Identity Management

Alberto Pace
CERN, Information Technology Department
alberto.pace@cern.ch

Computer Security

- The present of computer security
  - Bugs, Vulnerabilities, Known exploits, Patches
  - Desktop Management tools, anti-virus, anti-spam, firewalls, proxies, Demilitarized zones, Network access protection, …
- This is no longer enough. Two additional aspects
  - Social Engineering
    - “Please tell me your password”
    - Require corporate training plan, understand the human factor and ensure that personal motivation and productivity is preserved
  - Identity (and Access) Management

Discussed now

Definition

- 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 to Create/Read/Update/Delete records of persons, accounts, groups, organizational unit, …
    - All internal processes and procedures
    - All tools used for this purpose

More definitions

- Identity and Access Management (IAM)
- Access Management
  - For a given information system, the association of a right (use / read / modify / delete / …), an entity (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, …)

Typical misunderstandings

- Identity management
  - The LDAP directory of users with password hashes
  - The password expiration policy
- Access management
  - Web site to centrally manage group memberships or permissions

IAM Architecture

- The AAA Rule. Three components, *independent*
- Authentication
  - 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, …)
- Authorization
  - 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
- Accounting
  - List of actions (who, when, what, where) that enables traceability of all changes and transactions rollback

More on IAM Architecture

- 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)
- Be aware !
  - RBAC should be a simplification
  - Keep the number of roles to a minimum

Why Identity Management ?

- Legal Constraints
  - In many areas there is a legal obligation of traceability
  - Basel II (Global Banking financial regulations)
  - Sarbanes Oxley Act (SOX) in the US
  - 8th EU Privacy Directive + national laws in Europe
- Financial constraints
  - Offload IT experts from administrative tasks with little added value (user registration, password changes, granting permissions, …)
- Technical opportunity
  - Simplification of procedures, increased opportunity
  - Centralized security policy possible

Aware of legal constraints

- 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

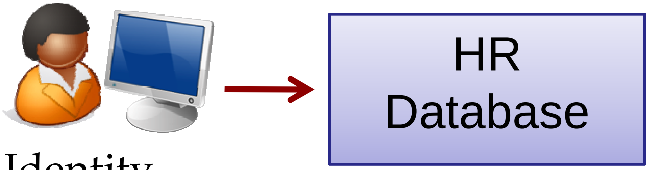
Implementing IM / IAM

- 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

IAM Architecture components (1/5)

- (web) application for person and account registration
  - Used by the administration to create identities
  - Approval, workflow and information validation depends on the type of data
    - Requiring a workflow or validation/approval by the administration. Examples: Name, passport no, date of birth
    - Available in self service to end-user:
      Examples: password change, preferred language, …

IAM Architecture

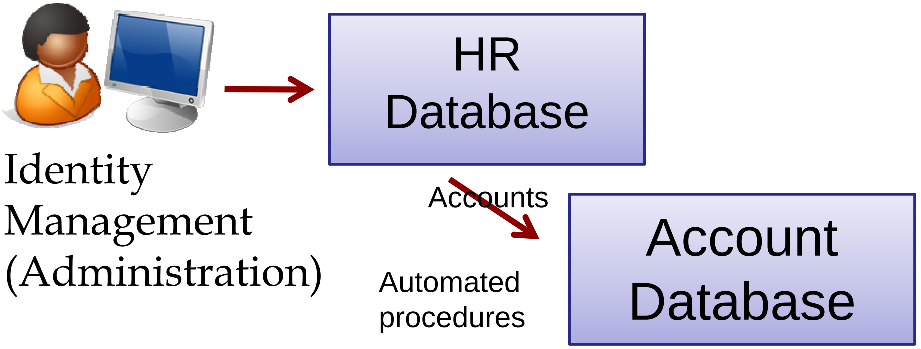


Identity
Management
(Administration)

IAM Architecture components (2/5)

- Process and workflow well defined
  - What are the “administrative” requirements to be “authorized” to use service “xyz”
  - “administrative” means that you have all information in the IAM database
  - You can define rules and process to follow. 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

