Concetti di base

Authentication

Authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product.

For a positive identification, elements from at least two, and preferably all three following factors must be verified:

- the **ownership factors**: Something the user **has** (e.g., wrist band, ID card, security token, software token, cell phone..)
- the **knowledge factors**: Something the user **knows** (e.g., a password,pass phrase, or personal identification number (PIN), challenge response (the user must answer a question)
- the **inherence factors**: Something the user **is** or **does** (e.g., fingerprint, retinal pattern, DNA sequence , face, voice, biometric identifier).

Authorization

- **Authorization** is the function of specifying access rights to resources. It is related to access control. More formally, "to authorize" is to define access policy.

- Authorizzation Methods:

  DAC (Discretional Access Control)

  MAC(Mandatory Access Control)

  RBAC (Role Based Access Control)

Identity Management & Directories

- **Identity** : set of attributes which represent a person in a computer system.

- **Identity repository :** system able to store and make available the identities. It provides tools, API, protocols to create and search the identities, to modify their attibutes, to realize relations among them and to define rules to control these relations.

- **Directory.** Identity repository in which the access is defined by the protocol **DAP(Direct Access Protocol)**

Directory Service and data-base:differences

. The accesses to the directory are almost always for reading information. Writing operations are limited to the system administrators and to single informations owners.

• The directory is not suitable to store frquently modified informations.

•Client-server model. The client calls a function (API) which produces a message for the server.

• The format and the content of the exchanged messages are based on the LDAP protocol

- **LDAP** (Lightweight Directory Access Protocol)

- Standard protocol for directory services.

- Simplified version of the standard DAP(Directory Access Protocol) (X.500 (CCITT)).

- **DSML** (Directory Service Mark-up Language).
XML access to LDAP directory

LDAP directory

- A directory is a tree of directory entries.
- An entry consists of a set of attributes.
- An attribute has a name (an *attribute type* or *attribute description*) and one or more values.
- Each entry has a unique identifier: its *Distinguished Name* (DN).
- he more common types of entities are
- **User**
- **Group**
- **Organizational Unit**
- **Organization**
- **Domain Context**

• Some objects have the role of containers, as Domain Context (DC), Organizational Unit (OU) and Organization (O); the others have a Common Name.

•The directory has a tree **organization**, realized through container objects. The name of these objects realizes the **distinguished name**, that is the acces key to the directory objects.

