

**GARR**

The Italian Academic & Research Network



www.garr.it

# Moodle federato: La federazione IDEM-GARR a supporto della formazione on line

**Maria Laura Mantovani**

GARR e Università di Modena e  
Reggio Emilia

marialaura.mantovani@garr.it

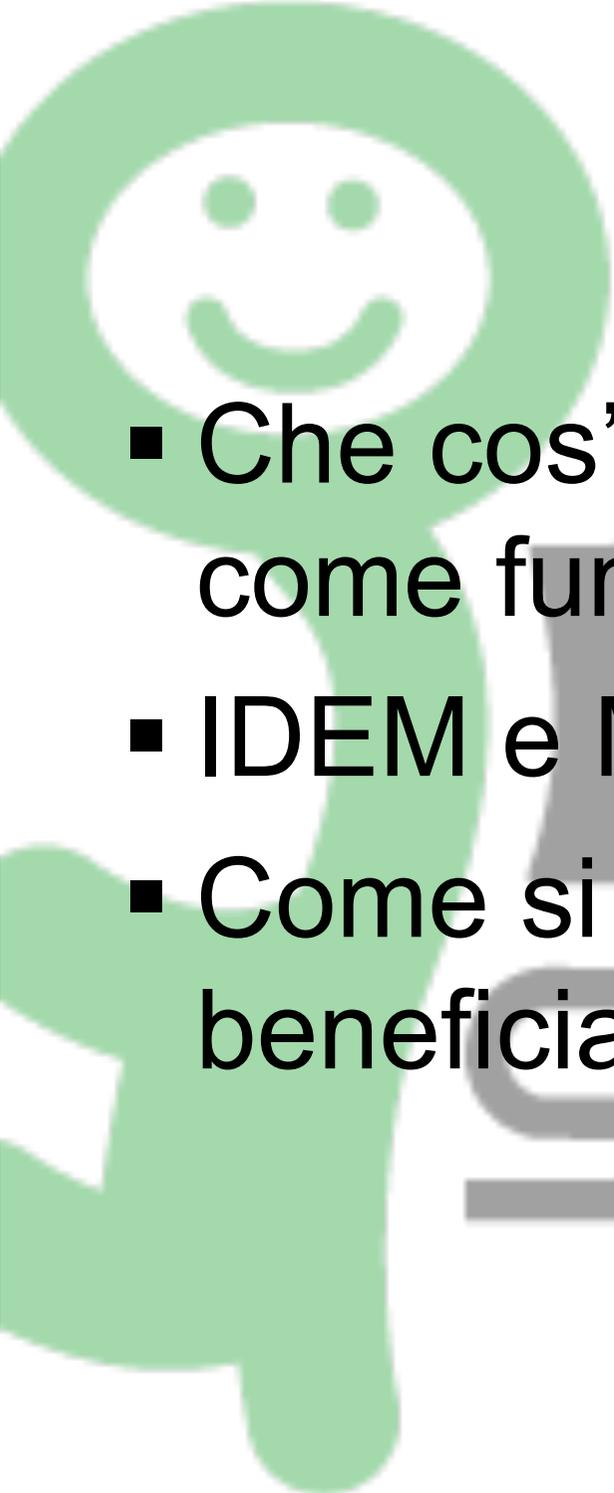


**Sandro Tumini**

Università Politecnica  
delle Marche

s.tumini@univpm.it

Convegno MoodleMoot 2013 - Ancona, 20.9.2013



# Agenda

- Che cos'è la Federazione IDEM e come funziona
- IDEM e Moodle
- Come si configura Moodle per beneficiare di IDEM

Quali sono le mie credenziali per entrare?



# Accesso ai servizi nel modo tradizionale

- Problemi connessi all'avere numerosi codici di accesso distinti per ogni servizio
  - compilare moduli
  - rilasciare i propri dati ad ogni nuovo servizio a cui si accede
  - i dati non vengono aggiornati
  - i servizi hanno un notevole carico di lavoro nella gestione delle utenze



# Accesso tramite un sistema federato

- In un **sistema federato** l'utente ha una sola coppia di credenziali, quelle istituzionali, che usa per accedere a tutti i servizi federati sia interni che esterni
  - riduce il rischio di smarrimento, furto e scambio di identità
- Il codice di accesso è gestito dall'istituzione di appartenenza dell'utente
  - non è gestito da estranei
  - dati non usati abusivamente