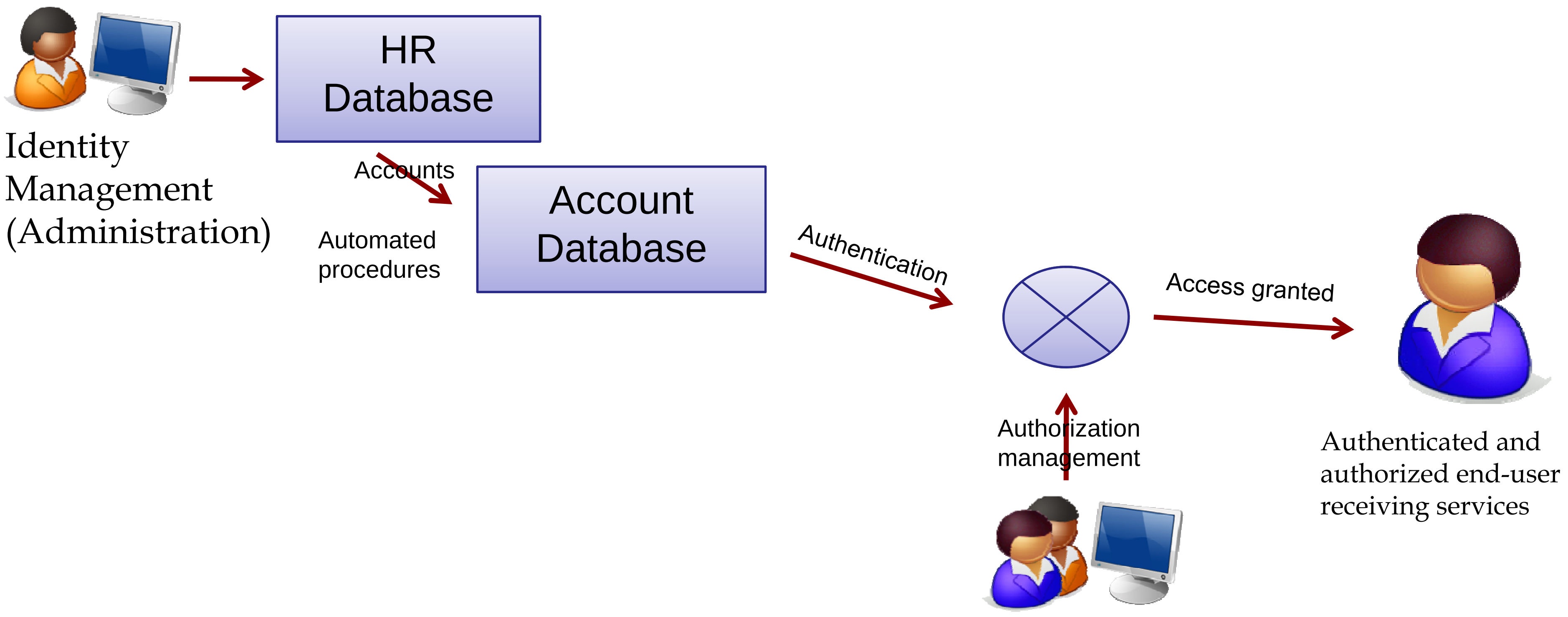
IAM Architecture



IAM Architecture components (3/5)

- Service-specific interfaces to manage authorization
  - 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

IAM Architecture



Identity Management (Administration)

HR Database

Accounts

Automated procedures

Account Database

Authentication

Access granted

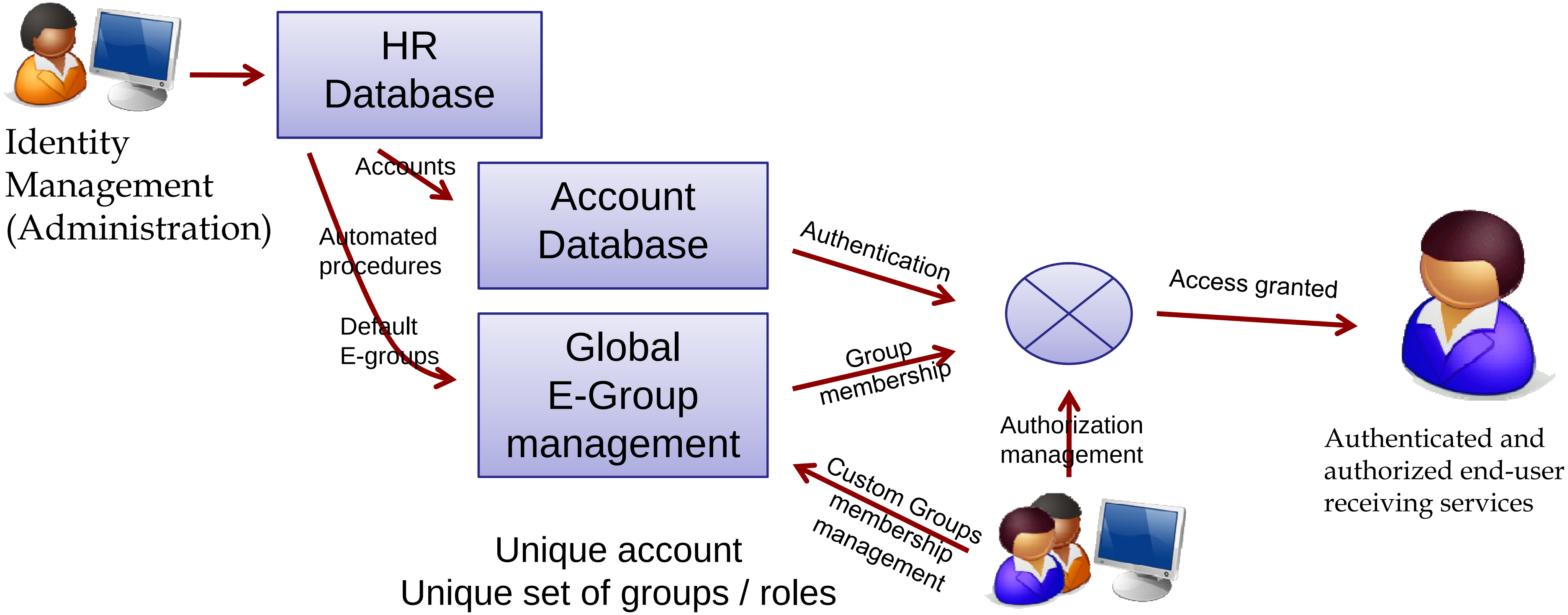
Authorization management

Authenticated and authorized end-user receiving services

IAM Architecture components (4/5)

- (web) application to manage group memberships
  - Indirect way to manage authorizations
  - 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

IAM Architecture



Identity Management (Administration)

