

Identity Management

Alberto Pace

CERN, Information Technology Department

alberto.pace@cern.ch



- The present of computer security
 - Bugs, Vulnerabilities, Known exploits, Patches
 - Desktop Management tools, anti-virus, anti-spam, firewalls, proxies, Demilitarized zones, Network access protection, ...
- No longer enough. Two additional aspects:
 - Social Engineering / Human factor
 - Require corporate training plan, understand the human factor and ensure that personal motivation and productivity is preserved
 - Identity (and Access) Management

Discussed now



- Identity Management (IM)
 - Set of flows and information which are (legally) sufficient and allow to identify the persons who have access to an information system
 - This includes
 - All data on the persons
 - All workflows, processes and procedures to Create/Read/Update/Delete records of persons, accounts, groups, organizational unit, ...
 - All tools used for this purpose

Internet
Services

- Identity and Access Management (IAM)
- Access Management
 - The information describing what end-user can do on the corporate computing resources. It is the association of a *right* (use, read, modify, delete, open, execute, ...), a *subject* (person, account, computer, group, ...) and a *resource* (file, computer, printer, room, information system, ...)
 - The association can be time-dependent, or location-dependent
 - Resources can be physical (room, a door, a terminal, ...) or a computing resource (an application, a table in a database, a file, ...)

Internet
Services



- The **AAA** Rule. Three components, *independent*
- **A**uthentication
 - Unequivocal identification of the person who is trying to connect.
 - Several technologies exist with various security levels (username / password, certificate, token, smartcard + pin code, biometry, ...)
- **A**uthorization
 - Verification that the connected user has the permission to access a given resource
 - On small system there is often the confusion between authorization and authentication
- **A**ccounting
 - List of actions (who, when, what, where) that enables traceability of all changes and transactions rollback



Internet
Services

- Role Based Access Control (RBAC)
 - Grant permissions (authorizations) to groups instead of person
 - Manage authorizations by defining membership to groups
- Separations of functions
 - granting permissions to groups (Role creation)
 - group membership management (Role assignment)
- RBAC should remain a simplification
 - Keep the number of roles to a minimum

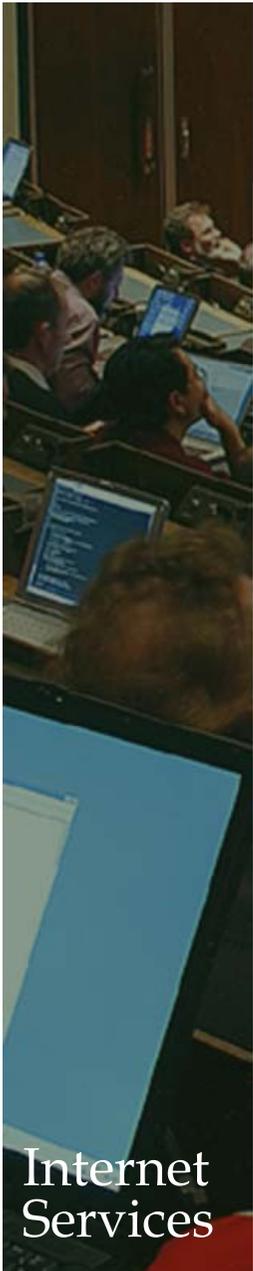


- Legal obligation
 - In many areas traceability is required
 - Sarbanes Oxley Act (SOX) in the US
 - 8th EU Privacy Directive + national laws in Europe
- Cost reduction
 - Reduce multiple authentication mechanism to a single one.
 - Offload qualified staff from administrative tasks (user registration, password changes, granting permissions, ...)
- Increased Security
 - Simplification of procedures, increased opportunity
 - Centralized global overview of authorizations / accounting



Internet
Services

- Laws are different in each country
- Laws depend on the type of institute
 - Public funded, Government, Privately owned, International Organization, ...
- Laws depend on the sector of activity
 - Archiving, traceability, retention of log files and evidences
- Not easy to find the good compromise between security / accounting / traceability and respect of privacy / personal life



Internet
Services

- Overall strategy
 - Be realistic. Base the project on “short” iterations (4 - 8 weeks) with clear objectives and concrete results at each iteration
 - Understand the perimeter of the project.
 - Services included / excluded
 - One single project cannot fix all existing and cumulated projects
 - Understand the stakeholders
 - Who is affected
 - Who pays
 - Ensure to have management support
 - Inventory, simplify, streamline and document all administrative procedures
- It is an heavy project, there are many parameters

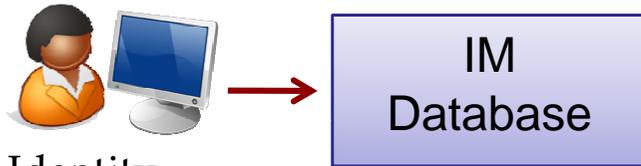


Internet
Services

- The Identity Management Database
 - (web) application for person and account registration, used by the administration to create identities
 - Multiple workflows and information validation depending on the type of data:
 - Example: last name, passport info modifications require a workflow with validation/approval by the administration.
 - Example: password change, change of preferred language is available in self service to end-user
- The *public* part of the database must be *accessible*
 - Directories, LDAP, ...