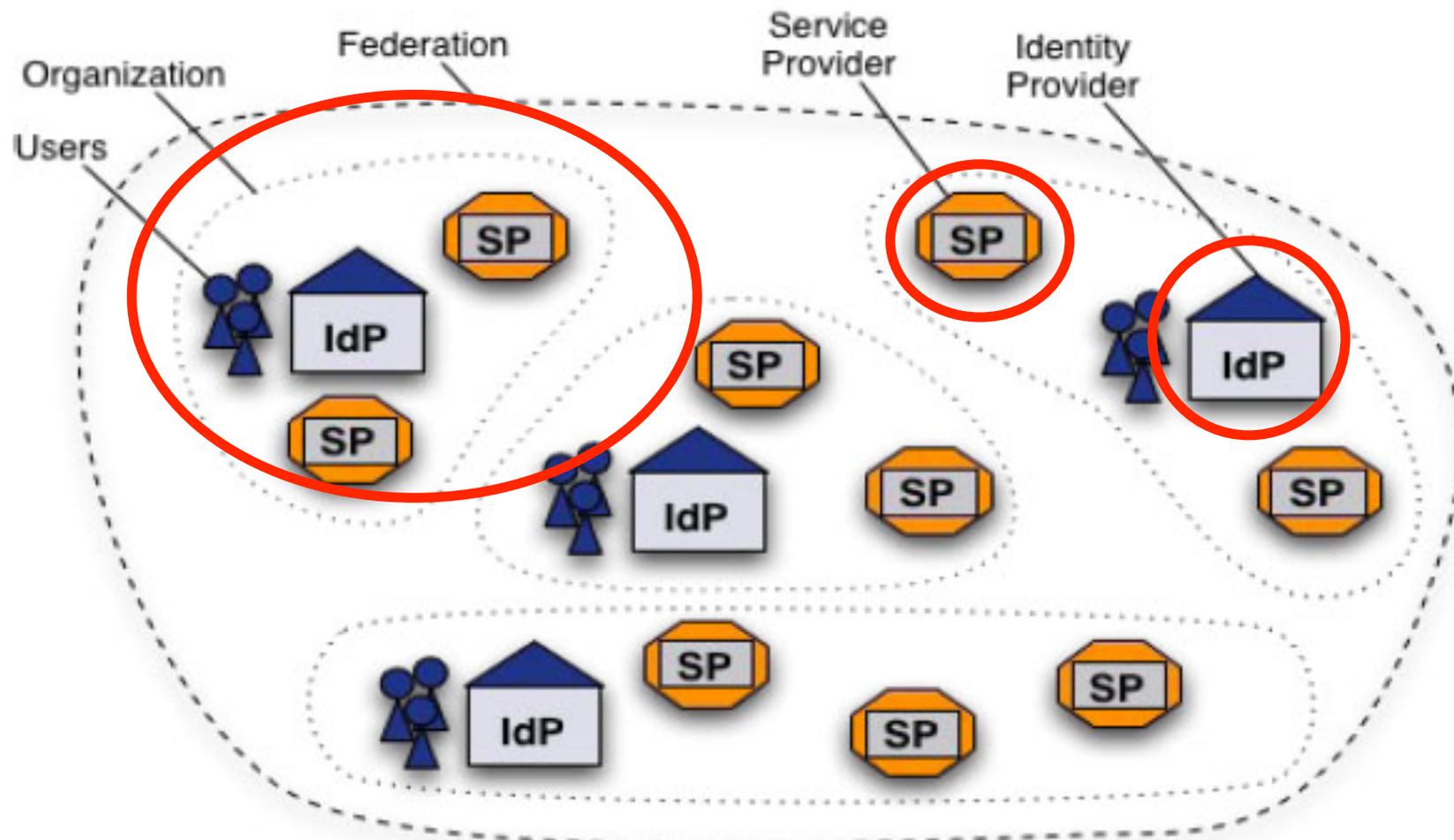


# Come funziona l'accesso federato?

- Accordo tra istituzioni e fornitori di servizi basato su regole e linee di condotta per gestire le relazioni di fiducia
- Implementato con soluzioni tecnologiche basate su SAML2 per lo scambio sicuro delle informazioni sulle identità degli utenti tra le istituzioni (**Identity Provider** – *idp*) e i servizi (**Service Provider** – *sp*)



