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, …
- 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

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

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

More definitions

- 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, …)

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

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)
- RBAC should remain a simplification
  - Keep the number of roles to a minimum

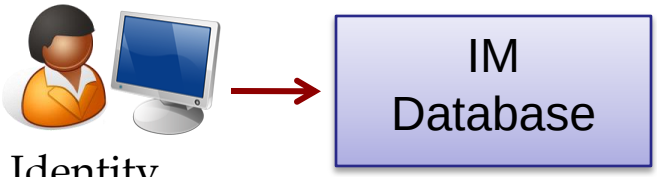
Motivations for Identity Management

- 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

IAM Architecture components (1/6)

- 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, …

IAM Architecture

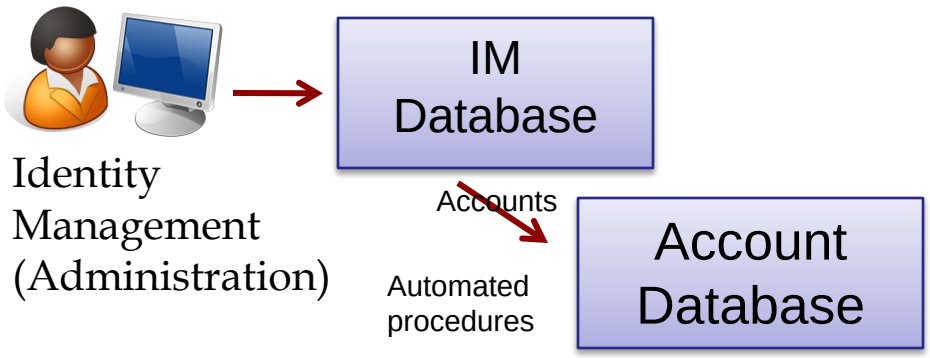


Identity Management (Administration)

IAM Architecture components (2/6)

- 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

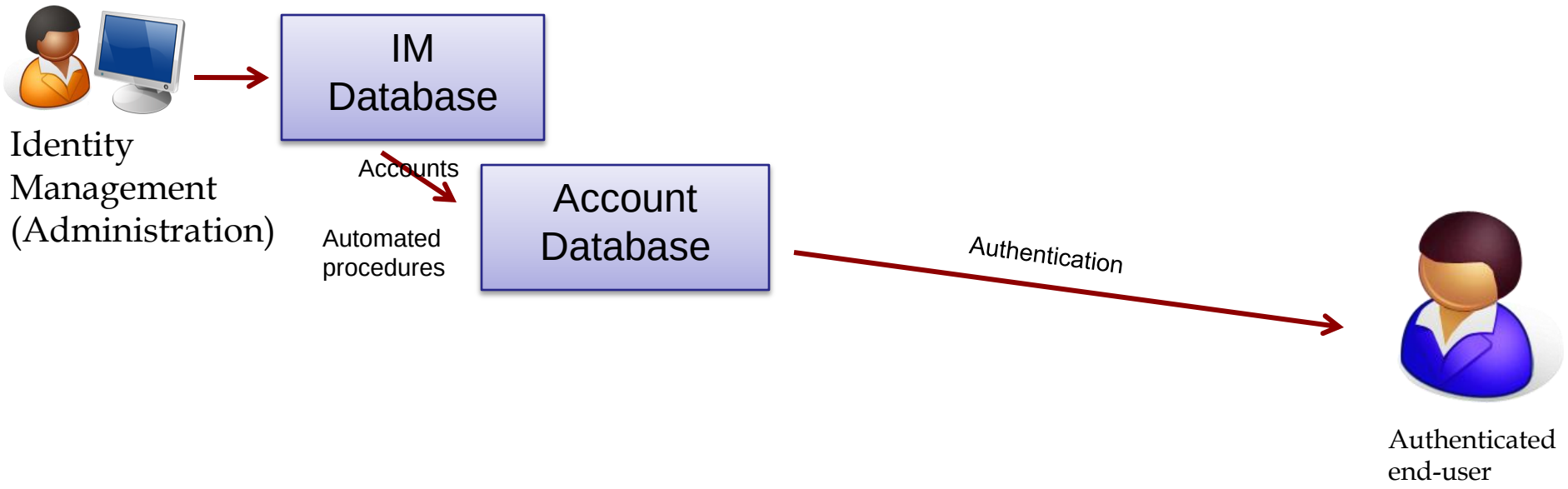
IAM Architecture



IAM Architecture components (3/6)

- Authentication 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)

