CERN Single Sign On solution

Emmanuel Ormancey

System Architect, *CERN IT/IS*
CERN, Route de Meyrin, CH-1211 Geneva 23, Switzerland

E-mail: Emmanuel.Ormancey@cern.ch

Abstract. The need for Single Sign On has always been restricted by the absence of cross platform solutions: a single sign on working only on one platform or technology is nearly useless. The recent improvements in Web Services Federation (WS-Federation) standard enabling federation of identity, attribute, authentication and authorization information can now provide real extended Single Sign On solutions. Various solutions have been investigated at CERN and now, a Web SSO solution using some parts of WS-Federation technology is available. Using the Shibboleth Service Provider module for Apache hosted web sites and Microsoft ADFS as the identity provider linked to Active Directory user, users can now authenticate on any web application using a single authentication platform, providing identity, user information (building, phone...) as well as group membership enabling authorization possibilities. A typical scenario: a CERN user can now authenticate on a Linux/Apache website using Windows Integrated credentials, and his Active Directory group membership can be checked before allowing access to a specific web page.

1. Historical view

A few years ago, a typical CERN user had to authenticate many times using many different credentials during a simple work day.

First to unlock the Windows desktop a login and password was required, then he had to type in another login and password to unlock the Linux desktop or session. Reading mails was requiring again credentials, administrative applications as well, Indico to submit CHEP presentations, etc…

Today the situation is better, but still not optimal. Two credential pairs are still not synchronized, but a large number of applications are using the same credentials, authenticating using SOAP Web Services technology. This is an interesting benefit to the user, but this solution generated some unexpected side effects: as a result a few experiments and applications are stealing credentials ‘on the fly’ to populate local databases, in case the central services become unavailable or fail.

Note also that many experiments are still implementing their own identity management applications, with no connection to the central services at all. This leads to mismatches, errors, and generates frustration on the user’s part.

2. CERN Authentication

The CERN Authentication service mandate serves the purpose of providing Single Sign On for CERN Applications, using a unique central account database.

2.1. Main goals

The first problem to solve was to reduce the number of user databases. Reducing the number of login and password pairs to remember has a direct impact on user satisfaction and on security: it is easy to remember only one password, and it reduces the number of password reminder stickers found under user's keyboards (five credentials pairs mean five stickers with hand written passwords available under half the organization's keyboards!).

Centralizing the user database in one location avoid leaks and reduces potential security holes. It also helps to provide extended services like External Accounts management (using a lightweight registration process for non CERN users). CERN Users centralized database also provides Groups and Roles membership, to enhance access rights to resources.

Improving security was also the objective of this project, always following the idea that **complexity does not increase security**. The centralized database permits to block access to all applications for a user in one click. Users can use permissions and delegation to give access to resources instead of sharing credentials: shouting a password in a corridor is not anymore a sharing option!

2.2. Authentication methods and user information

The CERN Single Sign On infrastructure provides different authentication methods, with different security levels:

- Classic Web Forms, where you type in login and password. Depending on the browser features, login and password can be saved locally for later use.
- Windows Integrated authentication: the current Windows session token is reused to authenticate the user, without retyping credentials. Security of Windows desktop sessions was increased at the same time by the deployment of a strong screen lock policy: screen savers with password locking have been forced on all Windows desktops with a short timeout, to avoid users leaving their screens unlocked for long periods of time.
- Certificates: authentication can be made using a certificate provided by the CERN Certification Authority or any Grid trusted CA member. Depending on the security level required, Smartcard tokens with pin codes can also be used.

The calling application can select all or only some authentication methods. For example, Experiment Controls can request an authentication using Certificates on Smartcards only for their operators to ensure maximum verification.