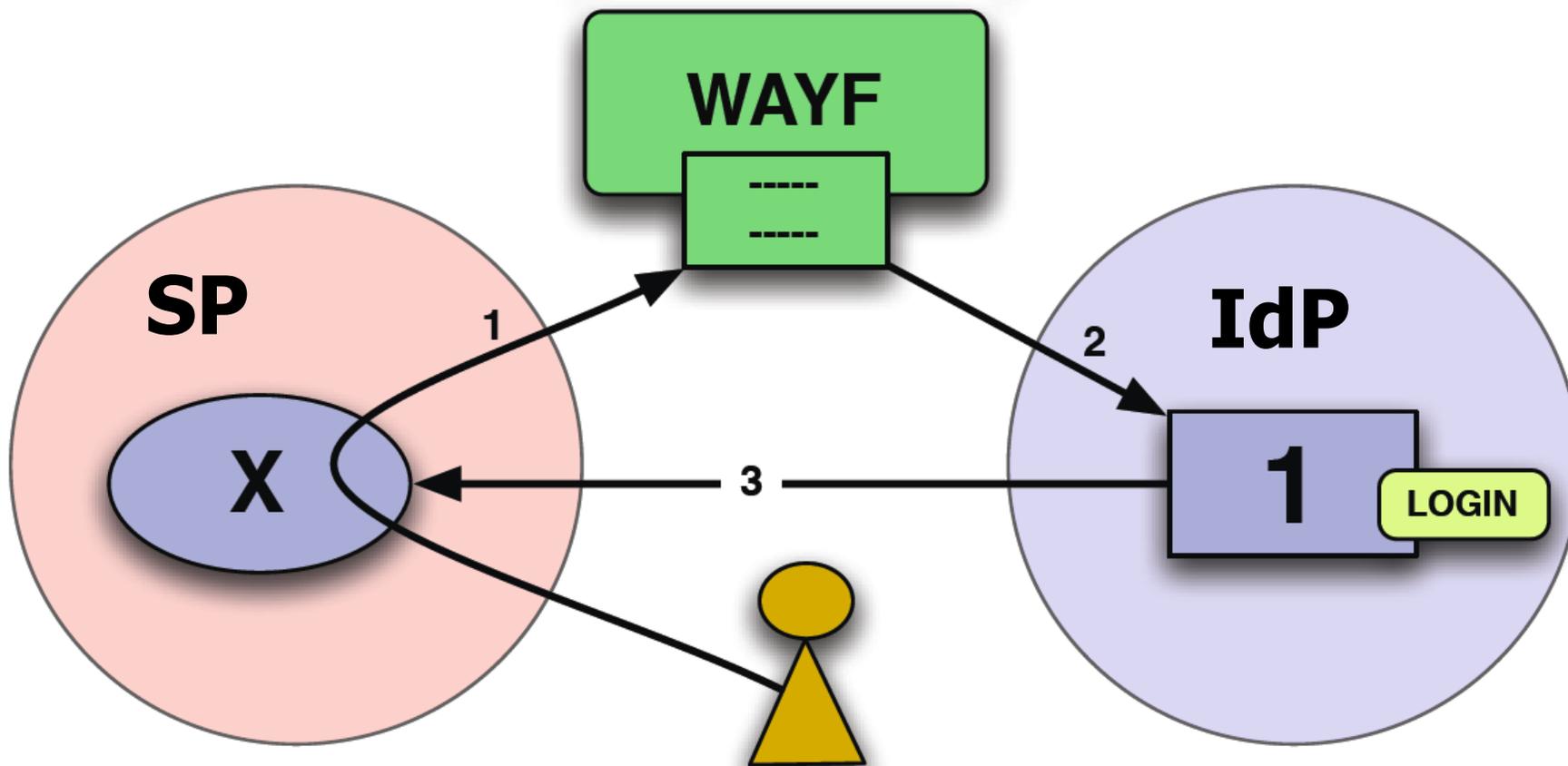
# Federazione: Organizzazioni, Persone, Identity Provider, Service Provider



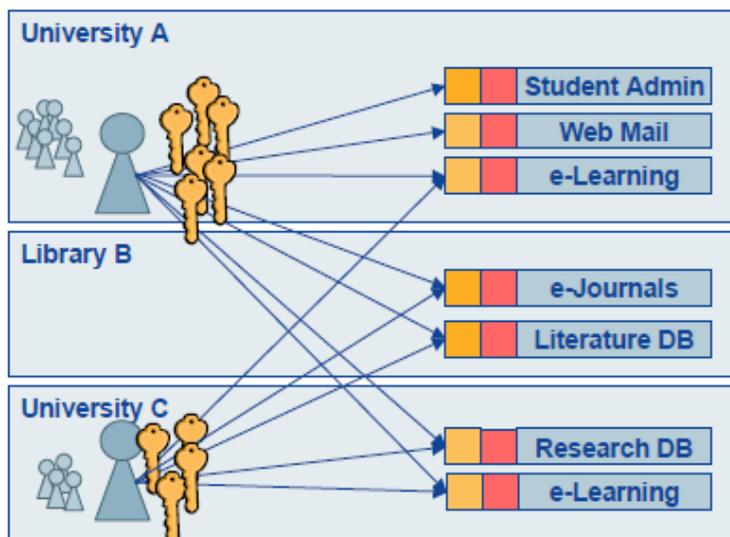
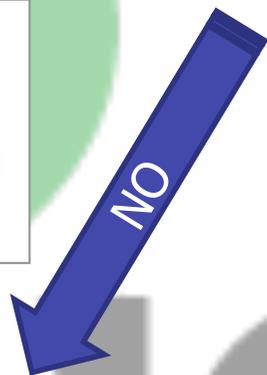
# Come funziona l'identità digitale e l'accesso federato

