

# **Registrare un SP nella Federazione GARR IDEM e in eduGAIN**

Corso IDEM: Abilitare le applicazioni web al  
Single Sign-on con strumenti SAML

Roma, 30.09.2014

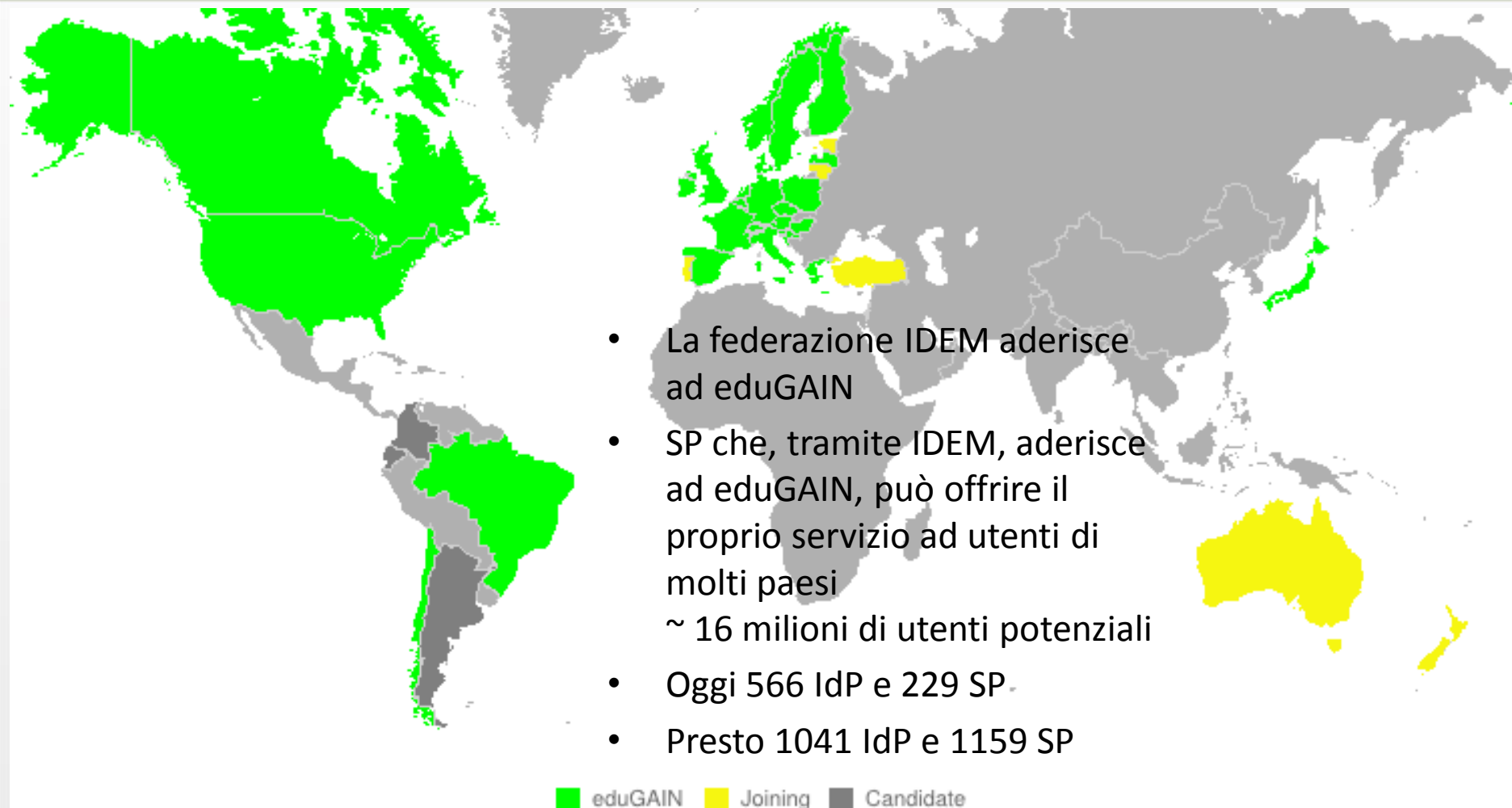
# Federazione IDEM: circle of trust in Italia degli IdP e degli SP del settore istruzione e ricerca