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

Authenticated and authorized end-user receiving services

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

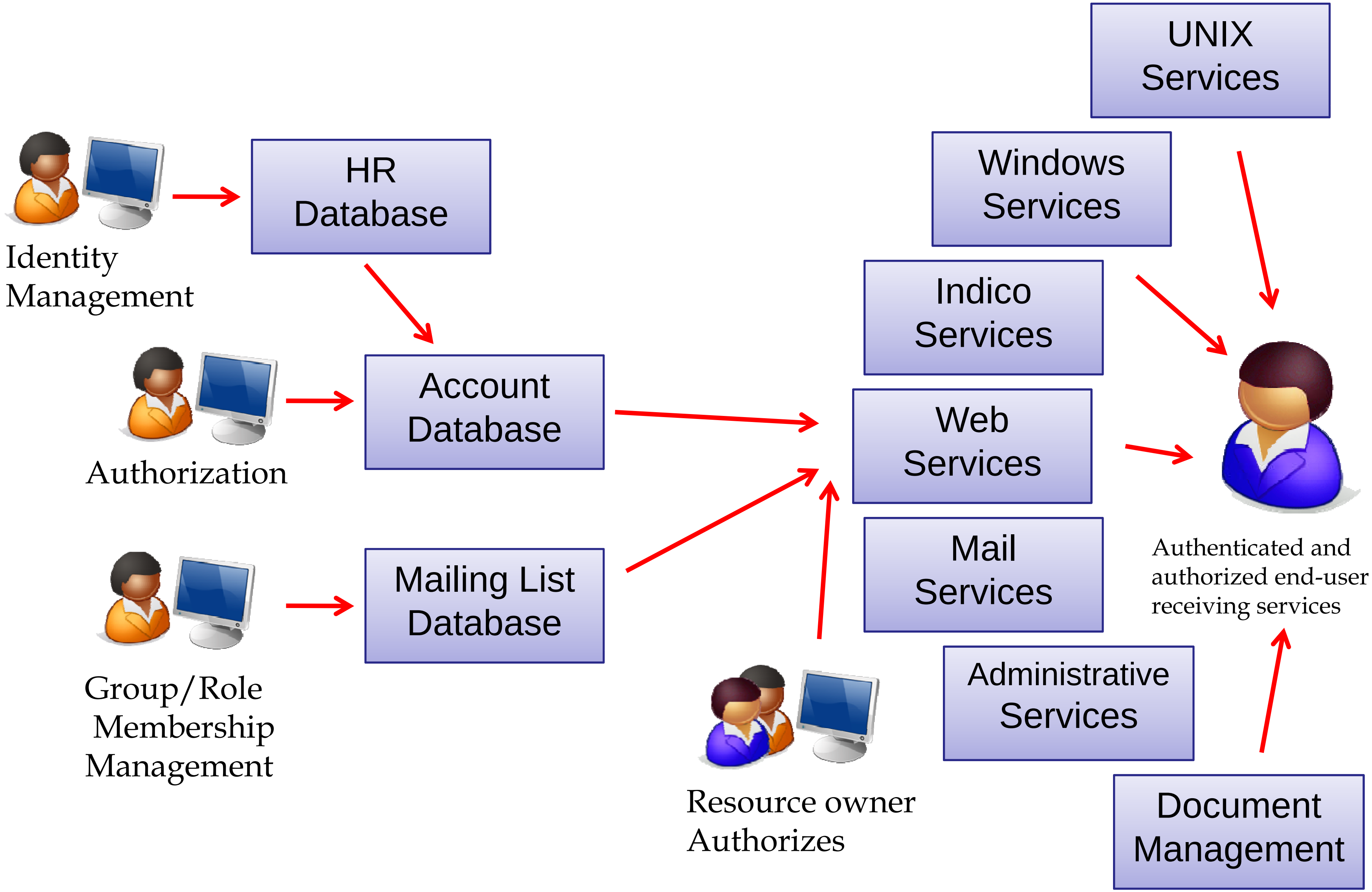
IAM Architecture components (5/5)

- Single-Sign-On (SSO) services
  - aware of group memberships
  - Authentication portal for web-based applications
  - Kerberos services for Windows and/or AFS users
  - Certification authority for grid users
- Directories, LDAP, …
- A well thought communication plan to inform all users

Experience at CERN

- 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, Oracle, …
  - Multiple accounts per person
  - Being migrated towards a unique identity management system with one unique account for all services