**Service**

**Institution**



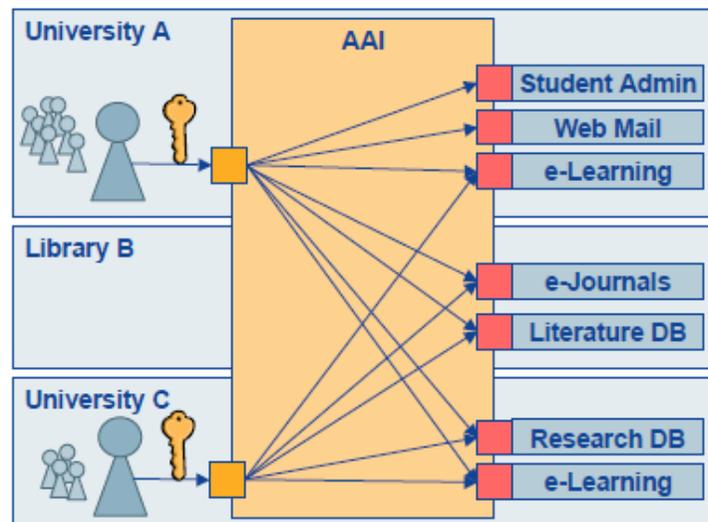
# L'identità digitale e l'accesso federato



User Administration  
Authentication

Authorization

Resource



User Administration  
Authentication

Authorization

Resource

(© SWITCH, CH).

## Quali sono i vantaggi

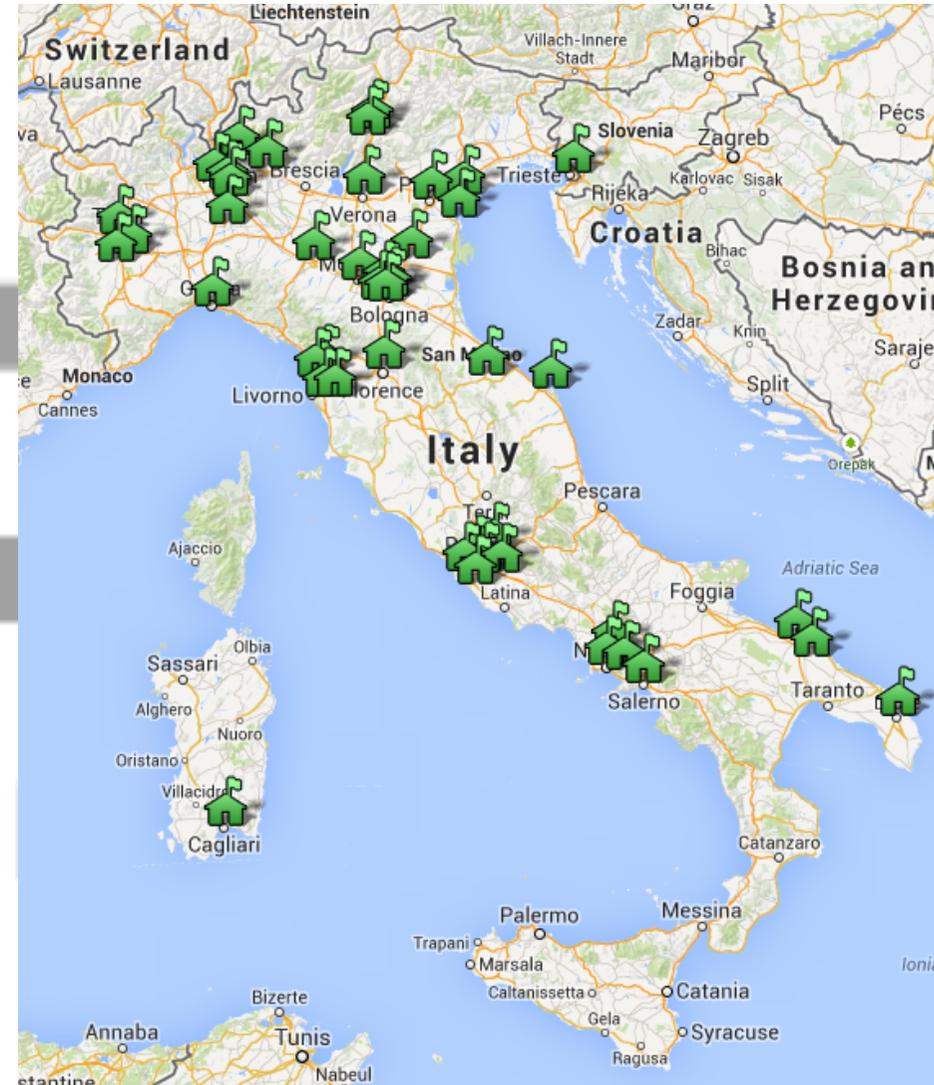
- Le informazioni sull'utente sono mantenute e conosciute solo dall'istituzione a cui l'utente è affiliato
- Unico punto centrale di gestione delle identità
- Sp e Idp non condividono informazioni personali sull'utente ma solo informazioni sul diritto o meno di accesso alle risorse: **gli attributi**
- Permette di ridurre l'uso illegittimo di servizi offerti tramite abbonamento
- Riduce il carico di lavoro per la gestione delle credenziali che attualmente grava sul personale

# IDEM:

dislocazione dei fornitori di e-identità (IDP)

I numeri della federazione:

- **59 IDPs**
  - 47 in federazione
  - 12 in test
- **~3.000.000 end users**





Forse nella vostra organizzazione esiste già un Identity Provider?