Internet
Services

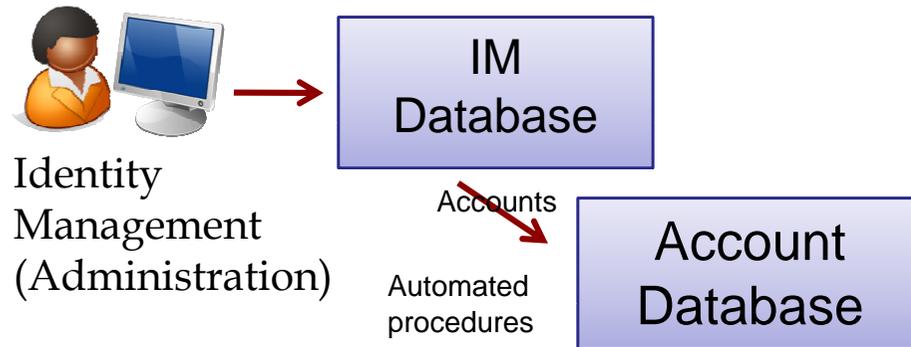


Identity
Management
(Administration)

- Automate account creation
 - What are the “administrative” requirements to be “known” to the information system
 - Do not confuse with: “authorized” to use service “xyz”
 - “administrative” means that you have all information in the IAM database, you can define rules, you can implement a workflow.
- If you can’t answer this question, you can’t automate
 - Putting an administrative person to “manually handle” the answer to that question won’t solve the problem in large organizations



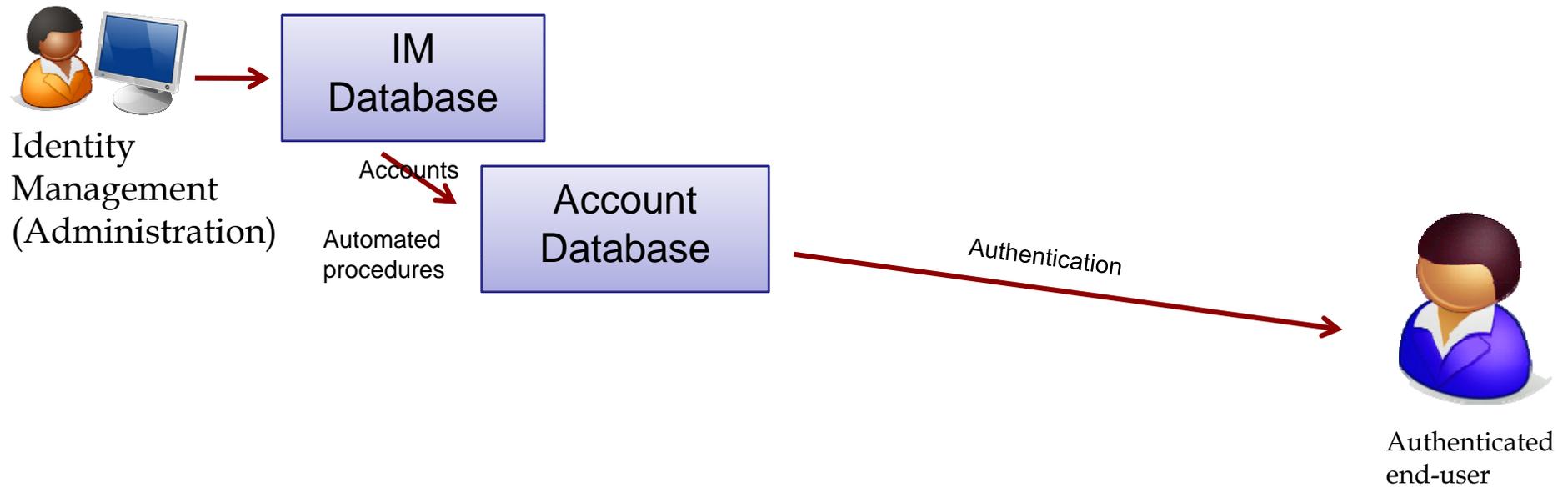
Internet
Services



- **A**uthentication Service
 - You can have multiple technologies (Kerberos, PKI, Biometry, ...), and multiple instances of the same technology, all generated from the same IM database
- Ideally: Single-Sign-On (SSO) services
 - Authentication portal for web-based applications
 - Kerberos services for Windows and/or AFS users
 - Certification authority for grid users
 - aware of group memberships (described later)