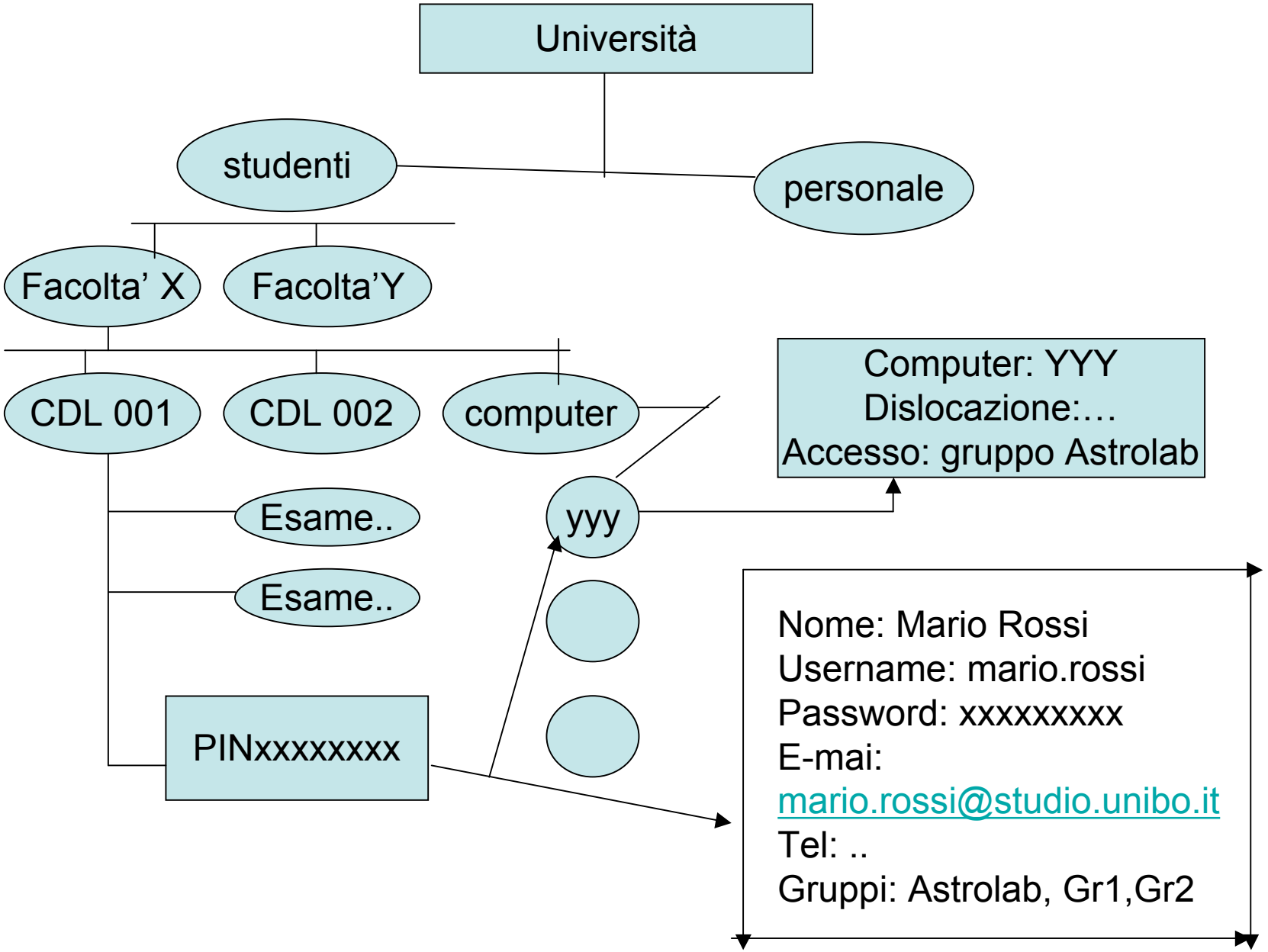
•For instance:
CN=Paolo Rossi, OU=Vendite, O=Fiat

• In a complex organization, the DS contains all the informations relative to the infrastructure and to its resources, to the people belonging to the different areas and to the users.

•For the people it’s important to provide personal data, e-mail, tel. num, fax,etc..,and their belonging to a specific sector of the organizations

I numeri del DSA

- 4266 personale docente e ricercatore
- 6531 docenti a contratto
- 3856 personale tecnico amministrativo
- 8264 dottorandi
- 5603 ospiti e collaboratori
- 316395 studenti
- 12111 gruppi sicurezza profilazione applicativa
- 1719 unità organizzative e sedi servizio


Università
studenti
personale
Facolta' X
Facolta'Y
CDL 001
CDL 002
computer
Esame..
Esame..
PINxxxxxxxx
yyy
Computer: YYY
Dislocazione:…
Accesso: gruppo Astrolab
Nome: Mario Rossi
Username: mario.rossi
Password: xxxxxxxxx
E-mai:
mario.rossi@studio.unibo.it
Tel: ..
Gruppi: Astrolab, Gr1,Gr2

Security

•The user **authentication and authorization** service is **centralized**

• It allows an access to resources based on the individual role and on the relative access right.

• All the applications based on the DS take advantage of the same authentication system, independently from users localization . Users can be connected on a local network or they can utilize a web application trough Internet

•The DS can be utilized also by external applications if the users are inserted in the DS.

•The external applications interrogate the DS la directory (web services) to know if the personal data inserted by the client are present in the DS.

• Example: students that intend to use an external library.

Active Directory: Microsoft
Lotus Notes: IBM
i-Planet: Sun
Directory service: Nowell
……

Single Sign On (SSO)

• Organizations today need to manage access not only to their own systems but also systems that belong to external partners or other division.

•Employes and customers struggler to access the information they need. The must visit multiple web sites, loggin in each time and are forced to maintain multiple user names and passwords.

•Meanwhile, the organization looses control over its users' identity information. Having this information managed by others at external organizations increase security risks, such as the risk of unauthorized access or identity theft. It also create administrative ovehead and redundancies.

• It also create administrative overhead and redundancies. For example, you must deal with the costs and hassies of getting your partner to update their systems every time there is a change to your users' identity information.

•When the users' identity information must be maintained by many external partners, it is inevitable that some of this information will became innacurate. For example, the access rights of terminated employees may remain active at certain partner sites, allowing them to alter data after their employment has ended.