- <https://www.idem.garr.it/servizi/idp>

idem  
garr

# Moodle: uno strumento utile per:

Favorire lo sviluppo e la gestione di servizi federati e inter-istituzionali per ottimizzare le risorse.

- Esempi:

- Didattica on-line
- Corsi rivolti al personale Tecnico-Amministrativo
- Corsi per le Scuole di Dottorato

# MOODLE IN GARR AAI

The screenshot shows a web browser window displaying the LearningGARR Moodle course page. The browser's address bar shows the URL <https://learning.garr.it/learning/>. The page header includes the LearningGARR logo and a user login status: "Sei collegato come Maria Laura Mantovani. (Esci)".

The main content area features a navigation menu on the left with "Home" and "Pagine del sito". Below this, there are sections for "Impostazioni" (with "Il mio profilo" link), "Videotutorial" (listing "ADOBE CONNECT", "MOODLE", and "FORUM"), and "Corsi". The "Corsi" section is expanded to show a list of courses under the "RETI" category, which is highlighted with a red box. The courses listed are:

- Webinar IPv6 6 Giugno 2012
- IPv6: dalla teoria alla pratica per gli amministratori di rete

Below the course list, there are sections for "Manuale Moodle" (with an "Installa Firefox" button), "News del sito", and "Corsi INTERNI ALLA DIREZIONE GARR" (with "Asterisk" listed). On the right side, there is a "Calendario" for September 2013 and a "Navigazione" menu with links to "Home", "My home", "Pagine del sito" (including "Blog" and "Tag"), and "News del sito".

A large red watermark is overlaid diagonally across the page, reading: "Rivolto ad utenti sparsi su tutto il territorio italiano... è probabile che abbiano già l'identità federata".

# MOODLE IN GARR AAI

**Ciao, sei ritornato?**

Per effettuare il login mediante il sistema di Single Sign On GARR clicca sull'icona qui di seguito. (Nella schermata successiva scegli "Consortium GARR SSO" come Identity Provider)

**È la prima volta che accedi qui?**

L'accesso a questo portale avviene mediante GarrSSO, il sistema di autenticazione ed autorizzazione **Single-Sign-On** GARR.

Una volta ottenuto un account potrai accedere, con una singola chiave, inserita una volta sola per sessione, a questo e ad **altri servizi** offerti da GARR e dai suoi partner. Il tutto evitandoti di compilare altri form di registrazione e razionalizzando l'organizzazione delle tue applicazioni in una **dashboard personale**.

Se ancora non hai un account, puoi registrarti qui

> [Registrazione al Corso IPv6](#)

> [Registrazione al Corso IPv6 \(per chi ha un account su Learning GARR\)](#)

*Il link di registrazione è valido anche nel caso in cui avessi già un account GarrSSO, magari utilizzato per accedere altre applicazioni del sistema, ma non ancora abilitato all'accesso a questo servizio specifico. In tal caso il processo di registrazione ti guiderà verso una semplice procedura di richiesta delle autorizzazioni necessarie.*

**Selezioni la sua Home Organisation**

È necessario autenticarsi per poter accedere alla risorsa sull' host 'learning.garr.it'.

GARR  
GARR  
ISTAT  
Istituto Nazionale di Fisica Nucleare  
Istituto Nazionale di Astrofisica - INAF  
Politecnico di Milano  
SISSA  
Seconda Università di Napoli  
Servizio Informatico di Ateneo - UnivPM  
Università di Bergamo  
Università di Bologna  
Università di Camerino  
Università di Ferrara  
Università di Genova  
Università di Milano-Bicocca  
Università di Roma TRE  
Università di Salerno  
Università di Trieste  
Università di Torino  
Universita' di Verona  
Università Ca Foscari di Venezia

**Consortium GARR Identity Provider Login**

Username: mantovani  
Password: [masked]  
[Reset my attribute release approvals](#)  
Login