Internet
Services

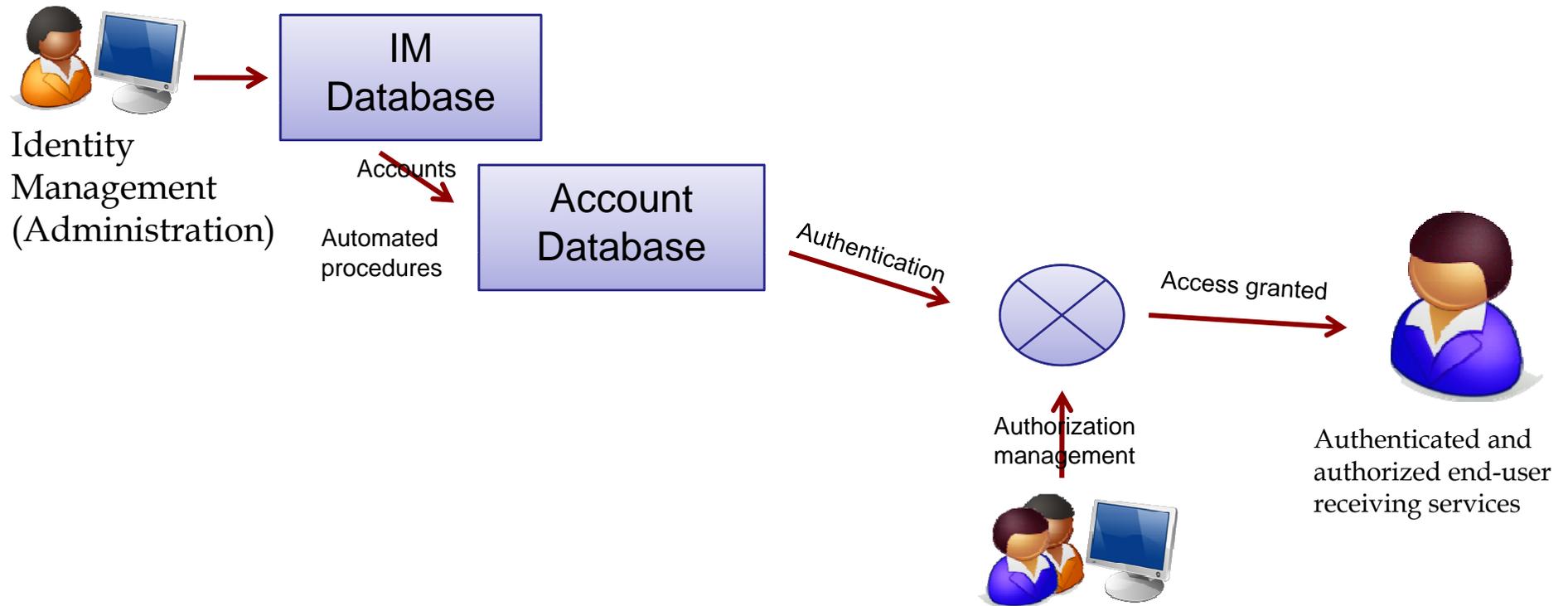




- Service-specific interfaces to manage **A**uthorizations
 - This is typically platform and service dependent
 - Allows assignment of permissions to groups or accounts or persons
 - Authorization can be made once to a specific group and managed using group membership