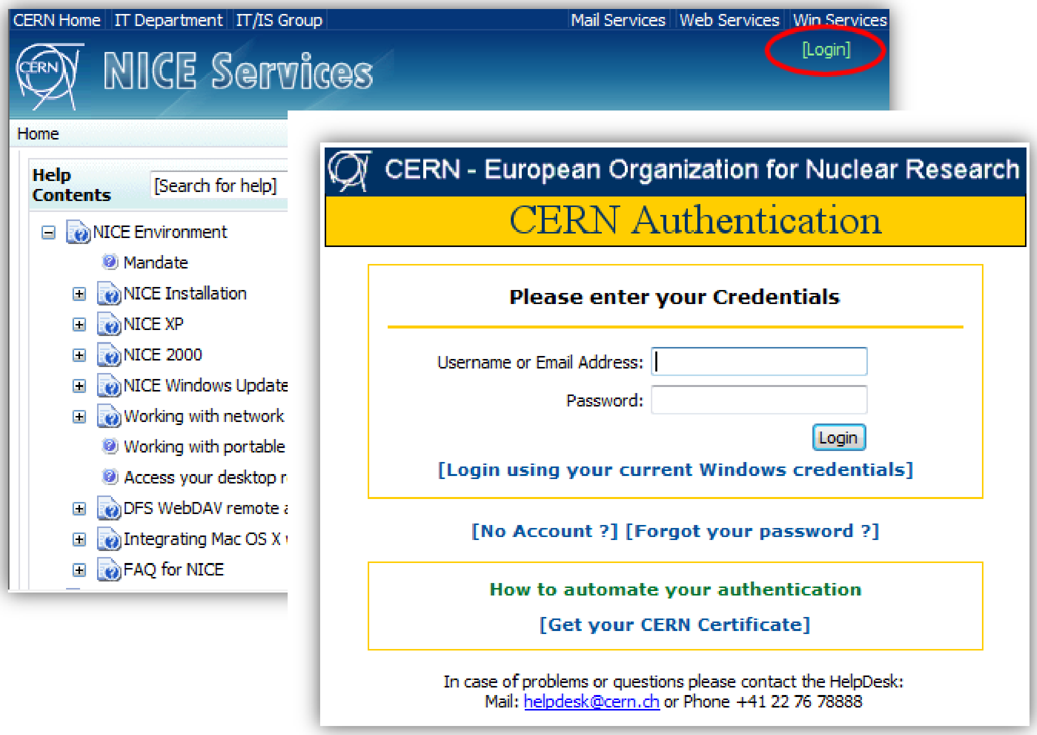
Providing a Single Sign On infrastructure can also help to provide user information needed for calling applications. All account information associated to the current user is returned to the calling application: name, email, building, etc…

The Groups and Mailing lists membership are also returned, so that the calling application can rely on central group membership to handle access control. We no longer have 'per application dedicated role system' but a centrally managed group management on which all applications can rely.

2.3. Authentication overview

The following screenshots show briefly the user experience when using the CERN Single Sign On service.

The user opens a Web site requiring authentication, and is then redirected to the Single Sign On form. From the application, his details and groups membership are available and can be used for example to restrict access to some pages. Finally, clicking on the Logout button will disconnect the user from all currently opened applications.


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

NICE Services [Login]

Home

Help Contents [Search for help]

- NICE Environment
  - Mandate
  - NICE Installation
  - NICE XP
  - NICE 2000
  - NICE Windows Update
  - Working with network
  - Working with portable
  - Access your desktop r
  - DFS WebDAV remote a
  - Integrating Mac OS X
  - FAQ for NICE

CERN - European Organization for Nuclear Research

CERN Authentication

Please enter your Credentials

Username or Email Address: |

Password:

Login

[Login using your current Windows credentials]

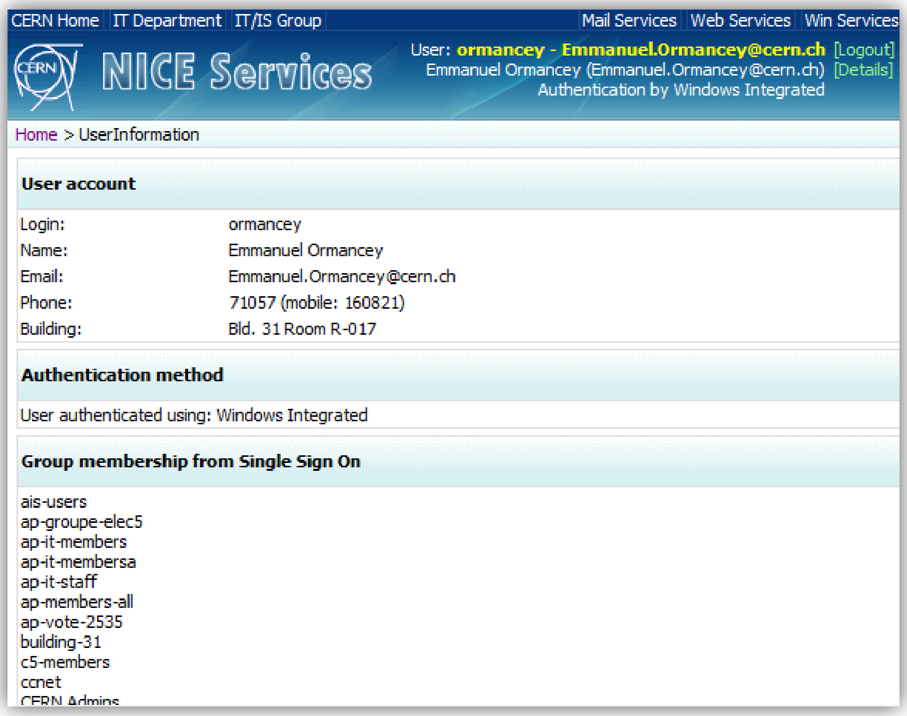
[No Account ?] [Forgot your password ?]