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



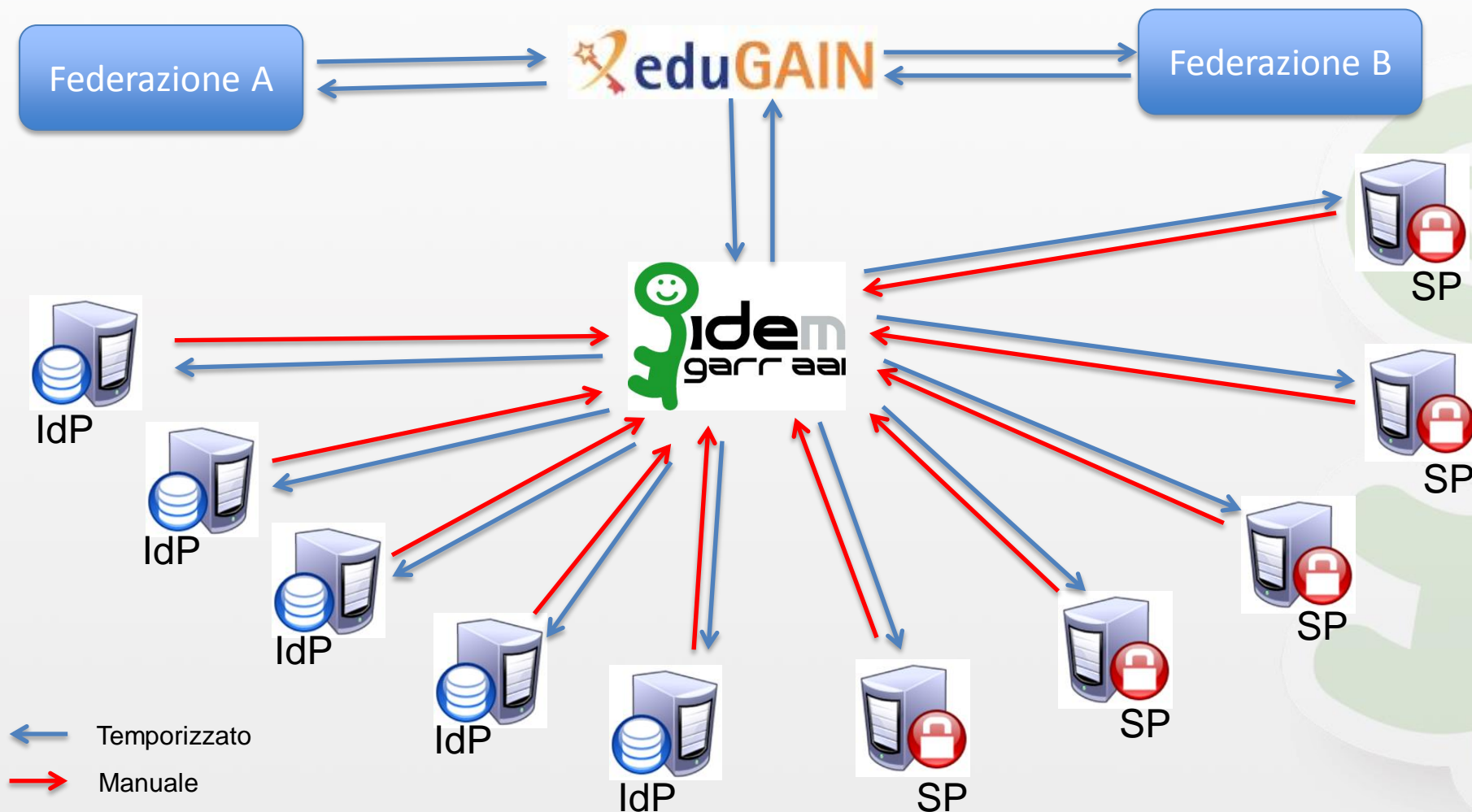
- Servizio IDEM GARR AAI ([idem-help@garr.it](mailto:idem-help@garr.it)) mantiene aggiornati quotidianamente i Metadati di tutti gli IdP e SP che hanno chiesto di aderire ad IDEM
- Ad oggi 112 SP e 59 IdP
- SP che aderisce ad IDEM può fornire il proprio servizio ad utenti italiani del settore R&E  
~ 3 milioni di utenti potenziali