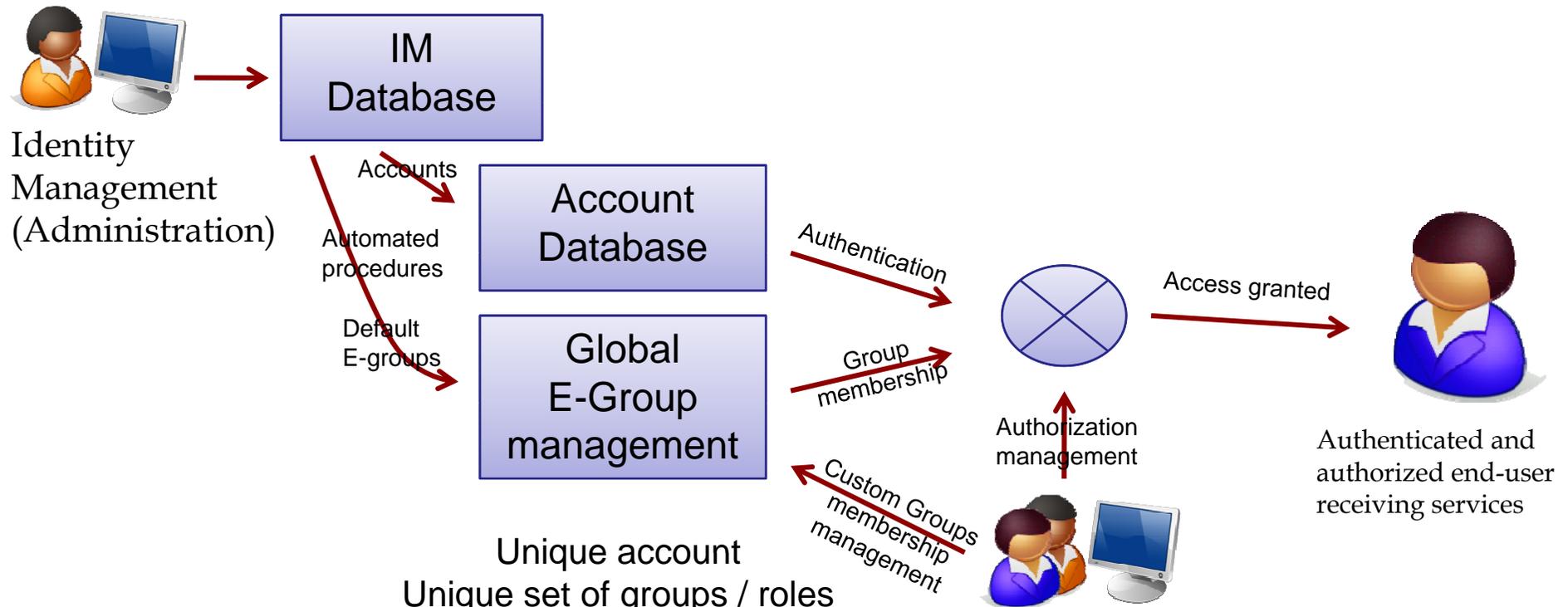


Internet
Services



- E-Group management (RBAC)
 - Indirect way to manage authorizations
 - (web) application to manage group memberships
 - Must foresee groups with manually managed memberships and groups with membership generated from arbitrary SQL queries in the IAM database
 - Must support nesting of groups





Unique account
 Unique set of groups / roles
 (for all services)

- Resource owner or Service manager
 Authorizes using
- User Accounts
 - Default E-groups
 - Custom E-groups