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

Figure 1. A Web application requires authentication, the Single Sign On authentication form is displayed


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

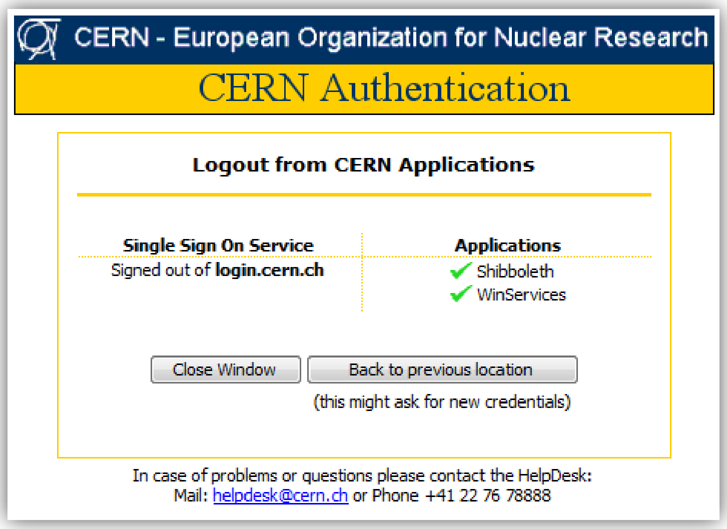
Authentication method

User authenticated using: Windows Integrated

Group membership from Single Sign On

ais-users
ap-groupe-elec5
ap-it-members
ap-it-membersa
ap-it-staff
ap-members-all
ap-vote-2535
building-31
c5-members
ccnet
CERN Admins

Figure 2. The calling application has user attributes and group membership information available



CERN - European Organization for Nuclear Research

CERN Authentication

Logout from CERN Applications

Single Sign On Service	Applications
Signed out of **login.cern.ch**	✓ Shibboleth ✓ WinServices

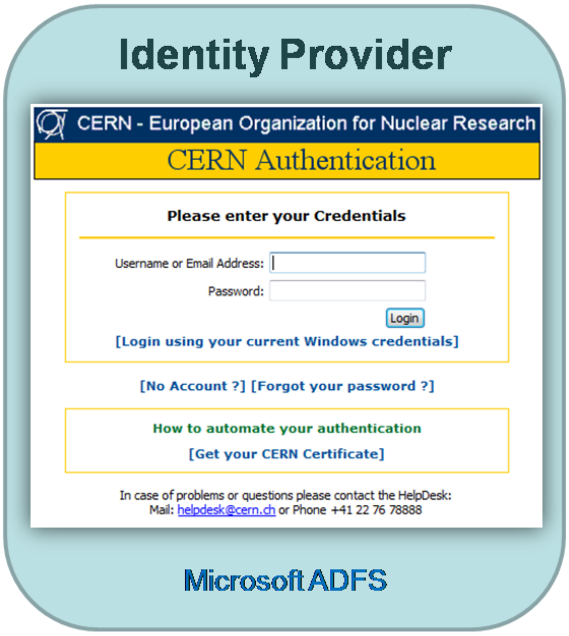
(this might ask for new credentials)

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

Figure 3. Logout from Single Sign On also logout from applications

3. Technical background

The CERN Single Sign On system has two components: the Identity Provider and the Service Provider.



