

CERN Single Sign On

<http://cern.ch/login>

Emmanuel Ormancey
CERN IT/IS

- **History**
- **CERN Authentication**
 - ◆ Main goals
 - ◆ Authentication methods
 - ◆ Demo overview
- **Technical background**
 - ◆ Identity provider
 - ◆ Service providers
- **The next steps**
- **Links**

A few years ago

- **Every day a CERN user had to type in:**
 - Credentials to open the Windows desktop
 - Credentials to open Linux
 - Credentials to read mails
 - Credentials to verify holidays
 - Credentials to upload CHEP presentations in Indico
 - ...

Different logins
Different passwords

Today

- **Situation is better, but not optimal**
 - Remains mainly 2 credential pairs (not synchronized)
 - Many experiments are still using dedicated user databases and credentials
 - *Some are stealing* credentials to populate local databases !!!

Main goals

- **Provide SSO for CERN Web Applications**
- **Simplify !**
 - ◆ Reduce number of user databases
 - ◆ Reduce number of login/password pairs to remember.
- **Centralize**
 - ◆ Only one user database, one credential pair to remember
 - ◆ Handle External accounts (lightweight registration)
 - ◆ Provide Groups and Roles membership
- **Improve security**
 - ◆ Block all accesses to applications in one click
 - ◆ Use permissions and delegation instead of sharing credentials
 - ◆ Complexity does not increase security !!!

Authentication Methods and user information

- **Different authentication methods**
 - ◆ Classic Forms (login and password)
 - ◆ Certificates (CERN CA Certificates, smartcards)
 - ◆ Windows Integrated (reuse windows current credentials)
- **User information, Groups and Roles**
 - ◆ All user information is available: name, email, building, etc...
 - ◆ Groups and Mailing Lists membership is available
 - ◆ No more 'per application dedicated role system'
- **Authentication is standalone**
 - ◆ Not linked to calling Web Application
 - ◆ A Linux/Apache application can use Windows Integrated authentication

Overview

CERN Home | IT Department | IT/IS Group | Mail Services | Web Services | Win Services

User: **ormancey - Emmanuel.Ormancey@cern.ch** [Logout] [Details]
Emmanuel Ormancey (Emmanuel.Ormancey@cern.ch)
Authentication by Windows Integrated

Home

Help

Contents

[Search for help]

- [-] NICE Environment
 - [-] Mandate
 - [+] NICE Installation
 - [+] NICE XP
 - [+] NICE 2000
 - [+] NICE Windows Updates
 - [+] Working with network files
 - [-] Working with portable computers
 - [-] Access your desktop remotely
 - [+] DFS WebDAV remote access
 - [+] Integrating Mac OS X with NICE (PILOT)
 - [+] FAQ for NICE

Users and Groups

- [-] Check A...
- [-] Change...
- [-] Group M...

Computers

- [-] List my C...
- [-] Compute...
- [-] Recreate...
- [-] Set Loca...
- [-] Set Loca...

Printing

[-] Print...

ap-groupe-elec
ap-it-members
ap-it-membesa
ap-it-staff
ap-members-all
ap-vote-2535
building-31
c5-members
ccnet
cern-ca-managers
cern-ca-managers Owners
cern-computing-postmasters

CERN - European Organization for Nuclear Research

CERN Authentication

Logout from CERN Applications

Single Sign On Service
Signed out of **login.cern.ch**

Applications
 Shibboleth
 WinServices

Close Window

Back to previous location

(this might ask for new credentials)

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

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

Overview

Service Provider



CERN Home IT Department IT/IS Group Mail Services Web Services Win Services

NICE Services User: **ormancey - Emmanuel.Ormancey@cern.ch** [Logout]
Emmanuel Ormancey (Emmanuel.Ormancey@cern.ch) [Details]
Authentication by Windows Integrated

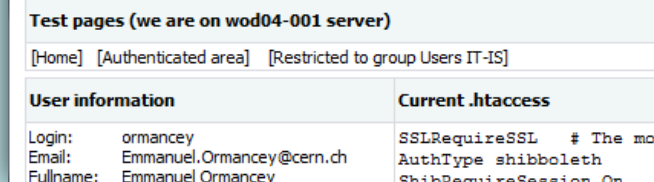
Home > UserInformation

User account

Login: ormancey
Name: Emmanuel Ormancey
Email: Emmanuel.Ormancey@cern.ch
Phone: 71057 (mobile: 160821)
Building: Bld. 31 Room R-017