# Federazione eduGAIN circle of trust mondiale nel settore istruzione e ricerca



# Circle of trust

## aggiornamento dei Metadati





# Come partecipare

<https://www.idem.garr.it/come-partecipare>

**Servizio IDEM AAI**

- Home
- IDEM & EduGAIN
- Chi Siamo
- Come Partecipare**
- Modulistica
- Partecipanti
- Servizi
- Informazioni Tecniche
- Fatti e Cifre
- Casi d'uso
- Documenti
- Link
- Area Riservata

## Aderire è Facile !

Il Servizio IDEM GARR AAI vi assisterà in ogni fase del processo, fornendovi tutte le informazioni necessarie.

Posso aderire ?



Accesso all'area di test



Richiesta di adesione



Procedura di approvazione



### Chi può aderire ?

Possono entrare a far parte della Federazione IDEM, in qualità di membri, tutti gli enti con finalità accademiche, scientifiche e culturali connesse alla Rete Italiana dell'Università e della Ricerca GARR. Possono inoltre partecipare alla Federazione IDEM, in qualità di partner, organizzazioni terze (ad esempio editori, fornitori di software o servizi online, ecc), purché forniscano contenuti o servizi che siano ritenuti utili alla Comunità GARR. Per tutti la partecipazione è soggetta all'approvazione del Comitato d'Indirizzo della Federazione IDEM.

### La Federazione di Test

Le organizzazioni che stanno pensando di aderire alla Federazione IDEM possono liberamente usare l'ambiente della Federazione di Test per sperimentare il proprio Identity Provider oppure i propri Service Provider. L'accesso alla Federazione di Test è garantito dal Servizio IDEM GARR AAI e si può richiedere a [idem-help@garr.it](mailto:idem-help@garr.it). Il passaggio per la Federazione di Test è obbligatorio prima di poter accedere con il proprio IdP o SP alla Federazione IDEM, per avere la garanzia che il nuovo servizio che entra in federazione sia aderente ai requisiti.

### La Richiesta di Adesione

Per partecipare alla Federazione IDEM come Membro o come Partner occorre sottoscrivere rispettivamente la Richiesta di Adesione o l'Accordo di Collaborazione e sottomettere contestualmente la Richiesta di registrazione di un servizio (IdP o SP). Tutta la documentazione compilata deve essere inviata in due copie originali, firmate dal rappresentante legale dell'organizzazione che chiede di aderire, a [Consortium GARR](#), Via dei Tizii, 6, 00185 Roma, ed una copia via email a [idem@garr.it](mailto:idem@garr.it). La modulistica è disponibile alla pagina [Modulistica](#).

### La Procedura di Approvazione

Al ricevimento della richiesta di adesione, il Servizio IDEM GARR AAI provvede ad effettuare i necessari controlli tecnici e di sicurezza. Il Comitato Tecnico Scientifico di IDEM valuta l'effettiva necessità degli attributi richiesti e l'aderenza ai requisiti indicati nelle Norme di Partecipazione e nella documentazione collegata. Al termine della procedura il Comitato di Indirizzo della Federazione IDEM stabilisce di comunicare al richiedente se la partecipazione alla Federazione è accettata o respinta.

### L'Attivazione nella Federazione di produzione

All'avvenuta approvazione della richiesta di adesione del nuovo partecipante, il Servizio IDEM GARR AAI provvederà ad assistervi nel trasferimento del vostro servizio dalla Federazione di Test alla Federazione di Produzione.

