



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**

← **THIS TALK**



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 / ...) and an entity (person, account, computer, group, ...) which grants access to a given resource (file, computer, printer, room, information system, ...), at a given time, from a given location**
 - ◆ **Access control can be physical (specific location, door, room, ...) or logical (password, certificate, biometric, token, ...)**
 - ◆ **Resources can also be physical (room, a terminal, ...) or logical (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**
 - ◆ **Portal web site to centrally manage group memberships or permissions**



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



Implementing IM / IAM

- ◆ It is an heavy project, there are many parameters
- ◆ 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



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



IAM Architecture

- ◆ 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



More 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**



IAM Architecture components (1/3)

- ◆ **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 answer this question, you can automate**
 - ◆ **If you can't, you have a problem**
 - ◆ **Putting an administrative person to “manually handle” the answer to that question won't solve the problem in large organizations**



More IAM Architecture components (2/3)

- ◆ (web) Portal for person and account registration
 - ◆ Used by the administration to create identities
 - ◆ Approval, workflow and information validation depends on the type of data
 - ◆ Examples requiring validation by the administration, approval or workflow : Name, passport no, date of birth
 - ◆ Examples available in self service to end-user: Password change, preferred language, ...
- ◆ 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



More IAM Architecture components (3/3)

- ◆ (web) Portal 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 foresee nesting of groups
- ◆ 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, ...
- ◆ Complicated 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



