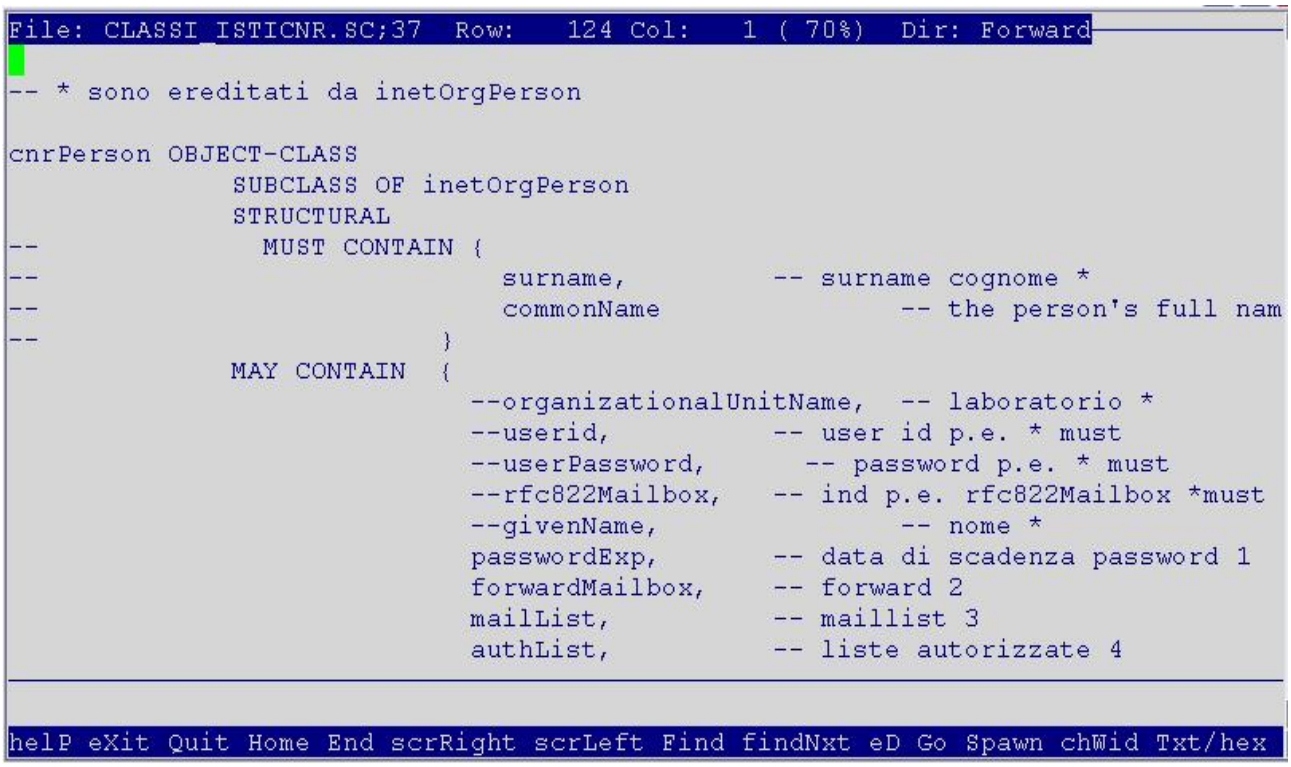

Figura 3: CLASSI_ISTICNR.SC, estensione dello schema per il personale dell'ISTI

Per estendere lo schema, e' stato necessario creare un file con estensione **.sc**, contenente la definizione dei nuovi attributi e della nuova object class, come mostrato in figura 3. Per rendere effettiva la modifica, il nome del file così creato è stato inserito nel file di configurazione **XP1000$DKB0:[DXD$SERVER]DXD$SCHEMA.SC** ed è stato ricompilato l'intero schema:

```
$ SET DEFAULT DXD$DIRECTORY
$ RUN SYS$SYSTEM:DXD$SCHEMA_COMPILER.EXE
```

Per mantenere il DIT aggiornato, e' stata scritta una procedura in DCL (Digital Command Language) che quotidianamente fa le operazioni di:

- interrogazione del database del personale e salvataggio in locale dei dati aggiornati
- aggiornamento del DIT

Nella figura successiva si vede un esempio di entry:

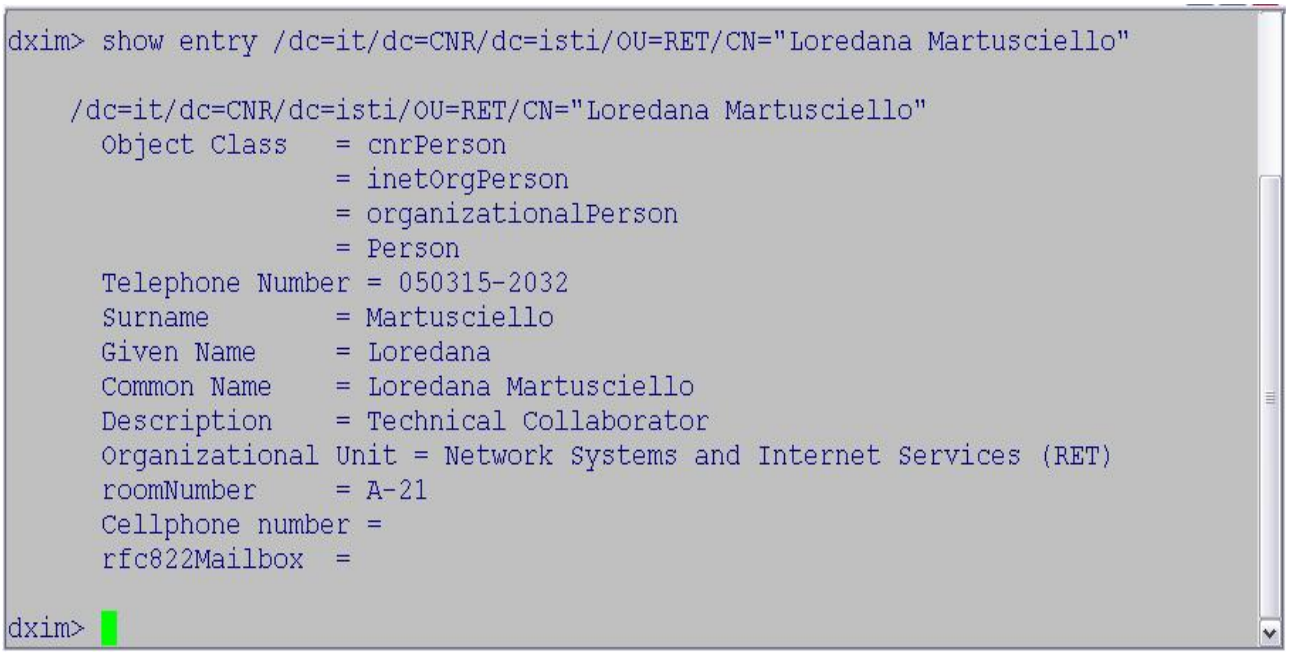

Figura 4: Interrogazione ed estrazione di una entry

Utilizzo da parte degli utenti

Un client inizia una sessione LDAP connettendosi ad un server LDAP, per default sulla porta 389, quindi inizia a inviare richieste di operazioni:

- Bind – autenticazione e specifica della versione del protocollo;
- Search – ricerca e recupero delle entry presenti nel DIT;
- Compare – verifica se un particolare attributo di una specifica entry (named entry) contiene un certo valore;
- Add – inserisce una nuova entry;
- Delete – cancella una entry;
- Modify – modifica una entry;
- Modify DN – muove o rinomina una entry;
- Unbind – chiude la connessione.

L'utilizzo più semplice del server LDAP da parte degli utenti è attraverso la rubrica di un client di posta elettronica. Praticamente tutti i più noti client consentono di accedere direttamente al DIT in

modo anonimo via protocollo LDAP, di visualizzare gli indirizzi di posta elettronica (e i valori degli attributi riconosciuti) e di selezionarli per l'invio dei messaggi.

Attualmente, il server **ldap.isti.cnr.it** può essere acceduto in questo modo da tutta la LAN dell'ISTI.