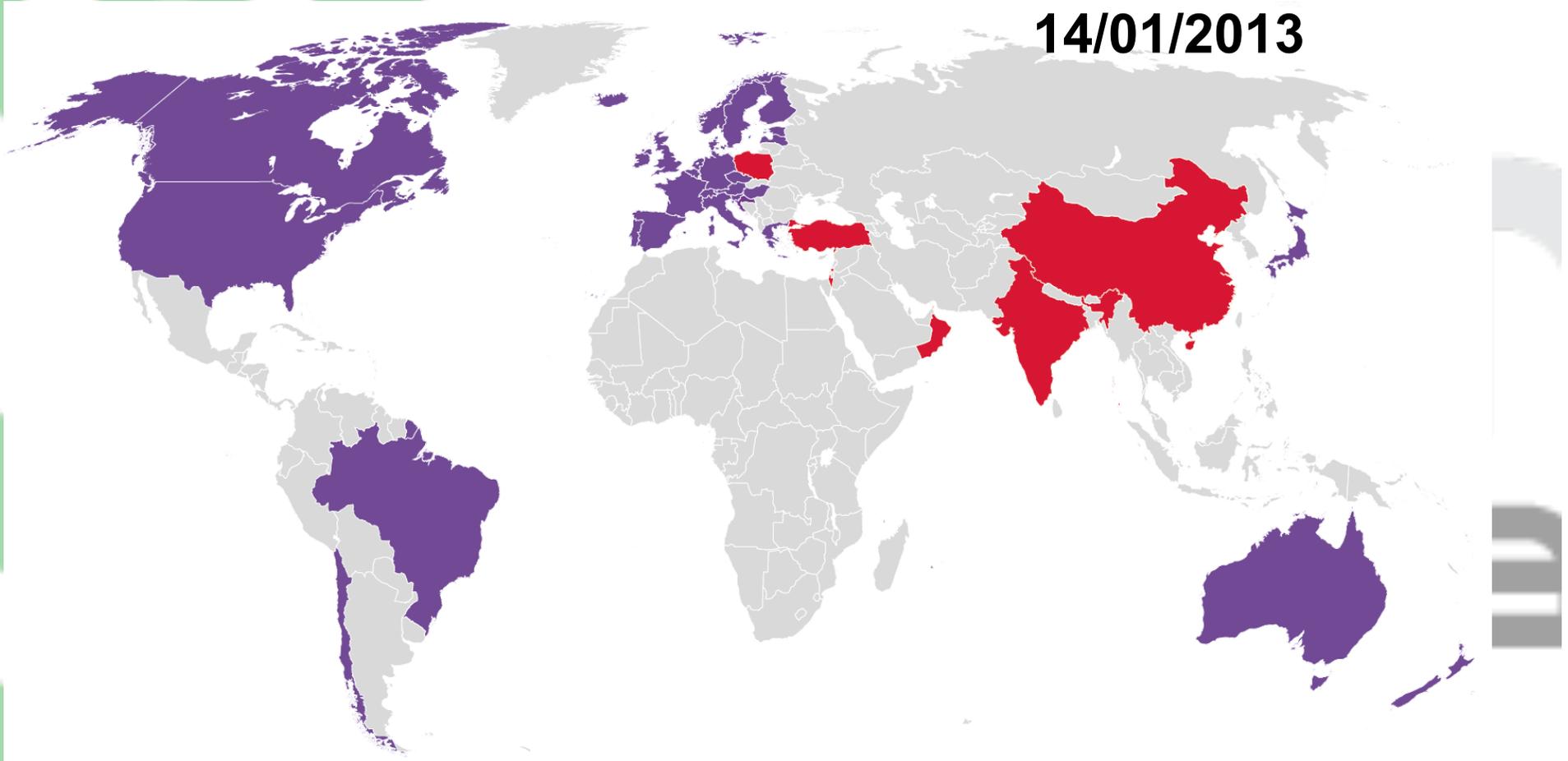
**Maria Laura Mantovani**

Istituzione: Consortium GARR  
Indirizzo email: marialaura.mantovani@garr.it  
Profili corso: IPv6: dalla teoria alla pratica per gli amministratori di rete  
Primo accesso: Saturday, 12 February 2011, 16:06 (2 anni 216 giorni)  
Accesso più recente: Monday, 16 September 2013, 13:16 (38 secondi)



# Federations in the world

**Last update  
14/01/2013**



# SHIBBOLETH CONSORTIUM:

“open source software package for web single sign-on adopted by research and education communities worldwide”



Shibboleth - Windows Internet Explorer

http://shibboleth.net/

HOME | ABOUT | DOWNLOADS | DOCUMENTATION



## Shibboleth.

Consortium Products Community What's Shibboleth? Join Now

**Shibboleth is among the world's most widely deployed federated identity solutions, connecting users to applications both within and between organizations. Every software component of the Shibboleth system is free and open source.**

Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

### Latest News

- Shibboleth SP V2.5.2 Available, Security Advisory Issued - 18 June 2013
- Shibboleth Consortium officially launched - 15 May 2013
- Shibboleth IdP V2.4.0 Available - 17 April 2013
- Shibboleth SP V2.5.1 Available - 10 December 2012
- Gluu and Shibboleth Consortium Finalize Partnership - 12 October 2012