CERN Today



Identity Management

HR Database

Authorization

Account Database

Group/Role Membership Management

Mailing List Database

UNIX Services

Windows Services

Indico Services

Web Services

Mail Services

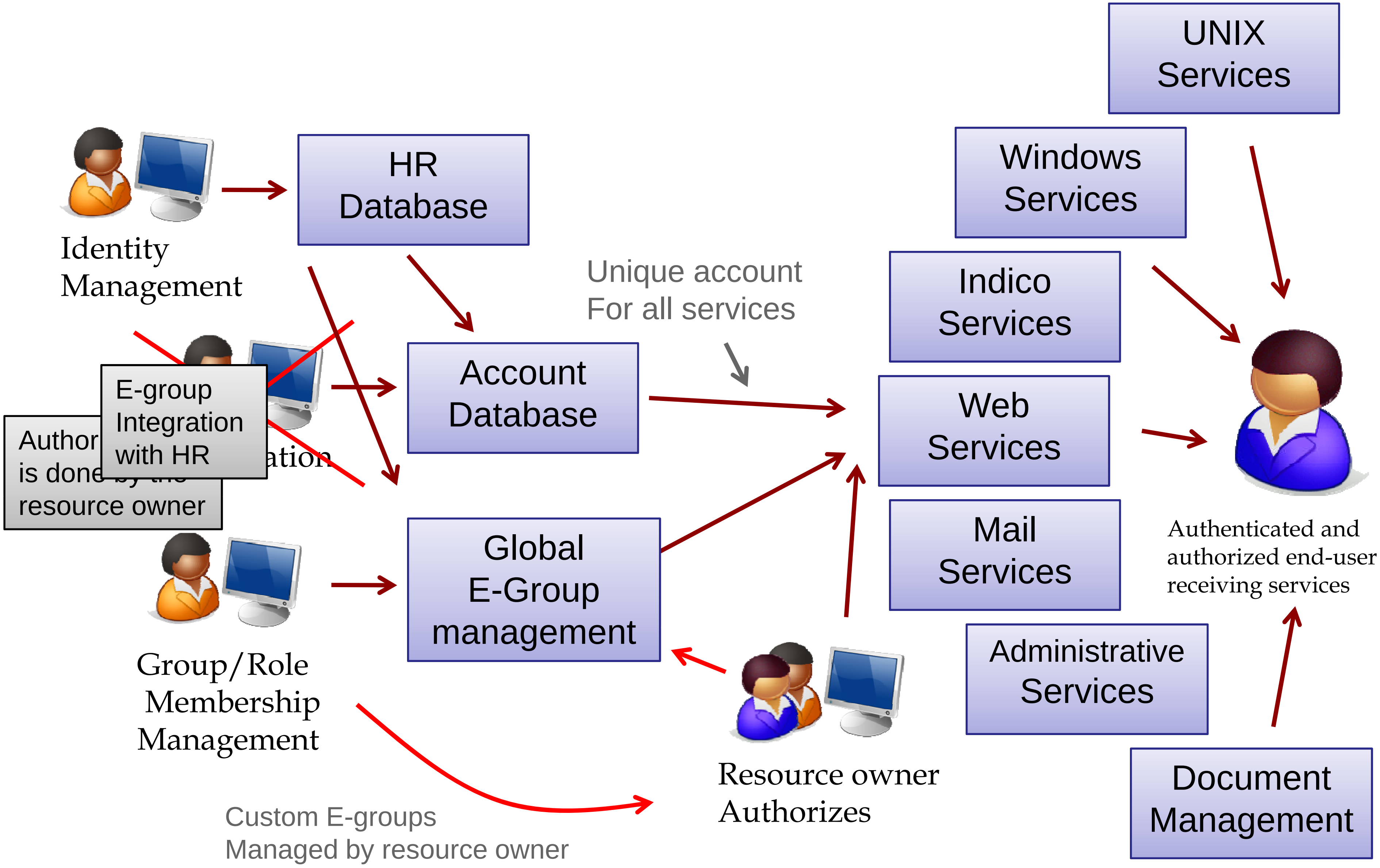
Administrative Services

Document Management

Resource owner Authorizes

Authenticated and authorized end-user receiving services

CERN Plan



Identity Management

HR Database

Account Database

Unique account
For all services

Author
is done by the
resource owner

E-group
Integration
with HR

ation

Global E-Group management

Group/Role Membership Management

Custom E-groups
Managed by resource owner

Resource owner Authorizes

UNIX Services

Windows Services

Indico Services

Web Services

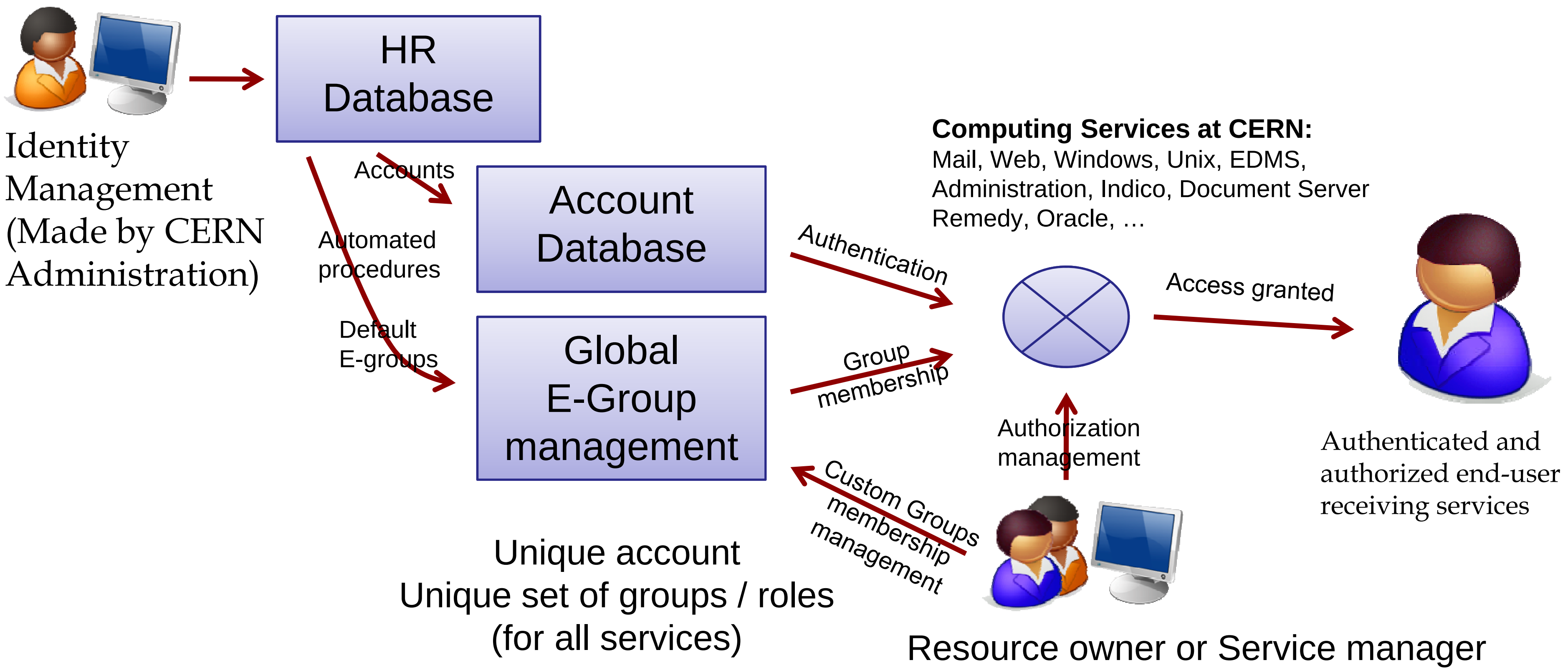
Mail Services

Administrative Services

Document Management

Authenticated and
authorized end-user
receiving services

CERN Plan



Identity Management (Made by CERN Administration)

HR Database

Accounts

Automated procedures

Default E-groups

Account Database

Global E-Group management