Allegato A

schema personalizzato CLASSI_ISTICNR.SC e file di configurazione DXD$SCHEMA.SC

```
--------------------- CLASSI_ISTICNR.SC ----------------------

-- new schema Enterprise Directory Isti-Cnr
--

cnrId    OBJECT-IDENTIFIER ::= {customerIntTelNumber 390503152111}
cnrAttributeType    OBJECT-IDENTIFIER ::= {cnrId 1}
cnrObjectClass      OBJECT-IDENTIFIER ::= {cnrId 2}
cnrNameForm         OBJECT-IDENTIFIER ::= {cnrId 3}

-- data di scadenza della password
-- da usare ATTRIBUTE-SYNTAX generalizedTimeSyntax
passwordExp       ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX stringSyntax (SIZE(1..25))
          EQUALITY MATCHING RULE caseIgnoreStringMatch
          ORDERING MATCHING RULE caseIgnoreStringMatch
          SUBSTRING MATCHING RULE caseIgnoreStringMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 1}

-- indirizzo di forward
forwardMailbox       ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX iA5StringSyntax (SIZE (1 .. 256))
          EQUALITY MATCHING RULE caseIgnoreIA5StringMatch
          SUBSTRING MATCHING RULE caseIgnoreIA5SubStringMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 2}

-- mailing list di appartenenza
mailList  ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX stringSyntax (SIZE(1..30))
          EQUALITY MATCHING RULE caseIgnoreStringMatch
          ORDERING MATCHING RULE caseIgnoreStringMatch
          SUBSTRING MATCHING RULE caseIgnoreSubstringMatch
          APPROXIMATE MATCHING RULE initialWordApproximateMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 3}

--
authList  ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX stringSyntax (SIZE(1..30))
          EQUALITY MATCHING RULE caseIgnoreStringMatch
          ORDERING MATCHING RULE caseIgnoreStringMatch
          SUBSTRING MATCHING RULE caseIgnoreSubstringMatch
          APPROXIMATE MATCHING RULE initialWordApproximateMatch
```

```
          STORE NORMALIZED
          :: = {cnrAttributeType 4}

-- dominio di appartenenza (per casella postale)
nameDomain    ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX stringSyntax (SIZE(1..30))
          EQUALITY MATCHING RULE caseIgnoreStringMatch
          ORDERING MATCHING RULE caseIgnoreStringMatch
          SUBSTRING MATCHING RULE caseIgnoreSubstringMatch
          APPROXIMATE MATCHING RULE initialWordApproximateMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 5}

-- user home page
homeURL       ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX stringSyntax (SIZE(1..80))
          EQUALITY MATCHING RULE caseIgnoreStringMatch
          ORDERING MATCHING RULE caseIgnoreStringMatch
          SUBSTRING MATCHING RULE caseIgnoreStringMatch
          APPROXIMATE MATCHING RULE initialWordApproximateMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 6}


-- web personale
personalURL       ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX stringSyntax (SIZE(1..80))
          EQUALITY MATCHING RULE caseIgnoreStringMatch
          ORDERING MATCHING RULE caseIgnoreStringMatch
          SUBSTRING MATCHING RULE caseIgnoreStringMatch
          APPROXIMATE MATCHING RULE initialWordApproximateMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 7}

-- numero interno
intPhone       ATTRIBUTE
          WITH ATTRIBUTE-SYNTAX telephoneNumberSyntax (SIZE(1..5))
          EQUALITY MATCHING RULE telephoneNumberMatch
          ORDERING MATCHING RULE telephoneNumberMatch
          SUBSTRING MATCHING RULE telephoneNumberSubstringMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 8}

-- Groups that person/object is a member of
memberOf       ATTRIBUTE
          WITH  ATTRIBUTE-SYNTAX distinguishedNameSyntax
          EQUALITY MATCHING RULE distinguishedNameMatch
          STORE NORMALIZED
          :: = {cnrAttributeType 9}

LABEL homeURL
      KEYWORD "URL"
```

```
      MENU "URL"
      DESCRIPTION "Personal web page"
END


LABEL mobileTelephoneNumber
      KEYWORD "cellphone", "mobile"
      MENU "cellphone"
      DESCRIPTION "Cellphone number"
END


cnrPersonNameForm NAME-FORM
          NAMES cnrPerson