- Windows + IIS
- Microsoft ADFS or Shibboleth SP

CERN Single Sign On - Apache Website demo



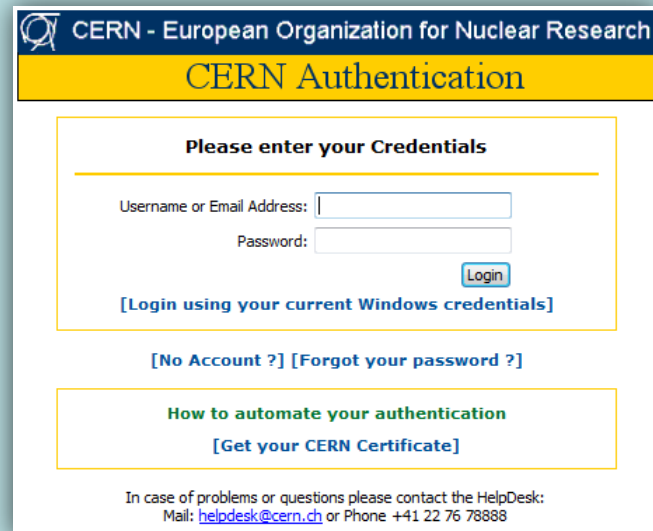
Test pages (we are on wod04-001 server)

[Home] [Authenticated area] [Restricted to group Users IT-IS]

User information	Current .htaccess
Login: ormancey	SSLRequireSSL # The mo
Email: Emmanuel.Ormancey@cern.ch	AuthType shibboleth
Fullname: Emmanuel Ormancey	ShibRequireSession On

- Linux or Unix + Apache
- Shibboleth SP

Identity Provider



CERN - European Organization for Nuclear Research

CERN Authentication

Please enter your Credentials

Username or Email Address:

Password:

[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: helodesk@cern.ch or Phone +41 22 76 78888

Microsoft ADFS

Identity Provider

- **Checks identity, supports various authentication methods**
- **Loads and shares user information: “Claims”**
- **Microsoft ADFS based**
 - ◆ **Active Directory Federation Services**
 - Credentials are checked in Active Directory
 - ◆ **WS-Federation Passive Requester Profile (WS-FPRP) compliant**
- **Hosted on load balanced servers, in critical UPS area**
 - ◆ **Minimize downtime: authentication is critical !**