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

Authentication

Group membership

Custom Groups membership management

Computing Services at CERN:
Mail, Web, Windows, Unix, EDMS, Administration, Indico, Document Server Remedy, Oracle, …

Access granted

Authorization management

Authenticated and authorized end-user receiving services

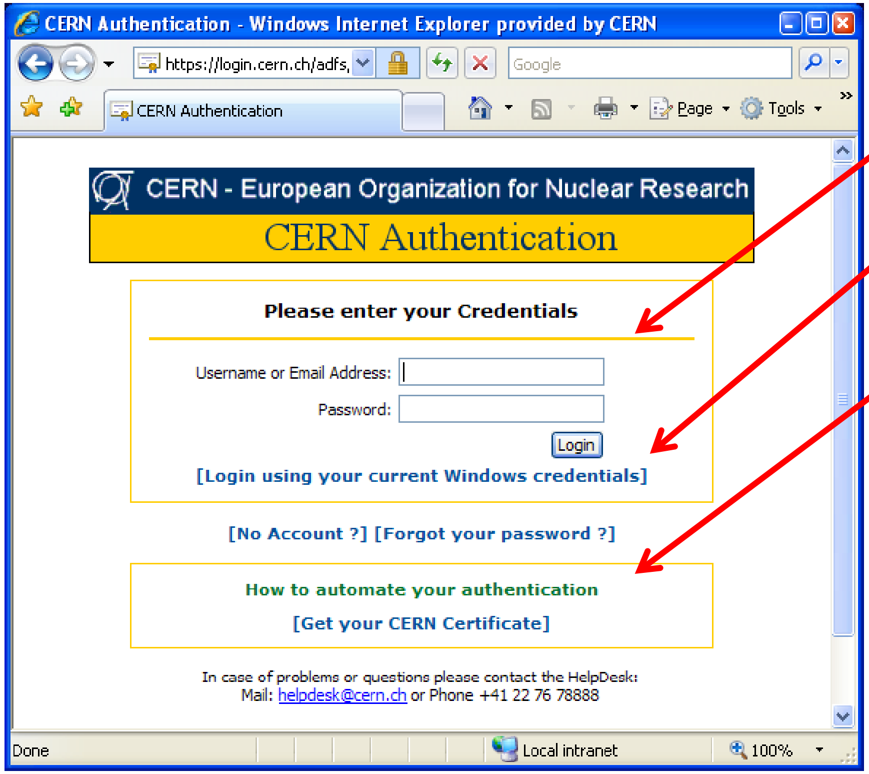
Resource owner or Service manager
Authorizes using

- User Accounts
- Default E-groups
- Custom E-groups

CERN Plan summary

- Central account management
- Only one account across services
  - – synchronize UNIX and Windows accounts
- Use Roles/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”.

Single Sign On Example


CERN Authentication - Windows Internet Explorer provided by CERN
https://login.cern.ch/adfs,
Google
CERN Authentication
Page
Tools
Done
Local intranet
100%

CERN - European Organization for Nuclear Research

CERN Authentication

Please enter your Credentials

Username or Email Address:

Password:

Login

[Login using your current Windows credentials]

[No Account ?] [Forgot your password ?]