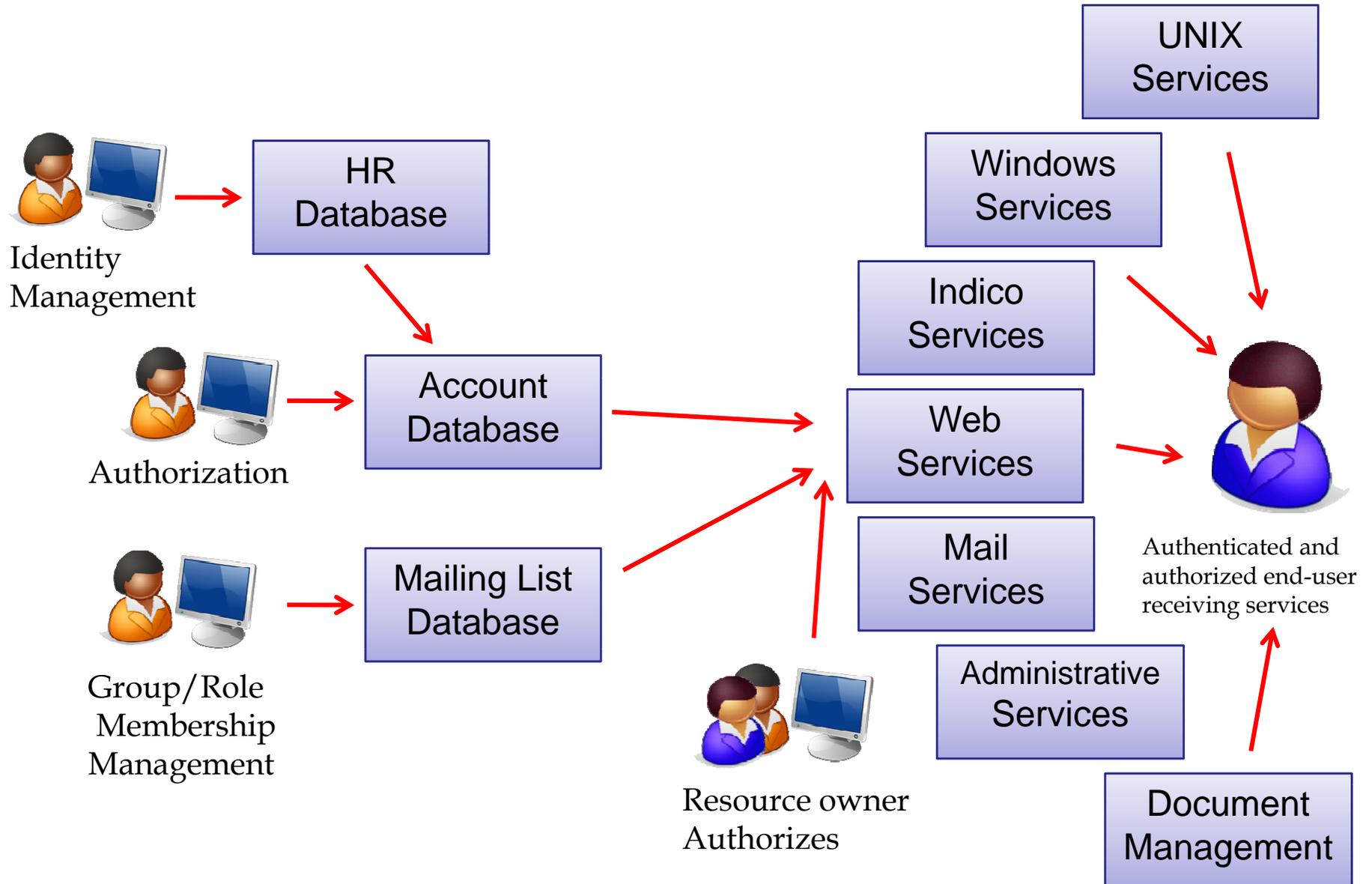
- **A**ccounting
 - Entirely service specific
 - What you account is the result of your “risk analysis” for that service to understand how far you may want to rollback your transactions.
 - Good accounting have large cost (eg: backups, archiving)
 - Not discussed further