--         WITH ATTRIBUTES userid
         WITH ATTRIBUTES commonName  --
          AND OPTIONALLY organizationalUnitName
          ::= {cnrNameForm 1}

cnrPersonStructureRule STRUCTURE-RULE
          NAME FORM cnrPersonNameForm
          SUPERIOR RULES
        localityStructureRule, localityRootStructureRule,
        stateOrProvinceStructureRule,
stateOrProvinceRootStructureRule,
        organizationStructureRule, organizationRootStructureRule,
        organizationalUnitStructureRule
          ::= 10001

-- * da inetOrgPerson

cnrPerson OBJECT-CLASS SUBCLASS OF inetOrgPerson STRUCTURAL
--            MUST CONTAIN {
--                           surname,     -- surname cognome *
--                           commonName   -- the person's full
name *
--                         }
              MAY CONTAIN  {
                           --organizationalUnitName,  -- lab *
                           --userid,        -- user id p.e. *
                           --userPassword,  -- password p.e. *
                           --rfc822Mailbox, -- ind p.e.
rfc822Mailbox *must
                           --givenName,     -- nome *
                           passwordExp,     -- scadenza pssw 1
                           forwardMailbox,  -- forward 2
                           mailList,        -- maillist 3
                           authList,        -- liste author. 4
                           nameDomain,      -- dominio p.e. 5
                           --description,   -- tipo di incarico *
                           --roomNumber,    -- numero stanza *
                           --title,         -- personalTitle" *
```

```
                    --telephoneNumber,  -- telefono uff. *
                    --mobileTelephoneNumber,    -- cell *
                    --facsimileTelephoneNumber, -- FAX *
                    homeURL,        -- web lavoro 6
                    personalURL,    -- web personale 7
                    --owner,        --
                    --userCertificate,      -- *
                    --userSMIMECertificate, -- *
                    --seeAlso,    -- Reference to another
                            -- related entry in the DIT *
                    intPhone         -- tel interno
                   }
::= {cnrObjectClass 1}
```

```
----------------------     DXD$SCHEMA.SC     ----------------------

-- Title dxd_schema.sc
-- Ident = V5.4-9
--
--%COPYRIGHT_START%
--
-- Copyright 2003 Hewlett-Packard Development Company, L.P.
--
-- Confidential computer software. Valid license from HP and/or
its
-- subsidiaries required for possession, use, or copying.
--
-- Consistent with FAR 12.211 and 12.212, Commercial Computer
Software,
-- Computer Software Documentation, and Technical Data for
Commercial
-- Items are licensed to the U.S. Government under vendor's
standard
-- commercial license.
--
-- Neither HP nor any of its subsidiaries shall be liable for
technical
-- or editorial errors or omissions contained herein. The
information in
-- this document is provided "as is" without warranty of any kind
and is
-- subject to change without notice. The warranties for HP
products are
-- set forth in the express limited warranty statements
accompanying
-- such products. Nothing herein should be construed as
constituting an
-- additional warranty.
--
--%COPYRIGHT_END%
--
-- FACILITY:
--      HP Enterprise Directory
--
-- ABSTRACT:
--      This file defines the Directory Schema. It is compiled by
--      the schema compiler into a binary file which is read by
the
--      DSA at creation time, and by Compaq DUAs.
--
--      This file simply includes each of the separate schema
modules in order.
--      Applications or users wishing to extend the schema should
do so by
--      creating a new module and INCLUDE'ing it from this module.
--
```

```
INCLUDE "dec.sc"
INCLUDE "x500.sc"
INCLUDE "x400.sc"
INCLUDE "mts.sc"
INCLUDE "dit.sc"
INCLUDE "cosine.sc"
INCLUDE "quipu.sc"
INCLUDE "dua.sc"
INCLUDE "ids.sc"
INCLUDE "entrust.sc"
INCLUDE "inet.sc"
INCLUDE "account.sc"
INCLUDE "classi_isticnr.sc"
```