How to automate your authentication

[Get your CERN Certificate]

In case of problems or questions please contact the HelpDesk:
Mail: helpdesk@cern.ch or Phone +41 22 76 78888

Username / Password

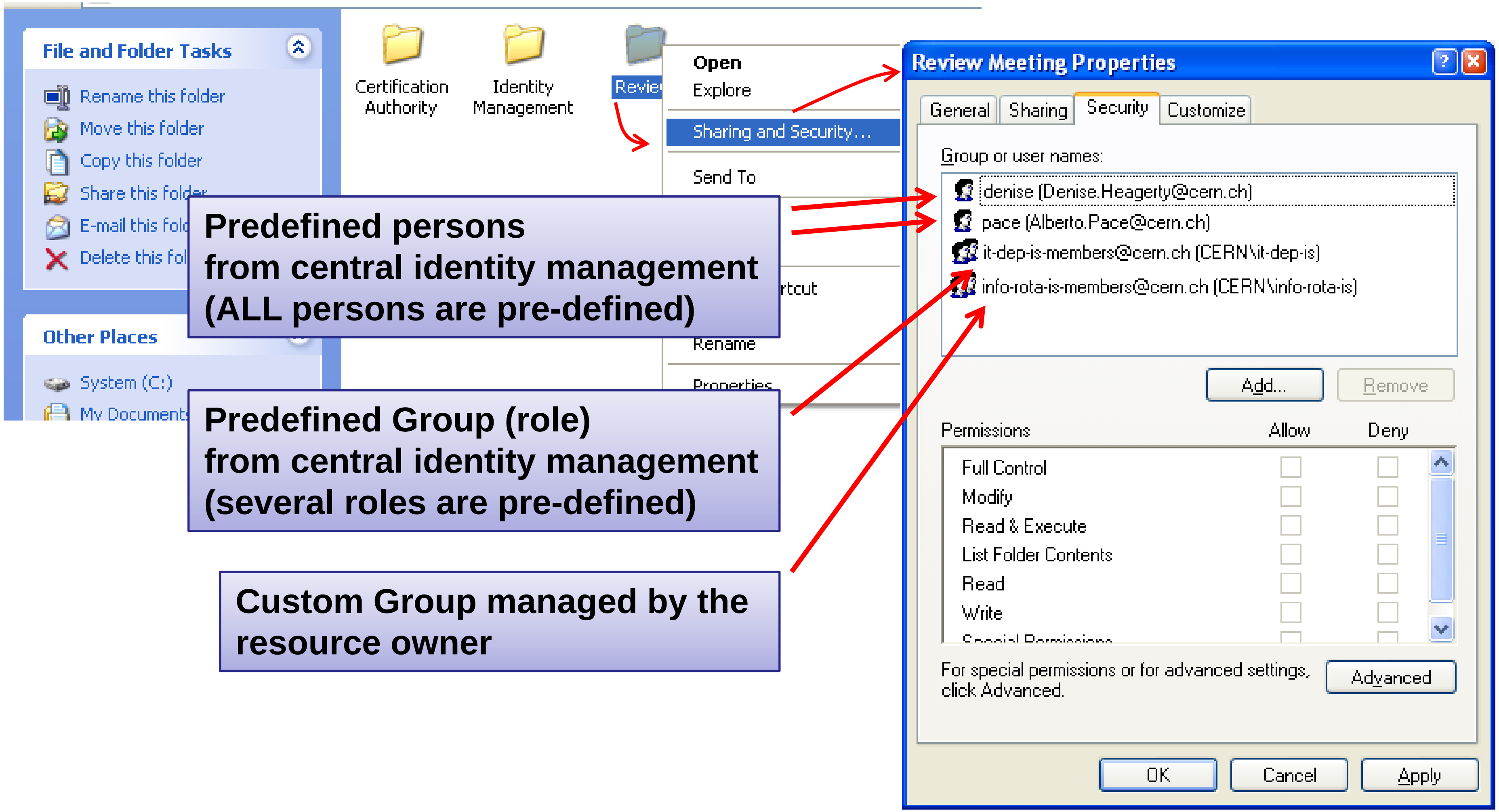
SSO using Windows Credentials

SSO using Grid Certificate

DEMO

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

Example



Group or user names:

- denise (Denise.Heagerty@cern.ch)
- pace (Alberto.Pace@cern.ch)
- it-dep-is-members@cern.ch (CERN\it-dep-is)
- info-rota-is-members@cern.ch (CERN\info-rota-is)

Permissions	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	□	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Predefined persons from central identity management (ALL persons are pre-defined)