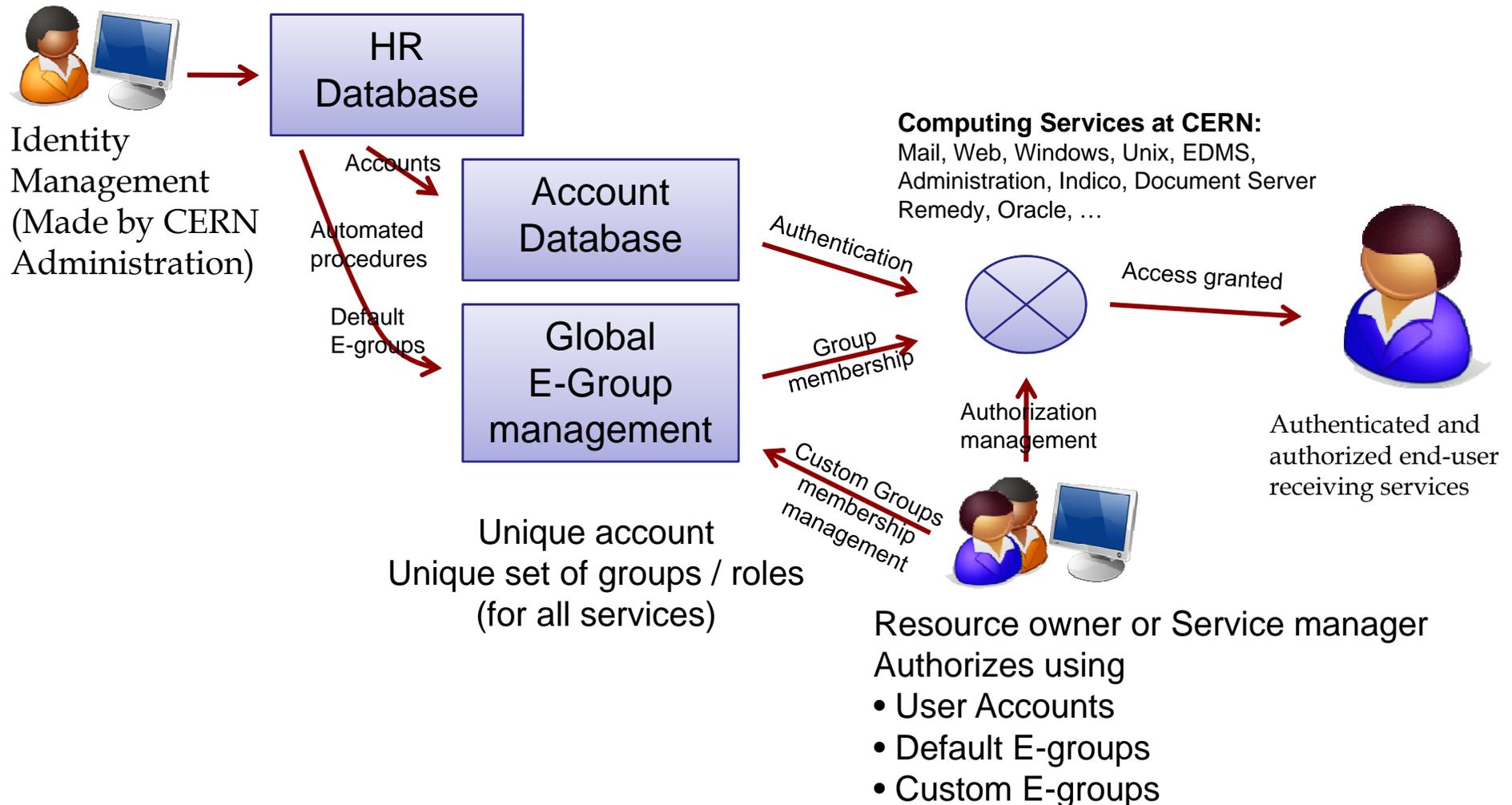


- CERN has an HR database with many records (persons)
- 23 possible status
 - Staff, fellow, student, associate, enterprise, external, ...
- Heavy rules and procedures to create accounts
 - Multiple accounts across multiple services
 - Mail, Web, Windows, Unix, EDMS, Administration, Indico, Document Server, Remedy, Landb, Oracle, ...
 - Multiple accounts per person
 - Being migrated towards a unique identity management system with one unique “CERN account”, valid for all services



Internet
Services





- Central account management
- Only one account across services
 - synchronize UNIX and Windows accounts
- Multiple login-id per person possible but many services will accept only the “*primary*” one
- Use Groups for defining access control to resources
 - No more: “close Windows Account, keep Mail account, block UNIX account”
 - But: “block Windows access, allow Mail access, block AIS access”.

Internet
Services





Username / Password

SSO using Windows Credentials

SSO using Grid Certificate

Do it yourself demo:

- Open a Windows hosted site:
 - <https://cern.ch/win>
 - Click login, check user information
- Open a Linux hosted site:
 - <https://shib.cern.ch>
 - Check various pages
- Go back to first site
 - Click logout
 - go back to the second site

The screenshot shows a Windows Explorer window with a folder named 'Review'. The 'Sharing and Security...' context menu option is selected. The 'Review Meeting Properties' dialog box is open, showing the 'Security' tab. The 'Group or user names' list contains four entries: 'denise (Denise.Heagerty@cern.ch)', 'pace (Alberto.Pace@cern.ch)', 'it-dep-is-members@cern.ch (CERN\it-dep-is)', and 'info-rot-a-is-members@cern.ch (CERN\info-rot-a-is)'. The 'Permissions' table below shows various permissions with 'Allow' and 'Deny' checkboxes.

| Permissions | Allow | Deny |
|----------------------|--------------------------|--------------------------|
| Full Control | <input type="checkbox"/> | <input type="checkbox"/> |
| Modify | <input type="checkbox"/> | <input type="checkbox"/> |
| Read & Execute | <input type="checkbox"/> | <input type="checkbox"/> |
| List Folder Contents | <input type="checkbox"/> | <input type="checkbox"/> |
| Read | <input type="checkbox"/> | <input type="checkbox"/> |
| Write | <input type="checkbox"/> | <input type="checkbox"/> |
| Social Permissions | <input type="checkbox"/> | <input type="checkbox"/> |

Annotations in blue boxes with red arrows pointing to the dialog box:

- Predefined persons from central identity management (ALL persons are pre-defined)**: Points to the first three entries in the 'Group or user names' list.
- Predefined Group (role) from central identity management (several roles are pre-defined)**: Points to the 'it-dep-is-members@cern.ch' entry.
- Custom Group managed by the resource owner**: Points to the 'info-rot-a-is-members@cern.ch' entry.