## Link di riferimento

# <http://shibboleth.net/>

<b>Consortium</b> <ul style="list-style-type: none"><li>Members</li><li>Consortium Board</li><li>Documents</li><li>Membership Benefits</li><li>Membership Fees</li><li>Join Now</li></ul>	<b>Products</b> <ul style="list-style-type: none"><li>Centralized Discovery Service</li><li>Embedded Discovery Service</li><li>Identity Provider</li><li>Metadata Aggregator</li><li>OpenSAML-C++</li><li>OpenSAML-Java</li><li>Service Provider</li></ul>	<b>Community</b> <ul style="list-style-type: none"><li>News &amp; Events</li><li>Mailing Lists</li><li>Shibboleth Wiki</li><li>Feature &amp; Bug Tracking</li><li>Security Advisories</li><li>Roadmap</li><li>Commercial Support</li></ul>	<b>About</b> <ul style="list-style-type: none"><li>What's Shibboleth</li><li>How Shibboleth Works</li><li>The Team</li><li>Contact Us</li></ul>
---	--	--	---

http://shibboleth.net/ 100%

Browser window: Ims.univpm.it: Amministrazione: Plugin: Autenticazione: Shibboleth - Windows Internet Explorer

URL: https://ims.univpm.it/admin/auth\_config.php?auth=shibboleth&adminedit=1

### Moodle 2.5 - Portale di E-Learning dell'Università Politecnica delle Marche

Sei collegato come Sandro Tumini. (Eso)

Home ► Amministrazione del sito ► Plugin ► Autenticazione ► Shibboleth

Termina modifica blocchi

#### Navigazione

Home

- My home
- Pagine del sito
- Il mio profilo
- Corsi

#### Segnalibri amministratore

Aggiungi questa pagina nei tuoi segnalibri

#### Amministrazione

- Impostazioni profilo
- Amministrazione del sito
  - Notifiche
  - Registrazione
  - Funzionalità avanzate
  - Utenti
  - Corsi
  - Valutazioni
  - Badge
  - Localizzazione
  - Lingua
  - Plugin
    - Panoramica plugin
    - Installazione plugin
    - Moduli attività
    - Plugin compito
    - Formati dei corsi
    - Blocchi
    - Instradamento
    - messaggi
    - Autenticazione
      - Gestione autenticazione
      - Server LDAP
      - Account manuali
      - Account

Utilizzando questo metodo gli utenti vengono creati e autenticati utilizzando Shibboleth

Username: <input type="text"/>	Nome
API per la modifica dei dati: <input type="text"/>	Puoi usare queste API per modificare ulteriormente i dati forniti da Shibboleth. Per maggiori informazioni, leggi <a href="#">README</a>
Servizio Moodle WAYF: <input type="checkbox"/>	E' possibile consentire a Moodle di usare i propri servizi WAYF al posto di quelli configurati per Shibboleth. In questo caso Moodle visualizzerà un menù a discesa dove l'utente potrà scegliere la pagina di login.
Identity provider: <input type="text" value="urn:mace:organization1:providerID, Example Organization 1"/>	Inserite un elenco di Identity Provider entityID tra cui l'utente potrà scegliere nella pagina di login. Su ogni riga dovrà essere presente una coppia separata da virgole composta da entityID dell'IdP (verifica il metadato file di Shibboleth) e dal Nome dell'IdP (il nome comparirà nel menù a discesa). E' possibile aggiungere un terzo parametro opzionale dove specificare la posizione del session initiator di Shibboleth utile nel caso in cui l'installazione di Moodle faccia parte di una multi federazione.
Shibboleth Service Provider logout handler URL: <input type="text"/>	Inserite l'URL del logout handler del Service Provider Shibboleth. In genere l'URL è /Shibboleth.sso/Logout
Logout return URL alternativa: <input type="text"/>	Inserite l'URL dove gli utenti Shibboleth saranno indirizzati dopo il logout. Se l'URL non viene inserita, allora gli utenti saranno indirizzati alla URL dove Moodle indirizza gli utenti.
Nome del metodo di autenticazione: <input type="text" value="Shibboleth Login"/>	Inserite un nome familiare ai vostri utenti per identificare il metodo di autenticazione Shibboleth. Un nome adatto potrebbe essere il nome della vostra federazione Shibboleth, ad esempio SWITCHaai Login oppure InCommon Login.
URL per cambiare password: <input type="text"/>	L'indirizzo della pagina dove gli utenti possono recarsi per cambiare o recuperare la propria password. L'indirizzo sarà raggiungibile tramite un pulsante presente nella pagina di login e nel profilo utente. Se l'indirizzo viene lasciato vuoto, il pulsante non verrà visualizzato.

Mappatura dei dati

Nome <input type="text"/>	Aggiorna dati interni <input type="text" value="Solo al primo accesso"/>	Campi bloccati nel profilo utente <input type="text" value="Libero"/>
Cognome <input type="text"/>	Aggiorna dati interni <input type="text" value="Solo al primo accesso"/>	Campi bloccati nel profilo utente <input type="text" value="Libero"/>
Indirizzo email <input type="text"/>	Aggiorna dati interni <input type="text" value="Solo al primo accesso"/>	Campi bloccati nel profilo utente <input type="text" value="Libero"/>

**Shibboleth**

**Gestione autenticazione**

## Modulo già presente di default in moodle

## PER GLI UTENTI:

**Login to Moodle via Shibboleth**

---

For authentication via Shibboleth, please select your organization from the drop down list:

I'm a member of ...