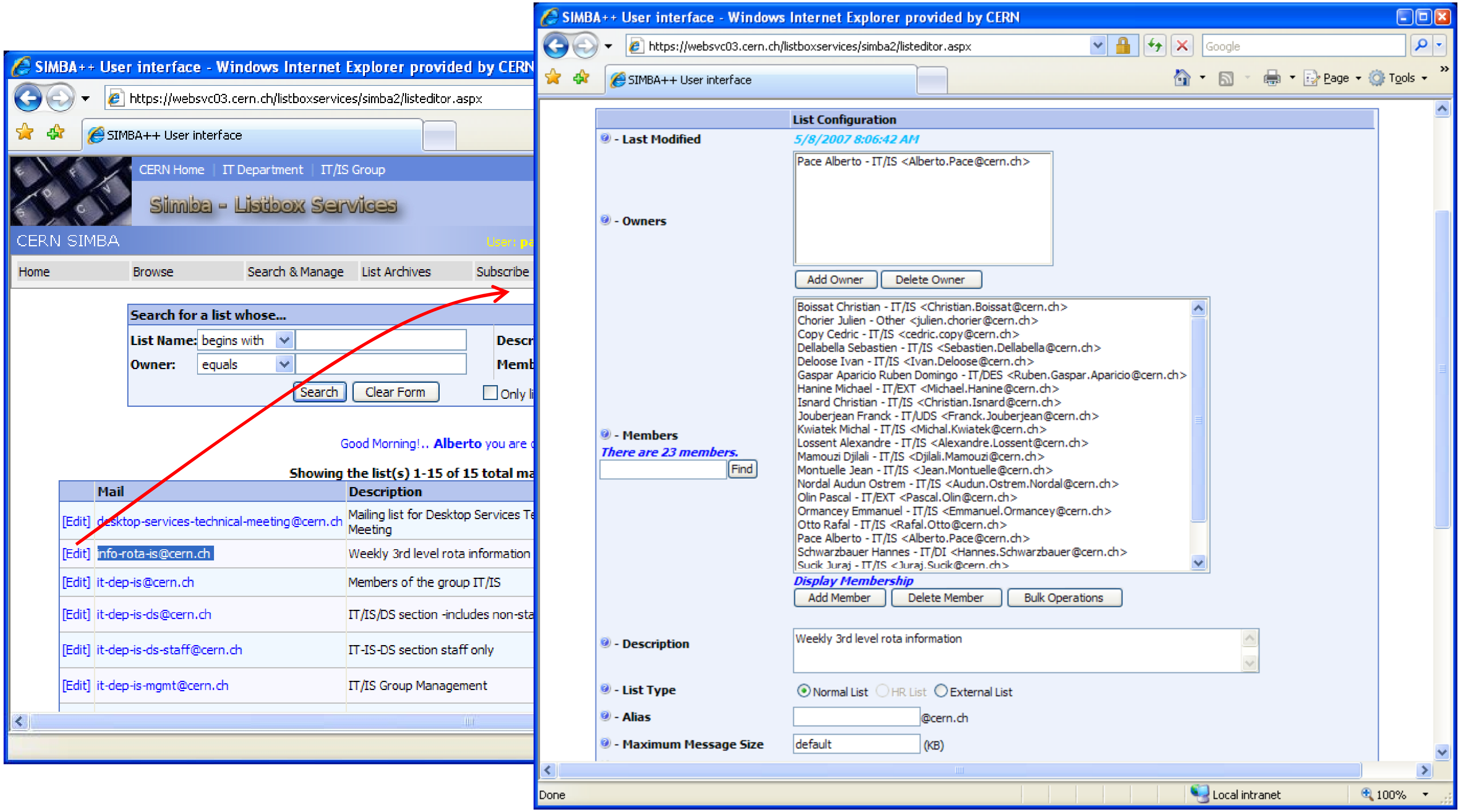
Predefined Group (role) from central identity management (several roles are pre-defined)

Custom Group managed by the resource owner

Internet Services

Managing custom group example

CERN IT Department



SIMBA++ User interface - Windows Internet Explorer provided by CERN

https://websvc03.cern.ch/listboxservices/simba2/listeditor.aspx

CERN Home | IT Department | IT/IS Group

Simba - Listbox Services

CERN SIMBA

Home | Browse | Search & Manage | List Archives | Subscribe

Search for a list whose...

List Name: begins with

Owner: equals

Search | Clear Form

Good Morning!.. **Alberto** you are

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

	Mail	Description
[Edit]	desktop-services-technical-meeting@cern.ch	Mailing list for Desktop Services Te Meeting
[Edit]	info-rota-is@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

SIMBA++ User interface - Windows Internet Explorer provided by CERN

https://websvc03.cern.ch/listboxservices/simba2/listeditor.aspx

List Configuration

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

- Owners

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

Add Owner | Delete Owner

- Members

There are 23 members.

Find

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>
Jouberjean Franck - IT/UDS <Franck.Jouberjean@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>
Sucik Juraj - IT/IS <Juraj.Sucik@cern.ch>

Display Membership

Add Member | Delete Member | Bulk Operations

- Description Weekly 3rd level rota information

- List Type ● Normal List ○ HR List ○ External List

- Alias @cern.ch

- Maximum Message Size default (KB)