•It is difficult to implement applications which share and/or aggregate dervices provided by different sites.

- SSO: only one user authentication.

- others authentication requests to access different resources are provided by the software in an invisible way for the user.

CAS (Central Authentication Service)

- The Central Authentication Service (CAS) is a single sign on protocol for the web. Its purpose is to permit a user to access multiple applications while providing their credentials (such as userid and password) only once. It also allows web applications to authenticate users without gaining access to a user's security credentials, such as a password.
- The name *CAS* also refers to a software package that implements this protocol.)
- This kind of architecture is mainly utilized for the access to services belonging to the same organization.

- Three components:

    - Client web browser

    - web application requesting authentication,

    - CAS server

- .When the client visits an application desiring to authenticate to it, the application redirects it to CAS. CAS validates the client's authenticity, usually by checking a username and password against a database (such as Kerberos or Active Directory)

- If the authentication succeeds, CAS returns the client to the application, passing along a security ticket. The application then validates the ticket by contacting CAS over a secure connection and providing its own service identifier and the ticket.

- CAS then gives the application trusted information about whether a particular user has successfully authenticated

Federated Identity management

Organizations today need to manage access not only to their own systems but also systems that belong to external partners or other division.

• Example:
  - Outsourcer service provider
  - Supply chain partners
  - Cross selling services
  - Co-developing products ….

• Objective; to enable individuals to interact with various service providers or web sites with trust relationships by signing in just once

Exampleempio.

• Fabrikam: bicycle manufacturer.

•web application which will allow authorized dealers to purchase bikes and part at wholesale prices.

•200 dealers , each with several people who need to use the application.

Objective

To realize a secure logon mechanism.

Solution

Centralized data base containing user names and passwords of all people enabled to access.

Problems

- Fabrikam , before to provide a user account must to contact someone they trust at the dealership to verify the employee's status.
- Maintenance cost of such a user account: people forget user names, passwords.
- Deprovisioning. What happens when the emploee is terminated from the dealership?
- As computing power has increased, passwords have become easier and easier to attack and many organizations now prefer to use stronger authentication techniques like smart cards..
- But because Fabrikam must work with so many different dealerships, it's going to have a difficult time supporting anything stronger than passwords.

Why build a user account database for the application when each dealerships already have software that authenticate their users ?

• each partner belonging to the federation authenticates its users by utilising the own authentication system.

• The access to one of the federated systems automatically enable the access to all the others

•Each partner **trusts the other partners to authenticate its own users.**
“The user is OK; he can utilize this application”

• L’accesso al server avviene **senza dover specificare la propria identità**.

• Le password **rimangono locali** al sistema di autenticazione cui fa capo l’utente.

• Trust tra i due siti. I due siti devono essere sicuri che gli attributi vengano rilasciati al sito deciso.

.

Scambio di messaggi utilizzando un protocollo standard
(SAML- Security Assertion Markup Language)

SAML Assertions:

1. Authentication statements
2. Attribute statements
3. Authorization statements

Active Directory Federation Services (ADFS)

- Un impiegato A di un dealer B tenta di accedere al sito di Fabricam.
- Il web agent si accorge che la richiesta non è accompagnata da un ticket (ADFS cookie)
- Il **web agent ridirige** il browser di A al servizio di federazione di Fabrikam senza che l'applicazione veda la richiesta .
- Il servizio di federazione di Fabrikam ridirige il browser al servizio di federazione del dealer con un identificatore di Fabrikam in modo che il dealer sappia **quale servizio** è richiesto.

• Il servizio di federazione del dealer chiede il logon di A e definisce un token usando SAML che descrive A.

• Il dealer ha un sistema di **Identity Provisioning** per tutti i suoi impiegati (appartenenza dell'impiegato al dealer, il suo ruolo attuale se ha diritto o no di fare l'acquisto)

• Fabrikam legge il contenuto del token ed invia un token SAML che contiene l'insieme delle richieste che l'applicazione vede.

• Questo token è un **cookie** che consente ad A di usare l'applicazione fino al termine di validità del token (default 10 ore)

Liberty Alliance

- 150 organizzazioni: AOL,Intel, novell,Oracle, Sun,….
- ID-FF 1.0 e 2.0
- OASIS(**Organization for the Advancement of Structured Information Standards)** : SAML standard