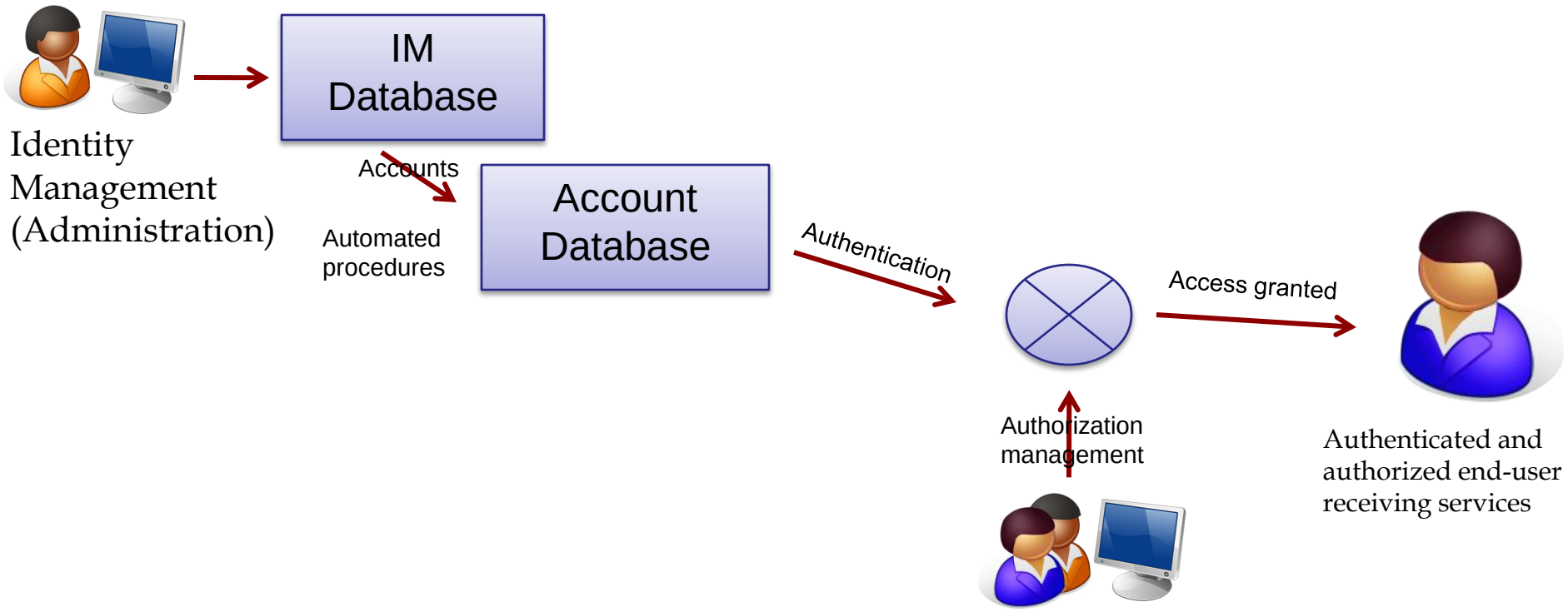
IAM Architecture



IAM Architecture components (4/6)

- Service-specific interfaces to manage Authorizations
  - 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