Done | Local intranet | 100%

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

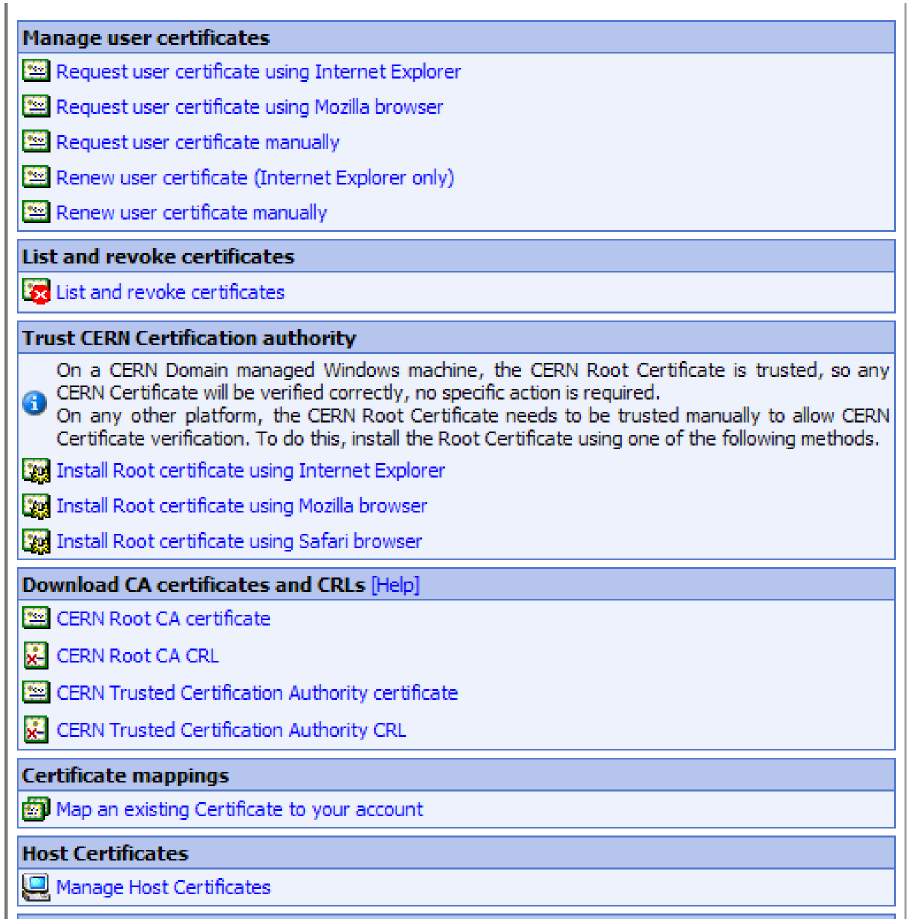
Integrating the big picture …

- Global identity management a requirement for HEP computing and Grid activities
- CERN efforts in identity management integrate in the global community 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 IM and Grid Certificates

- CERN Certification authority online and linked to the CERN Identity management
  - http://cern.ch/ca

- Offers grid certificates to authorized users
- Recognizes gridpma certificates and allows mapping to the CERN accounts



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

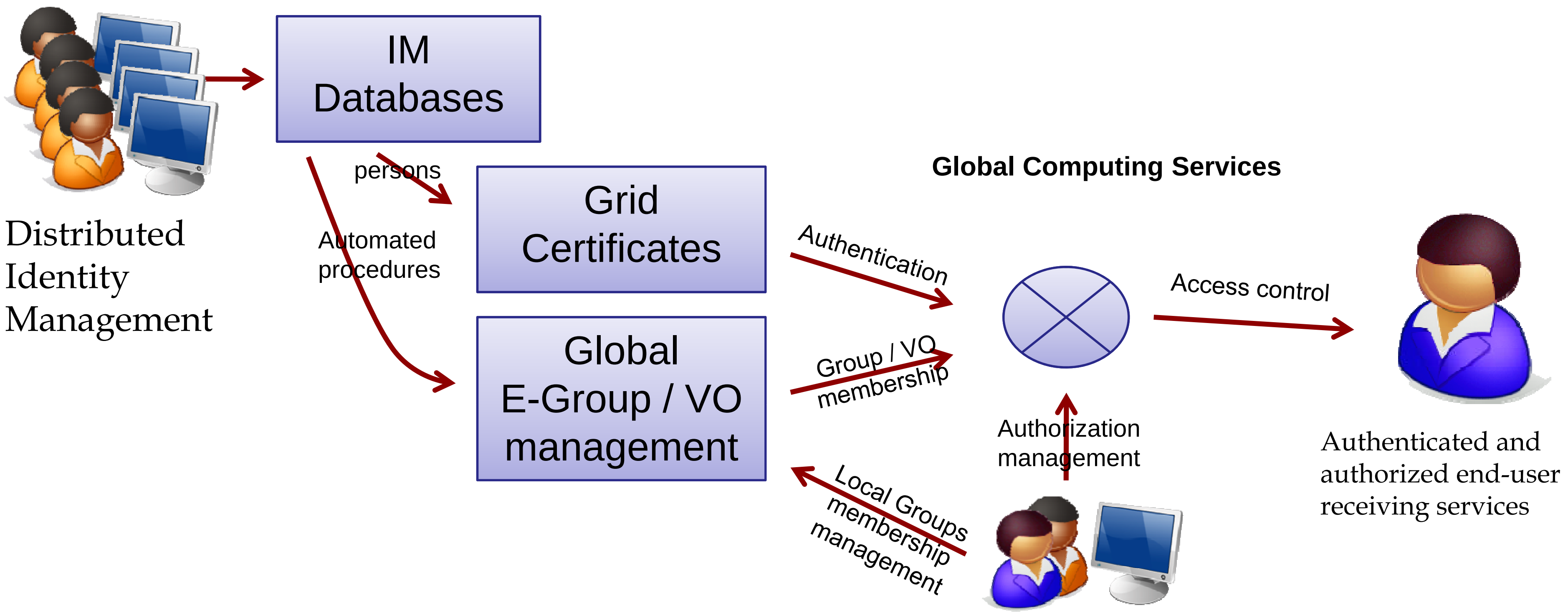
Certificate mappings

- Map an existing Certificate to your account

Host Certificates

- Manage Host Certificates

The big picture



Distributed Identity Management

IM Databases

persons

Automated procedures

Grid Certificates

Global E-Group / VO management

Global Computing Services

Authentication

Group / VO membership

Local Groups membership management

Authorization management

Access control

Authenticated and authorized end-user receiving services

Resource owner or Service manager
Authorizes using

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

Conclusion

- Necessary to resist to pressure of having
  - “Custom” solution for “special” users
  - Exception lists
- Security in focus
  - Complexity and security don’t go together
- Once identity management is in place …
  - … you wonder why this was not enforced earlier