The image displays two screenshots of the SIMBA++ User interface, a web-based tool for managing mailing lists. The left screenshot shows the search results page, and the right screenshot shows the configuration page for a specific list.

Left Screenshot: Search Results

Search for a list whose...

List Name: begins with [] Descr

Owner: equals [] Mem

[Search] [Clear Form] [Only li

Good Morning!.. Alberto you are c

Showing the list(s) 1-15 of 15 total ma

| Mail | Description |
|---|---|
| [Edit] desktop-services-technical-meeting@cern.ch | Mailing list for Desktop Services Technical Meeting |
| [Edit] info-rotas@cern.ch | Weekly 3rd level rota information |
| [Edit] it-dep-is@cern.ch | Members of the group IT/IS |
| [Edit] it-dep-is-ds@cern.ch | IT/IS/DS section -includes non-sta |
| [Edit] it-dep-is-ds-staff@cern.ch | IT-IS-DS section staff only |
| [Edit] it-dep-is-mgmt@cern.ch | IT/IS Group Management |

Right Screenshot: List Configuration

List Configuration

- Last Modified: 5/8/2007 8:06:42 AM

Pace Alberto - IT/IS <Alberto.Pace@cern.ch>

- Owners

[Add Owner] [Delete Owner]

Boissat Christian - IT/IS <Christian.Boissat@cern.ch>
 Chorier Julien - Other <julien.chorier@cern.ch>
 Copy Cedric - IT/IS <cedric.copy@cern.ch>
 Dellabella Sebastien - IT/IS <Sebastien.Dellabella@cern.ch>
 Deloose Ivan - IT/IS <Ivan.Deloose@cern.ch>
 Gaspar Aparicio Ruben Domingo - IT/DES <Ruben.Gaspar.Aparicio@cern.ch>
 Hanine Michael - IT/EXT <Michael.Hanine@cern.ch>
 Isnard Christian - IT/IS <Christian.Isnard@cern.ch>
 Joubert Jean Franck - IT/UDS <Franck.Joubert@cern.ch>
 Kwiatek Michal - IT/IS <Michal.Kwiatek@cern.ch>
 Lossent Alexandre - IT/IS <Alexandre.Lossent@cern.ch>
 Mamouzi Djilali - IT/IS <Djilali.Mamouzi@cern.ch>
 Montuelle Jean - IT/IS <Jean.Montuelle@cern.ch>
 Nordal Audun Ostrem - IT/IS <Audun.Ostrem.Nordal@cern.ch>
 Olin Pascal - IT/EXT <Pascal.Olin@cern.ch>
 Ormancey Emmanuel - IT/IS <Emmanuel.Ormancey@cern.ch>
 Otto Rafal - IT/IS <Rafal.Otto@cern.ch>
 Pace Alberto - IT/IS <Alberto.Pace@cern.ch>
 Schwarzbauer Hannes - IT/DI <Hannes.Schwarzbauer@cern.ch>
 Suick Juraj - IT/IS <Juraj.Suick@cern.ch>

- Members

There are 23 members.

[Find]

- Description

Weekly 3rd level rota information

- List Type

Normal List HR List External List

- Alias

[]@cern.ch

- Maximum Message Size

default (KB)

[Add Member] [Delete Member] [Bulk Operations]

Errors to avoid

- Legal
- Organizational Factors
 - Lack of management support, of project management / leadership
 - No clear and up to date communication
 - Inform user of constraints and benefits
 - RBAC with too many roles
- Technical
 - Incorrect estimation of quality of existing data
 - Implement an exception on each new demand
 - Lost mastering of technical solutions



Internet
Services



- Global identity management a requirement for HEP computing and Grid activities through the “International Grid Trust Federation” (www.gridpma.org)
- Coordination is done through the regional Policy Management Authorities
 - Asia Pacific Grid PMA
 - European Grid PMA
 - The Americas Grid PMA
- CERN efforts in identity management integrate *directly* in the global grid services



Internet
Services

- The CERN Certification Authority is online and part to the CERN Identity management
 - <http://cern.ch/ca>
- Identity validation is done using the SSO service (which also recognizes grid certificates)
- Offers grid certificates to authorized users
- Recognizes gridpma certificates and allows mapping to the CERN accounts



The screenshot displays the CERN Certification Authority web interface with the following sections:

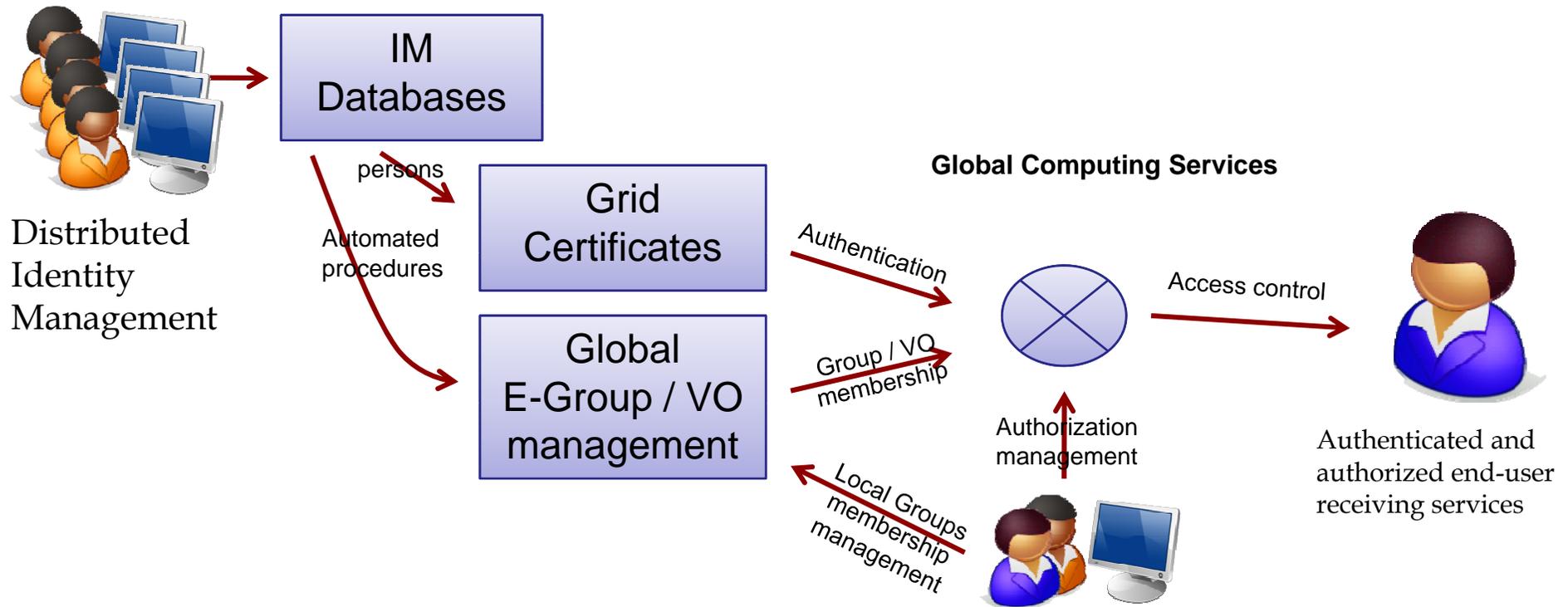
- Manage user certificates**
 - Request user certificate using Internet Explorer
 - Request user certificate using Mozilla browser
 - Request user certificate manually
 - Renew user certificate (Internet Explorer only)
 - Renew user certificate manually
- List and revoke certificates**
 - List and revoke certificates
- Trust CERN Certification authority**

On a CERN Domain managed Windows machine, the CERN Root Certificate is trusted, so any CERN Certificate will be verified correctly, no specific action is required.
On any other platform, the CERN Root Certificate needs to be trusted manually to allow CERN Certificate verification. To do this, install the Root Certificate using one of the following methods.

 - Install Root certificate using Internet Explorer
 - Install Root certificate using Mozilla browser
 - Install Root certificate using Safari browser
- Download CA certificates and CRLs [Help]**
 - CERN Root CA certificate
 - CERN Root CA CRL
 - CERN Trusted Certification Authority certificate
 - CERN Trusted Certification Authority CRL
- Certificate mappings**
 - Map an existing Certificate to your account
- Host Certificates**
 - Manage Host Certificates



Internet
Services



Resource owner or Service manager
Authorizes using

- User Accounts (Certificate Subjects)
- VO or local E-groups

- Identity Management is a strategy to simplify complex computing infrastructures and is an essential component of a secure computing environment
- Security in focus
 - Complexity and security don't go together
- Cost reduction available as a side benefit
- Necessary to resist to pressure of having
 - “Custom” solution for “special” users
 - Exception lists