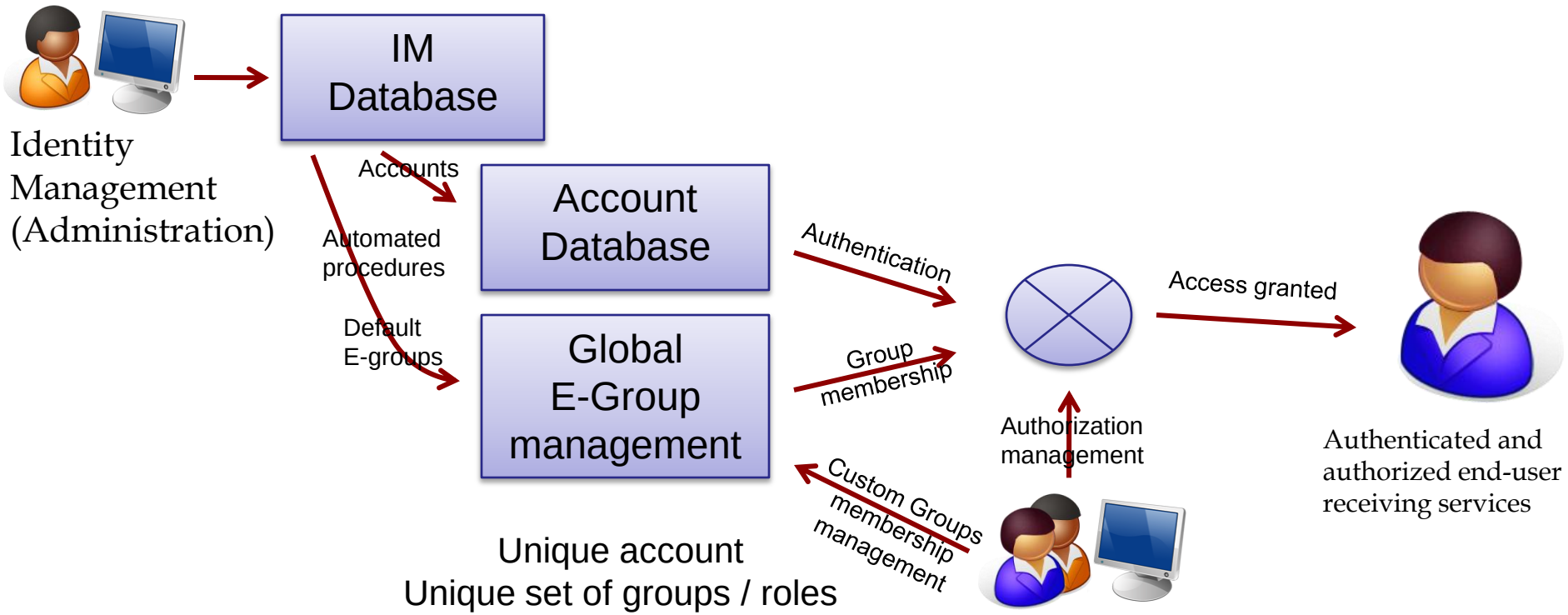
IAM Architecture



IAM Architecture components (5/6)

- 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

IAM Architecture



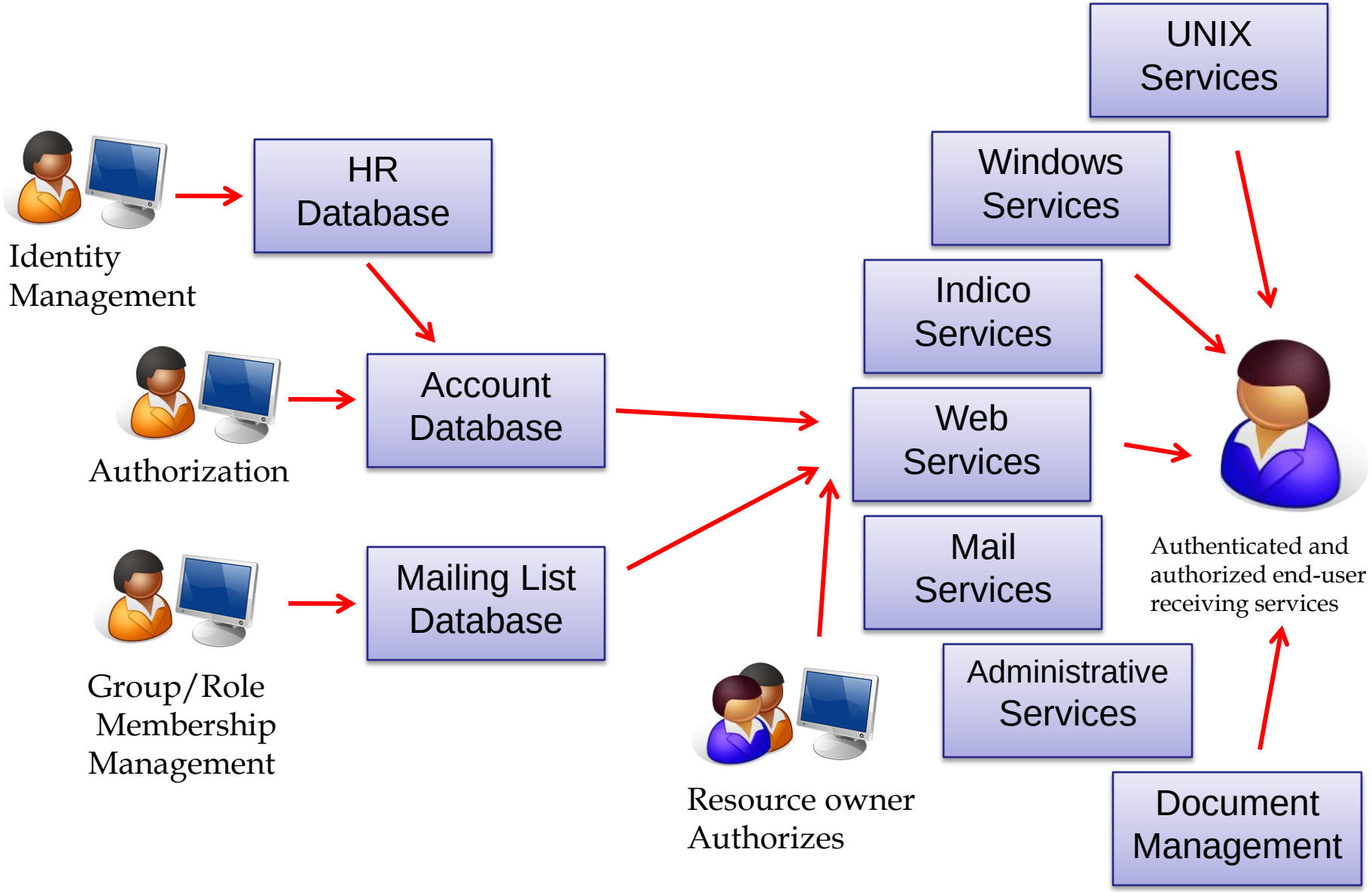
IAM Architecture components (6/6)