In case you are not associated with the given organizations and you need access to a course on this server, please contact the [Moodle Administrator](#).

---

Some courses may allow guest access

---

You are not logged in. ([Login](#))

### Possibile esempio di Attributi Richiesti:

Per poter effettuare il login sul portale Moodle attraverso IDEM, e' necessario che l'Identity Provider rilasci gli attributi obbligatori indicati da IDEM:

**eduPersonTargetedID;**

**eduPersonScopedAffiliation;**

**E' inoltre necessario che l'Identity Provider fornisca alcuni attributi supplementari. In particolare:**

- **cn (userName);**
- **sn (cognome);**
- **givenName (nome);**
- **mail (e-mail).**

**Questi attributi sono necessari per l'identificazione dell'utente e per gestire l'utilizzo del servizio.**

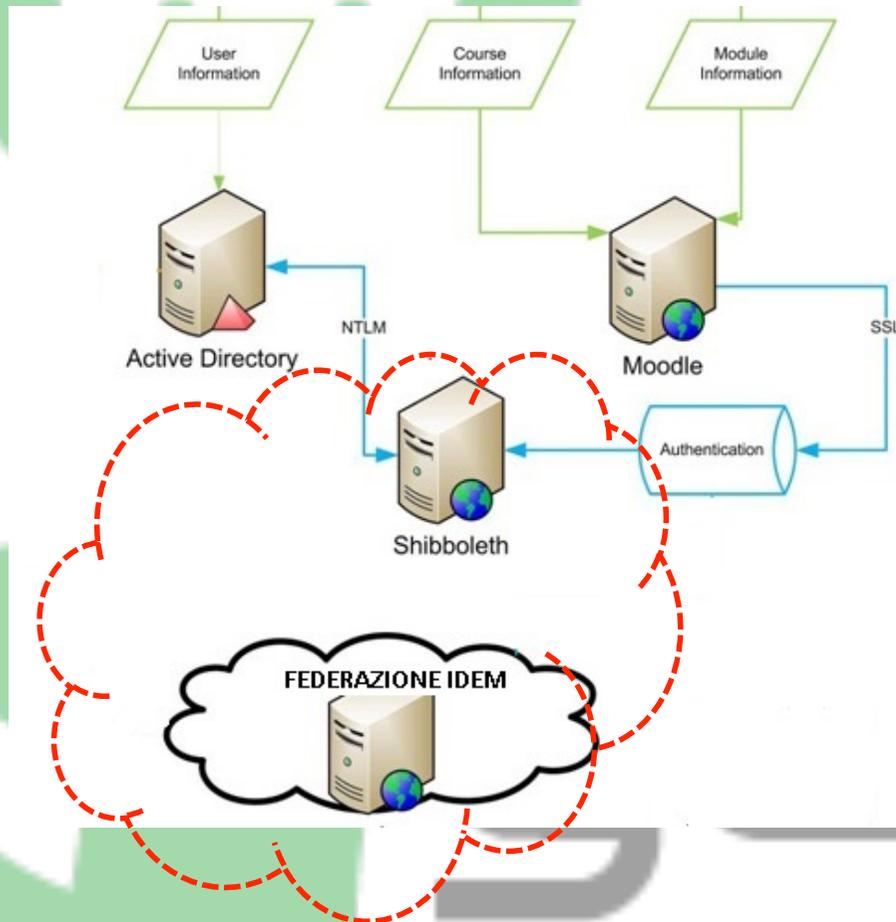
## PER GLI AMMINISTRATORI >>>>>

HOW TO INSTALL AND CONFIGURE SHIBBOLETH MODULE:

<https://github.com/moodle/moodle/tree/master/auth/shibboleth>

# Moodle UnivPM-Shibboleth:

This feature is coming soon



## VANTAGGI

La procedura di Single Sign-On è intrinsecamente sicura dato che:

1. Utilizza il protocollo https per la comunicazione criptata della password;
2. Separa la fase di autenticazione da quella di autorizzazione, ciò significa che tutte le credenziali (username e password) per l'accesso vengono gestite da un solo server, quello del SSO, mentre i server che gestiscono i servizi (ad es. moodle) vengono sgravati dall'onere della sicurezza degli accessi perché non vengono nemmeno a conoscenza di tali informazioni;

3. Inoltre il server che gestisce il Single Sign-On è ospitato in un data center sicuro sia dal punto di vista fisico-ambientale che dal punto di vista

Grazie per l'attenzione!  
All Info: <https://www.idem.garr.it>