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 ?]

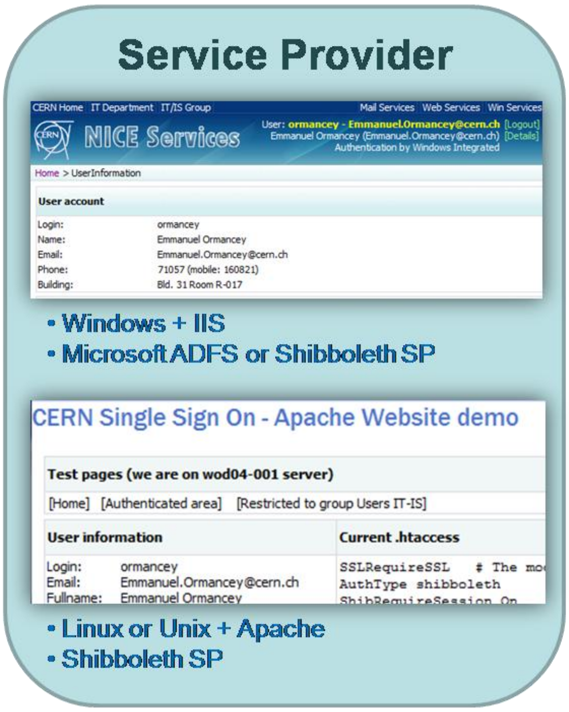
How to automate your authentication

[Get your CERN Certificate]

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

Microsoft ADFS

Figure 4. Identity Provider, where the user enters credentials



Service Provider

User: ormancey - Emmanuel.Ormancey@cern.ch
Emmanuel Ormancey (Emmanuel.Ormancey@cern.ch)
Authentication by Windows Integrated

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 Email: Emmanuel.Ormancey@cern.ch Fullname: Emmanuel Ormancey	SSLRequireSSL # The mo AuthType shibboleth ShibRequireSession On

- Linux or Unix + Apache
- Shibboleth SP

Figure 5. Service Provider, the calling application where the user details can be used

3.1. Identity Provider

The Identity Provider (IdP) checks identity of the users, supporting various authentication methods. It can be seen as the server side of the Single Sign On service.

It verifies credentials and loads user information for the calling application, using so-called 'Claims' or 'Attributes'. Note that each application can retrieve a different set of attributes, depending on the confidentiality level required.

CERN implementation of the Identity Provider is Microsoft ADFS based: Active Directory Federation Services is an extension of Microsoft Active Directory central authentication database, using the WS-Federation Passive Requester Profile (WS-F PRP) standard, SOAP Web Services based: http://technet2.microsoft.com/windowsserver/en/technologies/featured/adfs/default.mspx.

The production service is hosted in CERN Computer Center critical area, on load balanced servers to minimize downtime as authentication is a highly critical service.

3.2. Service Providers

The Service Provider (SP) is the client side of the Single Sign On service. It allows identities to access web Applications after they have been successfully verified with the Identity Provider.

The Service Provider can be a Microsoft Internet Information Service (IIS) module, an Apache module or an application module (for example some Java classes).

On Windows and IIS hosted Websites, an IIS ADFS module comes with Microsoft Windows 2003 R2 version as a additional component. It can easily replace an existing authentication system using basic or NTLM authentication.

On Linux, Unix and Apache hosted Websites, the Shibboleth Apache module can be used. Shibboleth is an Open Source middleware software: http://shibboleth.internet2.edu. The upgrade is quite simple, as the classic Apache configuration files for access control are still used and can be kept; only the authentication module needs to be replaced.

In both cases, moving to Single Sign On solution is a straight forward procedure, with only small configuration changes, and it's transparent for all applications relying on the default authentication systems provided by Web servers.

3.3. Non Web Applications

For applications that are not Web based, the CERN Single Sign On classic service cannot be used. For these specific cases, the CERN Single Sign On service provides a dedicated SOAP Web Service that can be used to verify credentials and retrieve user information as well as group memberships.

This specific service requires some coding on the client side: a SOAP client, sending credentials to the Web Service and decoding return codes accordingly is required. Note that this implementation is not standard, but a CERN specific implementation based on SOAP standards.

4. Conclusion: The Next Steps

Today many CERN Central services are already using the Single Sign On service, mainly on Windows and Linux platforms.