- Accounting
  - 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

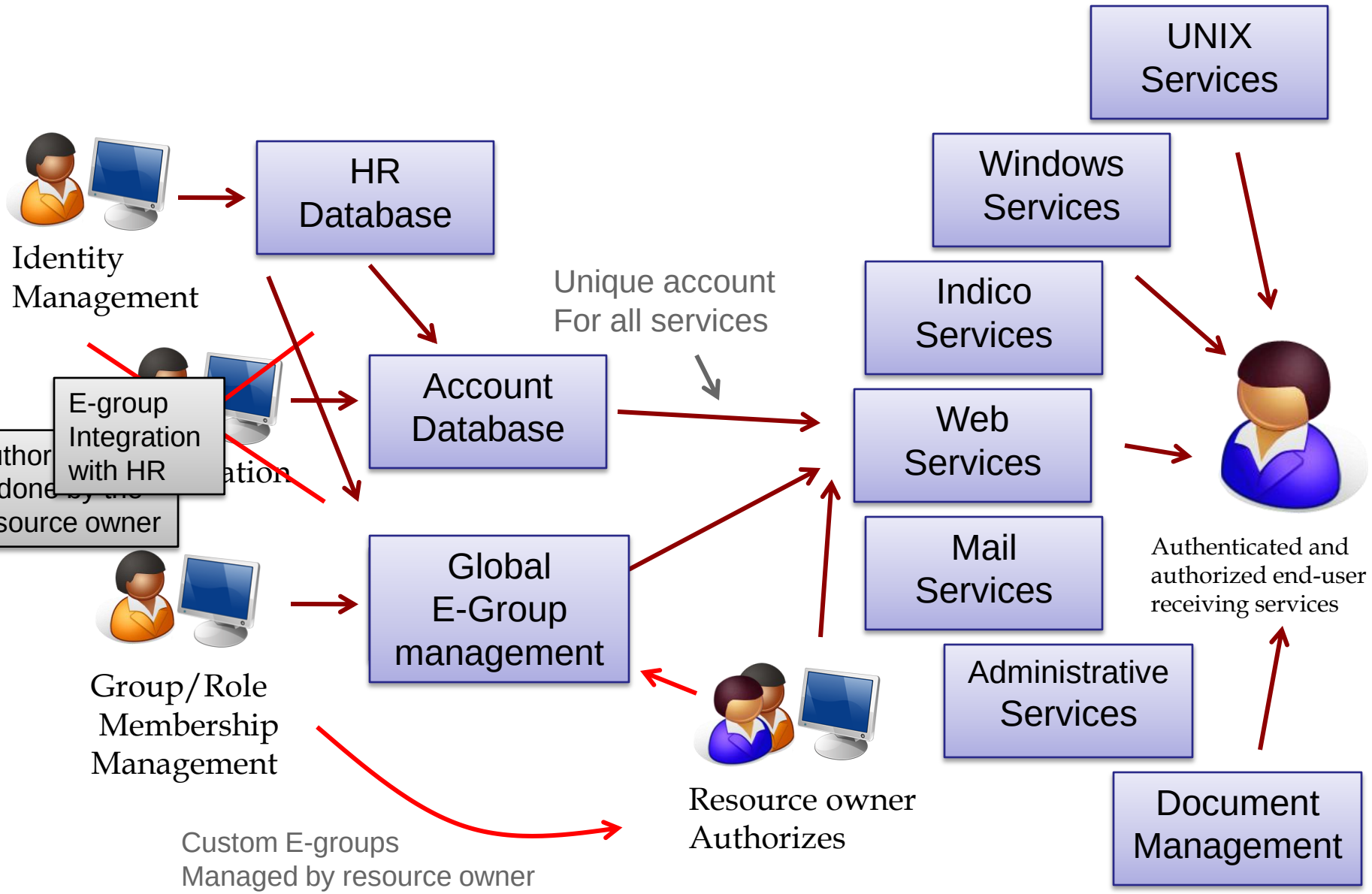
Experience at CERN

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

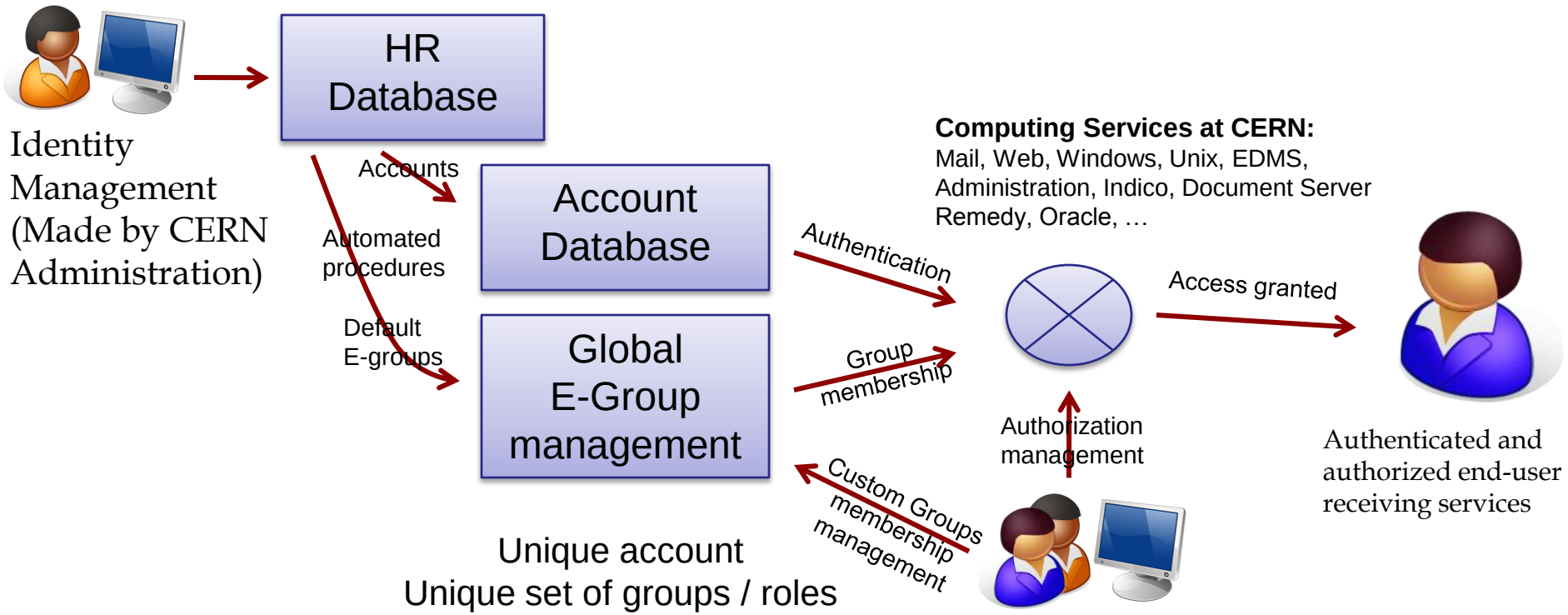
CERN Yesterday / Today



CERN Plan


UNIX Services
Windows Services
HR Database
Identity Management
Unique account For all services
Indico Services
Account Database
Web Services
E-group Integration with HR
Author
is done by the resource owner
Mail Services
Global E-Group management
Authenticated and authorized end-user receiving services
Group/Role Membership Management
Administrative Services
Resource owner Authorizes
Document Management
Custom E-groups Managed by resource owner