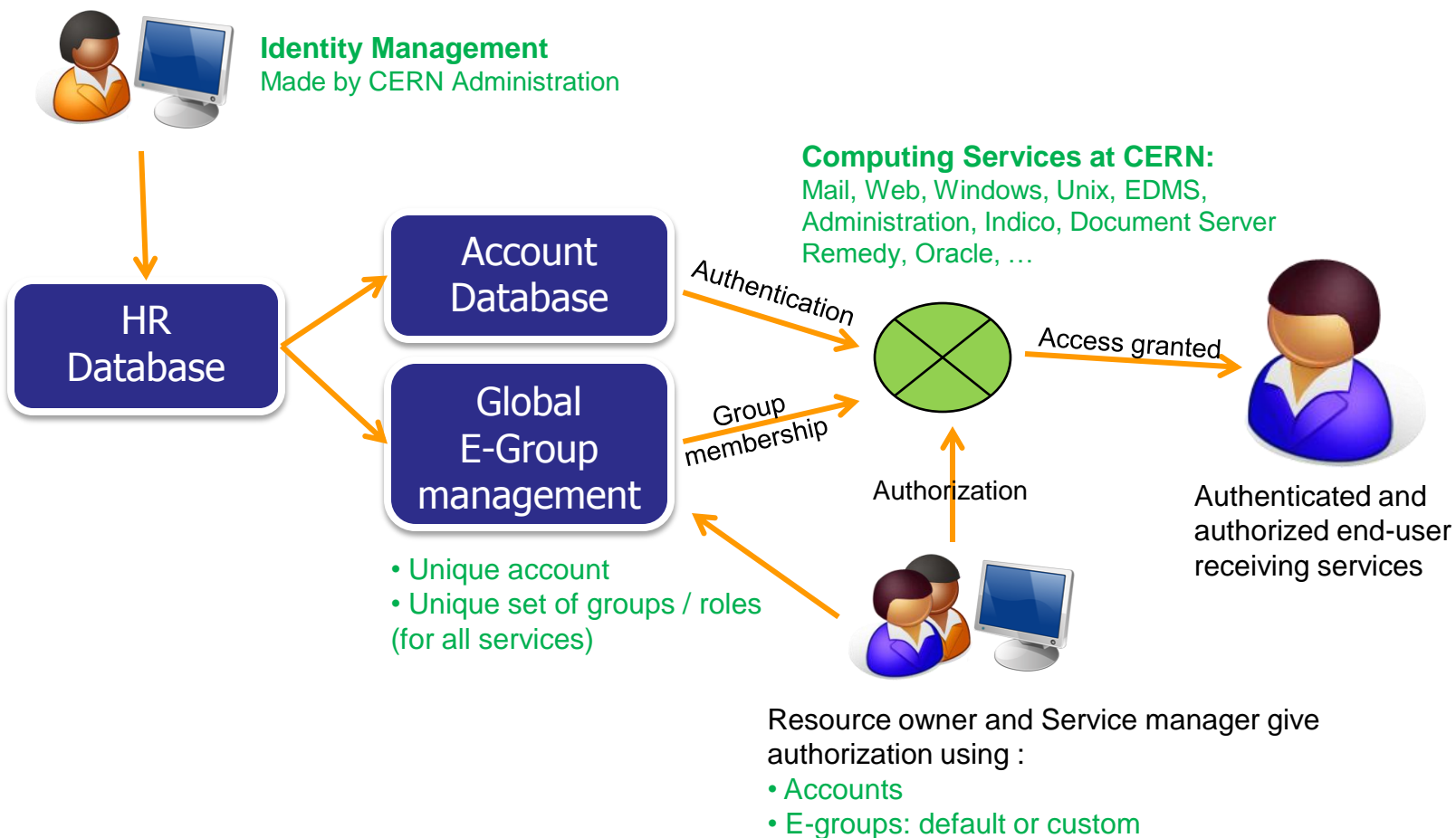
Service Providers

- **SSO 'clients'**
 - ◆ Allow identities to access Web Applications
 - ◆ IIS module, Apache module, or application module (i.e. Java)
- **Windows hosted Websites**
 - ◆ IIS (Internet Information Services) module comes with Windows 2003 R2.
- **Linux/Apache hosted Websites**
 - ◆ Shibboleth Apache module, Open Source project (Internet2)
- **IIS or Apache modules replace the basic authentication modules**
 - ◆ Transparent for the Application

Non Web applications

- **For NON Web ‘clients’**
 - ◆ **Use a SOAP Web Service**
 - To verify credentials
 - To get and verify group membership
 - ◆ **Requires some coding:**
 - Write a SOAP client
 - Send credentials and decode return codes
 - ◆ **Not a standard: a CERN made interface (but based on SOAP standard)**

- **Internet Services Websites are using SSO**
 - ◆ No major problems
- **Several pilots are running**
 - ◆ On many different platforms (Linux SLC, RedHat, Ubuntu, Solaris, Windows...)
 - ◆ For many different services
- **Clarify account management**
 - ◆ Cleanup to have only one account for all services
 - ◆ Use Roles to define resources access control
 - No more: “close NICE Account, keep Mail account, block AIS account”
 - But: “block Windows access, allow Mail access, block AIS access”.



- **Identity Management Plenary session**
 - ◆ 05-Sep-2007 at 08:30, by Alberto Pace
- **CERN Authentication**
 - ◆ <http://cern.ch/login>
- **Microsoft ADFS**
 - ◆ <http://technet2.microsoft.com/windowsserver/en/technologies/featured/adfs/default.aspx>
- **Shibboleth**
 - ◆ <http://shibboleth.internet2.edu>

Questions ? Comments ?

emmanuel.ormancey@cern.ch