Several pilots are also running on different Linux distributions as well as on Solaris, for different services, and there is a fast growing interest for this service. The fact that interaction between Windows and Unix is working opens many possibilities, and is finally the only way to achieve a real viable Single Sign On Solution.

As a parallel task, CERN also needs to improve and clarify account managements. Cleanup must be done, reducing to only one account per user for all services, and finally a big improvement must be done to use centrally managed roles to define resources access control.

Figure 6. *Identity Management at CERN* below is showing the overall view of account, groups and roles management. For more details on this concept, see Reference [4] - Alberto Pace, CERN: Identity Management (Chep 2007 Plenary session).

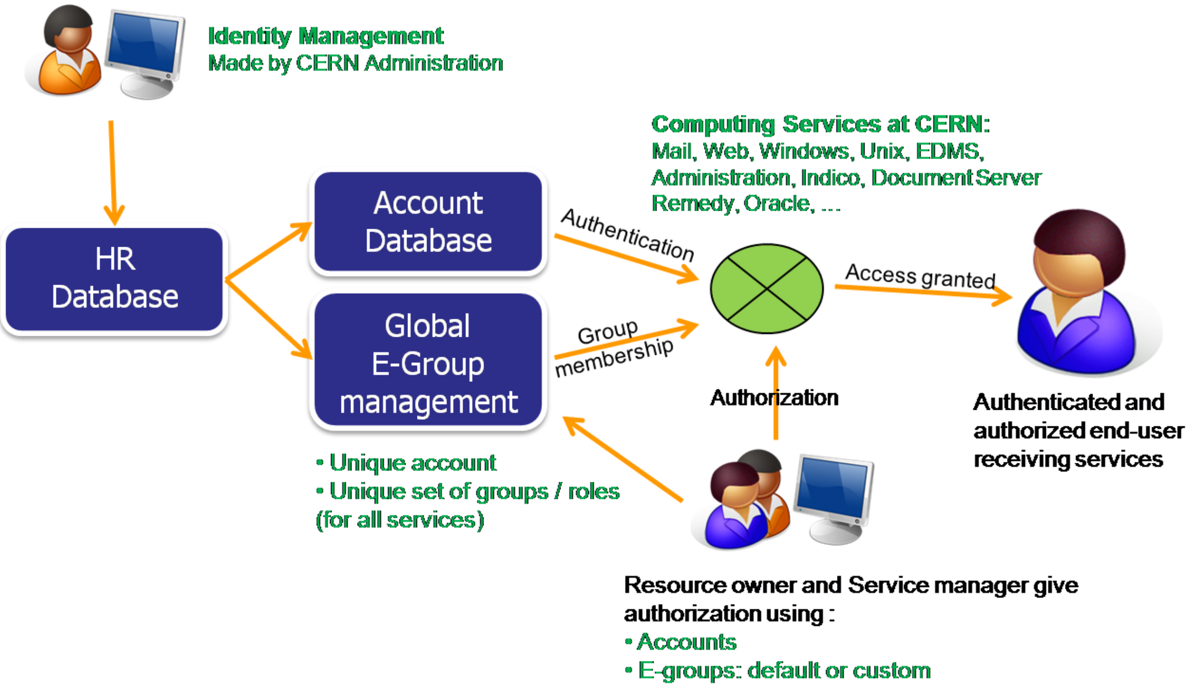

Identity Management
Made by CERN Administration
HR Database
Account Database
Global E-Group management
• Unique account
• Unique set of groups / roles (for all services)
Computing Services at CERN:
Mail, Web, Windows, Unix, EDMS, Administration, Indico, Document Server Remedy, Oracle, ...
Authentication
Group membership
Access granted
Authorization
Authenticated and authorized end-user receiving services
Resource owner and Service manager give authorization using :
• Accounts
• E-groups: default or custom

Figure 6. Identity Management at CERN

References

[1] CERN Authentication: http://cern.ch/login

[2] Shibboleth: http://shibboleth.internet2.edu

[3] Microsoft ADFS: http://technet2.microsoft.com/windowsserver/en/technologies/featured/adfs/default.mspx

[4] Alberto Pace, CERN: Identity Management (Chep 2007 Plenary session): http://indico.cern.ch/contributionDisplay.py?contribId=54&amp;confId=3580