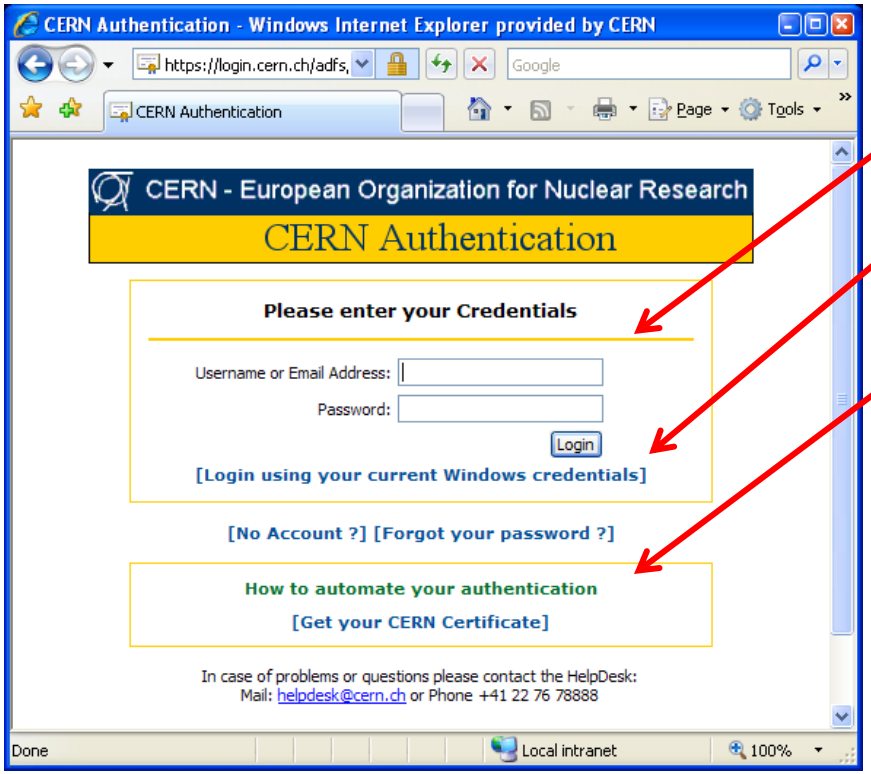
CERN Plan


HR Database
Accounts
Automated procedures
Default E-groups
Account Database
Global E-Group management
Authentication
Group membership
Custom Groups membership management
Authorization management
Access granted
Computing Services at CERN:
Mail, Web, Windows, Unix, EDMS, Administration, Indico, Document Server Remedy, Oracle, …
Identity Management (Made by CERN 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

CERN Plan summary

- 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".