Resource owner Authorizes

Windows Services

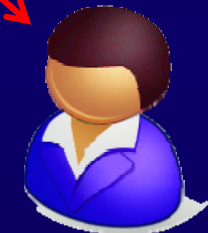
Indico Services

Web Services

Mail Services

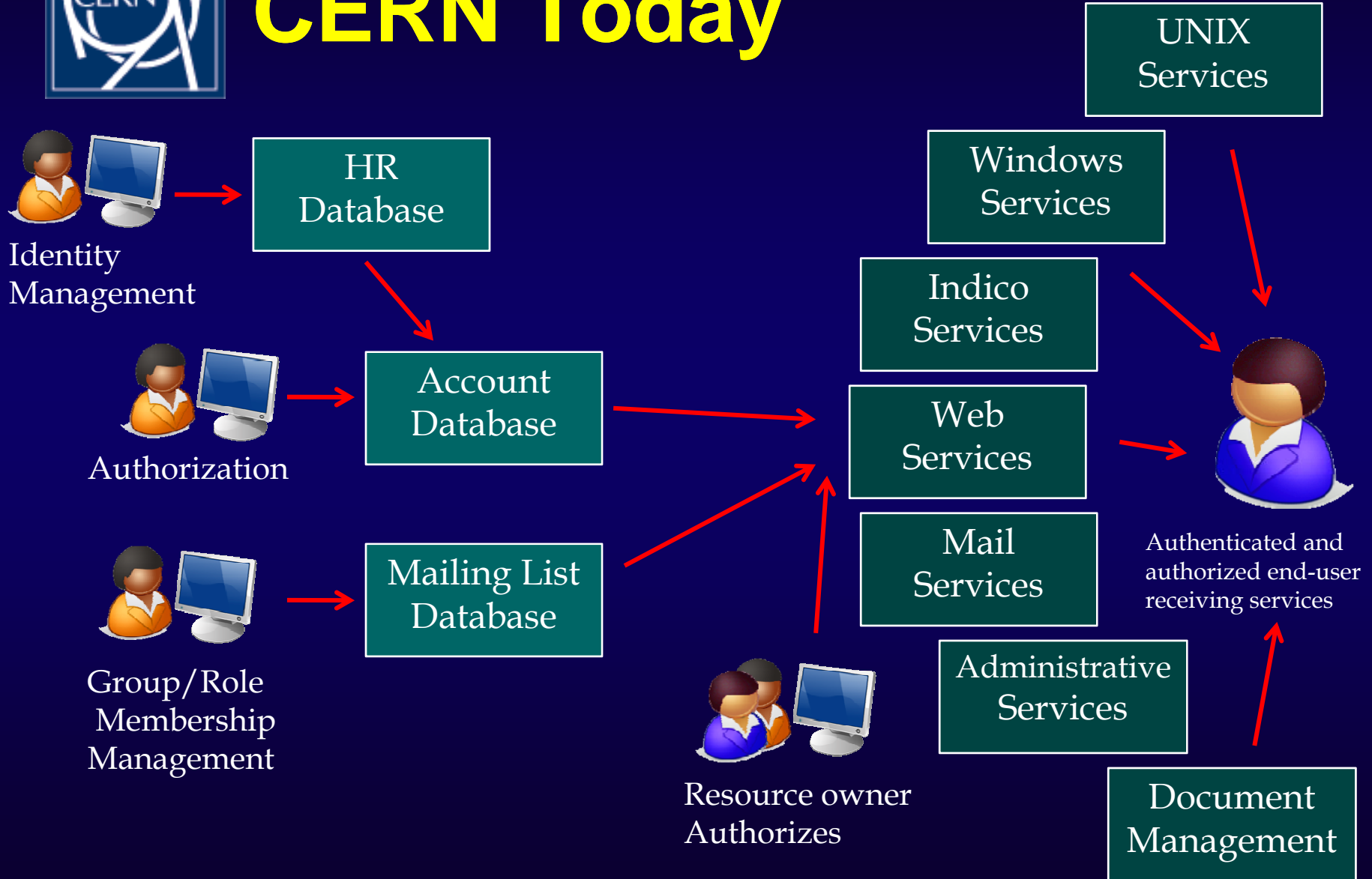
Administrative Services

UNIX Services



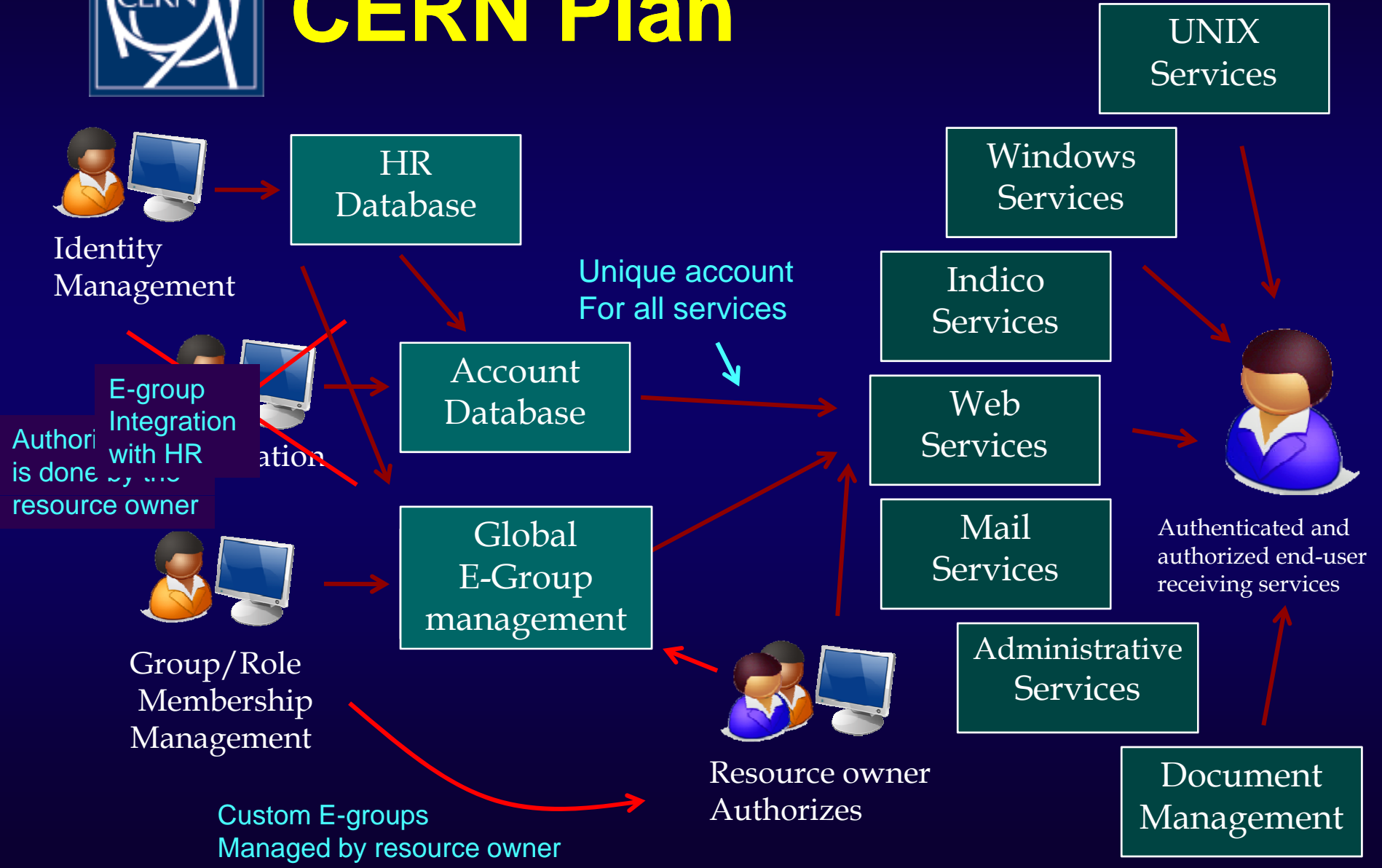
Authenticated and authorized end-user receiving services

Document Management





CERN Plan





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)

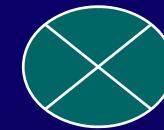
Computing Services at CERN:

Mail, Web, Windows, Unix, EDMS, Administration, Indico, Document Server Remedy, Oracle, ...

Authentication

Group membership

Custom Groups membership management



Authorization management

Access granted



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/

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

Done Local intranet 100%

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

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

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"/>



Managing custom group example

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 [] 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-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

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>
Kwiatk Michal - IT/IS <Michal.Kwiatk@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>
Ormaney Emmanuel - IT/IS <Emmanuel.Ormaney@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>
Sudik Juraj - IT/IS <Juraj.Sudik@cern.ch>

- Members

There are 23 members.

[Find]

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)



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



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