Single Sign On Example



Username / Password

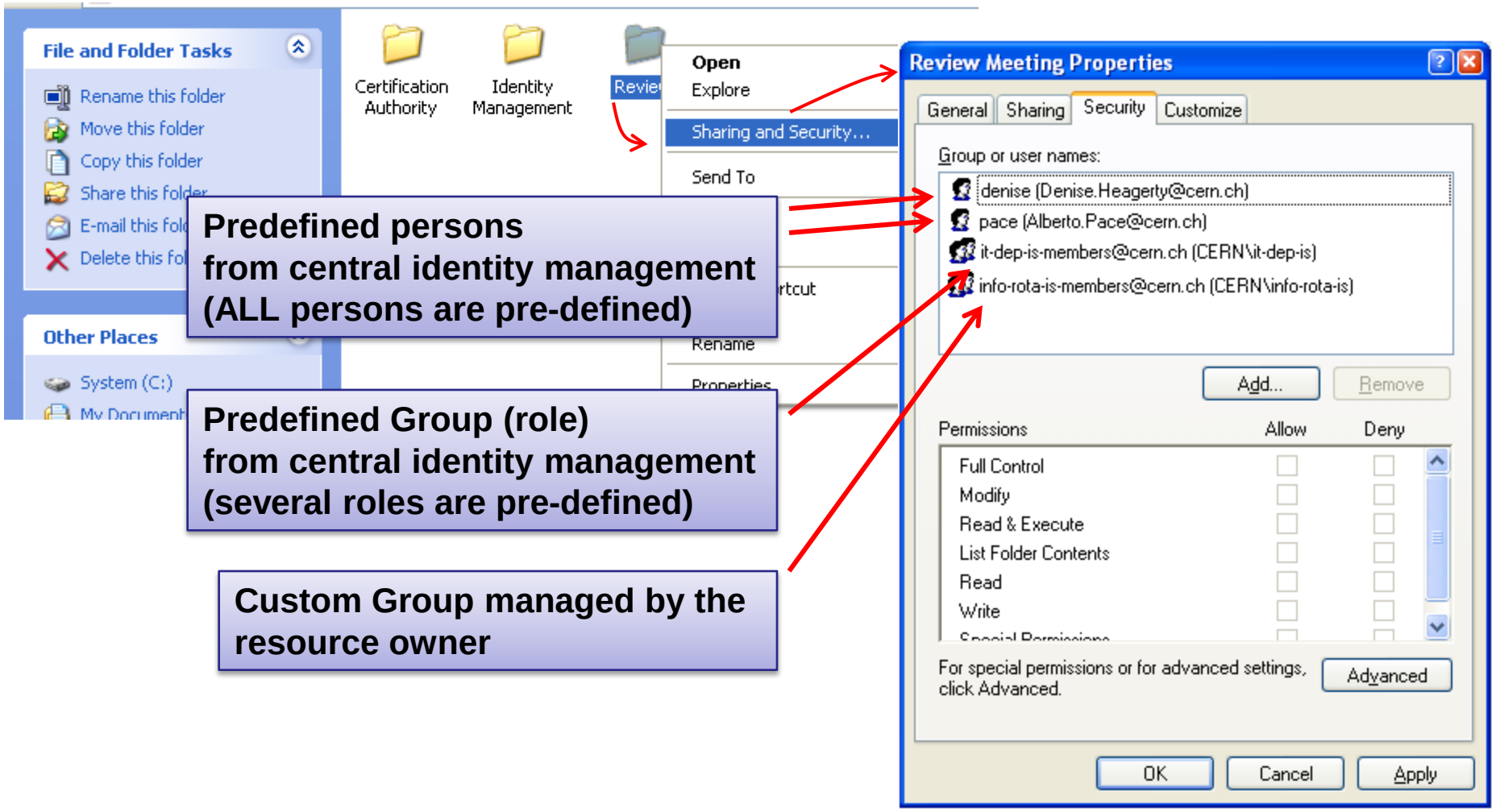
SSO using Windows Credentials

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

Example

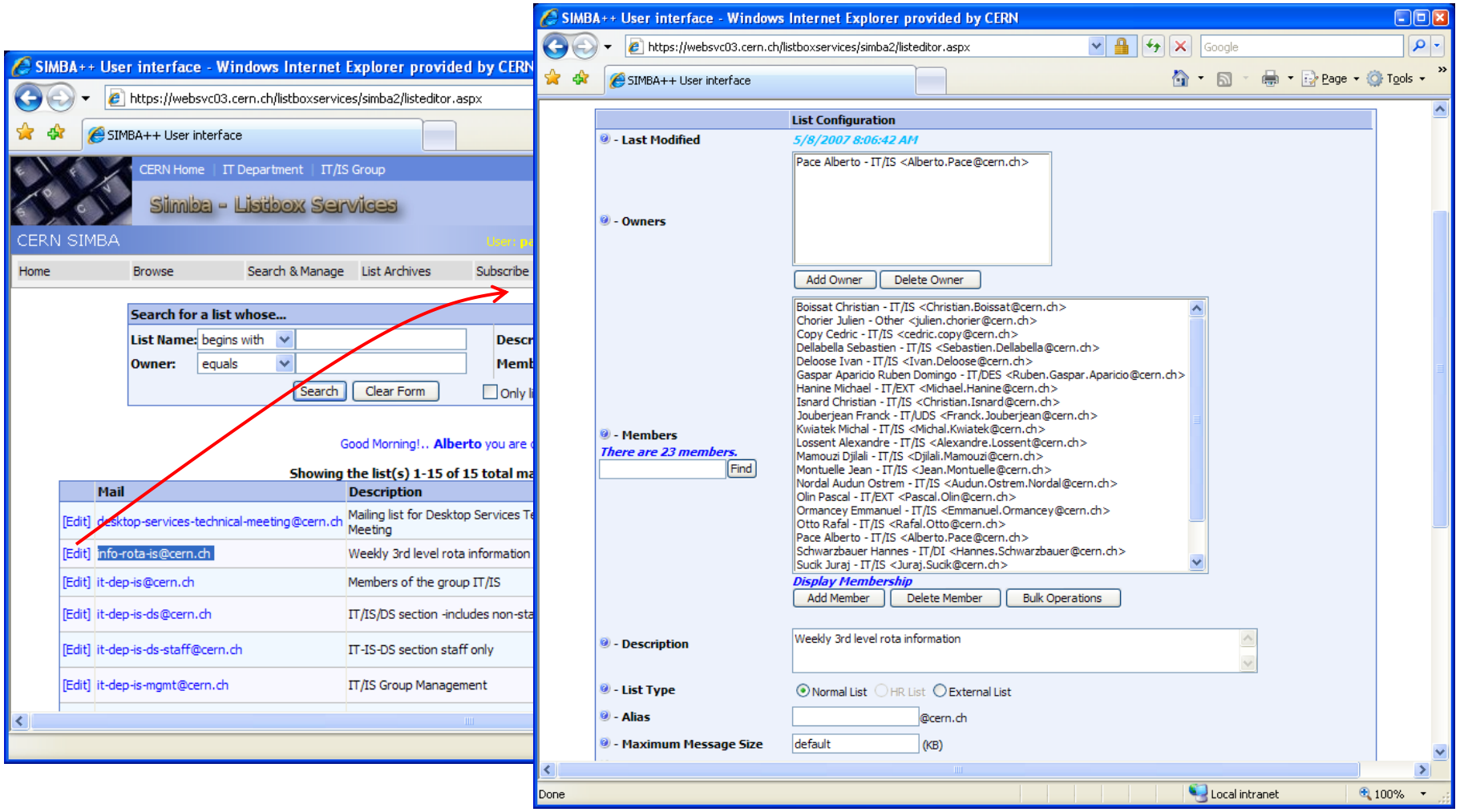


Predefined persons from central identity management (ALL persons are pre-defined)

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

Custom Group managed by the resource owner

Managing custom group example



Integrating the big picture …

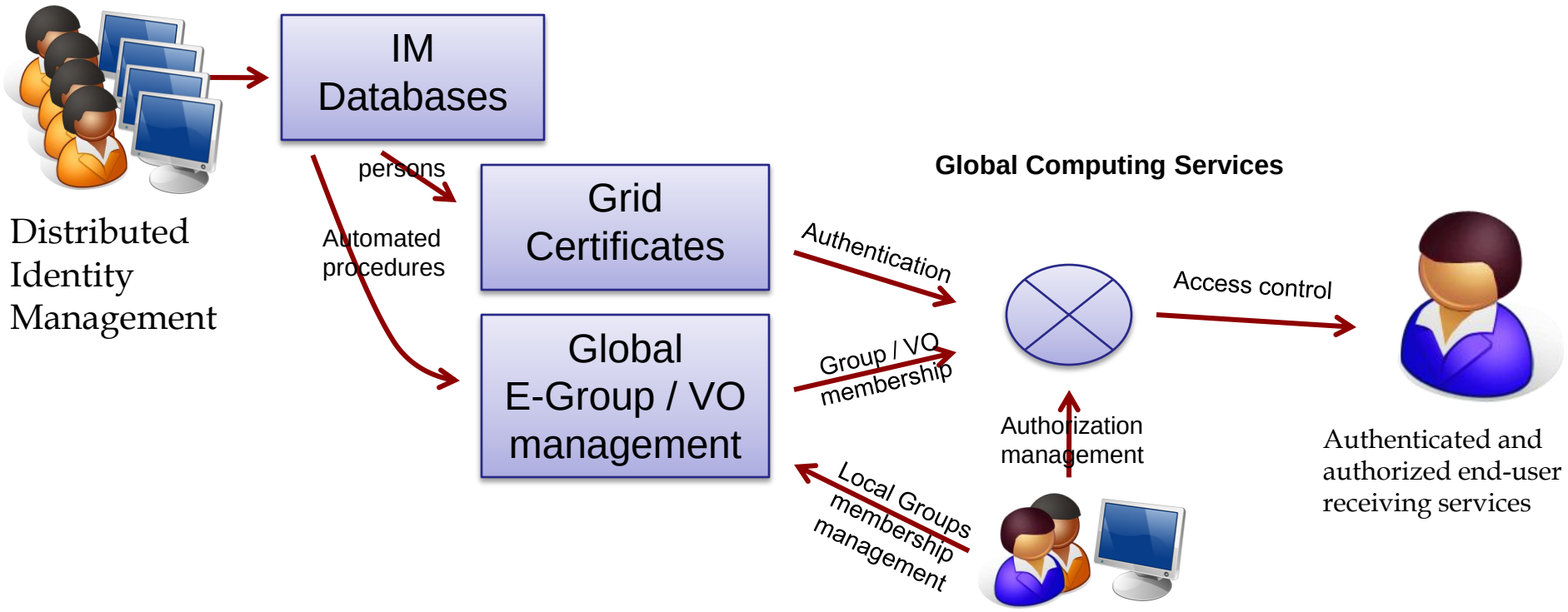
- Global identity management a requirement for HEP computing and Grid activities through the "International Grid Trust Federation" (www.gridpma.org)
- Coordination is done through the regional Policy Management Authorities
  - Asia Pacific Grid PMA
  - European Grid PMA
  - The Americas Grid PMA
- CERN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

CERN IM and Grid Certificates

- 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

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

The big picture



Resource owner or Service manager
Authorizes using
- User Accounts (Certificate Subjects)
- VO or local E-groups

Summary / Conclusion

- 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