# Metadata del vostro SP

- SP: <https://sp1.local/Shibboleth.sso/Metadata>

<!--

This is example metadata only. Do *\*NOT\** supply it as is without review, and do *\*NOT\** provide it in real time to your partners.

-->

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_66976f829043f44b424fb1a61711630e6c35682c"
entityID="https://sp1.local/shibboleth">
```

...

```
<md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:1.0:protocol">
```

...

**Ci sono molte cose importanti... ma ne mancano altrettante**

# Metadata Profile per IDEM

<https://www.idem.garr.it/documenti/idem-metadata-profile>

```
<md:OrganizationName>  
<md:OrganizationDisplayName>  
<md:OrganizationURL>  
...  
<mdui:DisplayName>  
<mdui:Description>  
<mdui:InformationURL>  
<mdui:PrivacyStatementURL>  
<mdui:Logo>  
...  
<md:RequestedAttribute>  
...  
<md:ContactPerson>  
<md:EmailAddress>
```

in italiano e in inglese

Template metadati per SP:

[https://www.idem.garr.it/it/documenti/doc\\_download/256-sp-metadata-template](https://www.idem.garr.it/it/documenti/doc_download/256-sp-metadata-template)

# IDEM Entity Registry

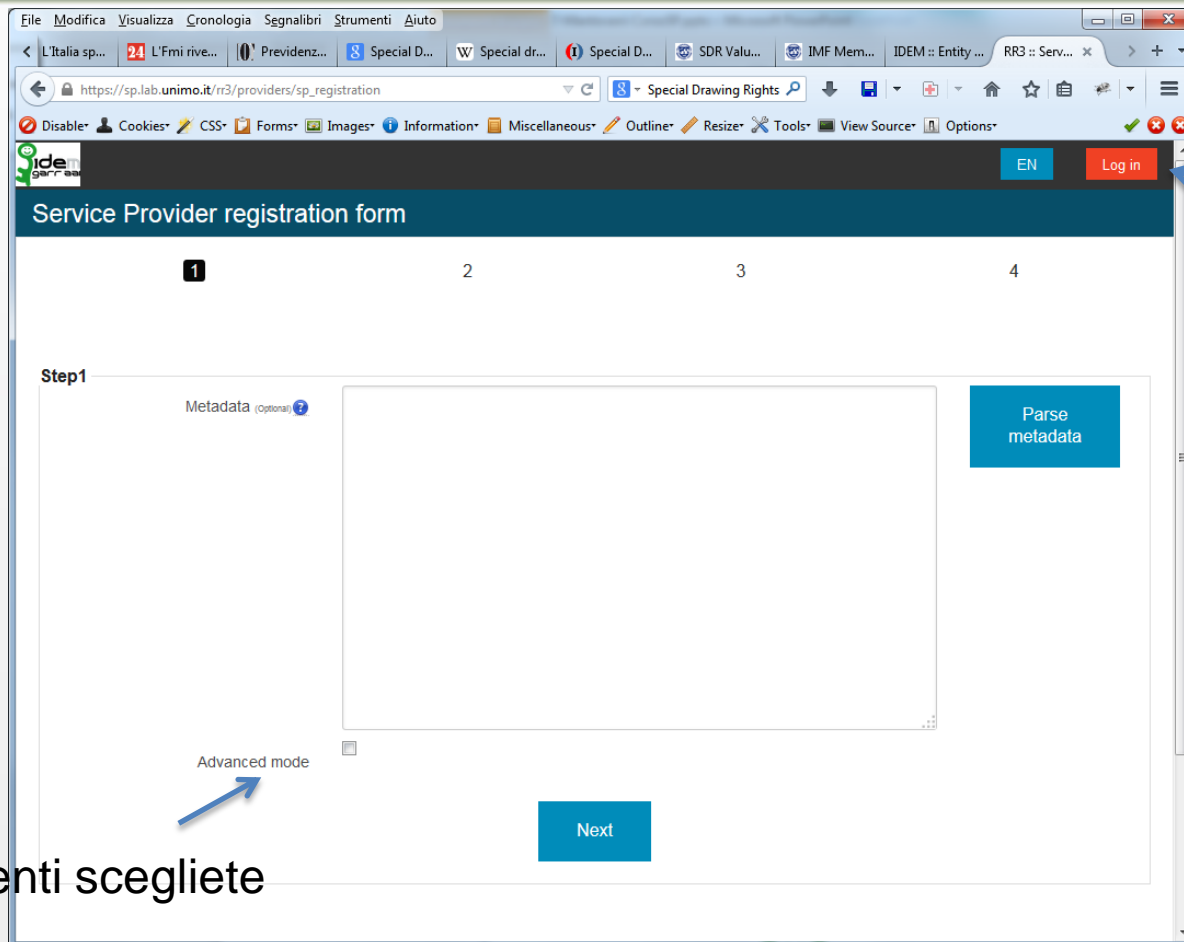
## <https://registry.idem.garr.it>



Per il corso usiamo il registry di prova: <https://sp.lab.unimo.it/rr3/>



# Inserire i metadati creati dal SP



Service Provider registration form

1 2 3 4

Step1

Metadata (optional) ?

Parse metadata

Advanced mode

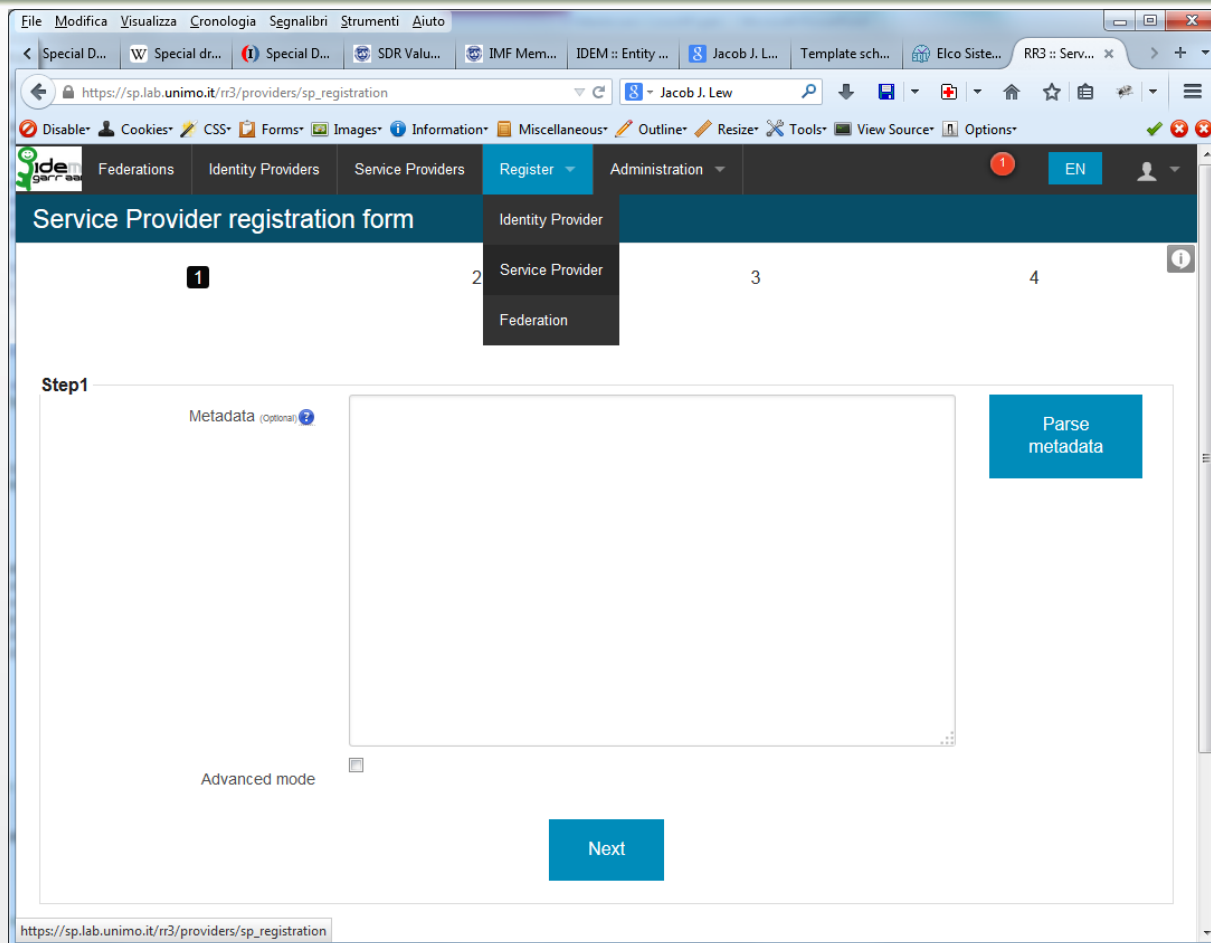
Next

Log in

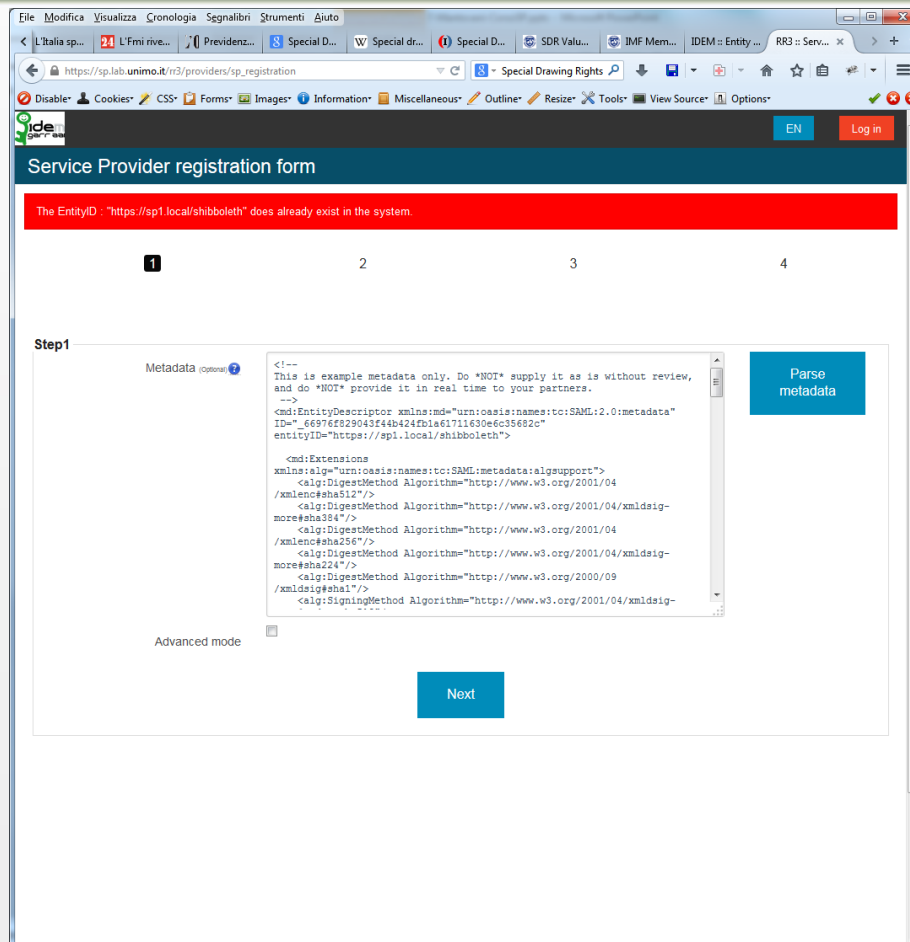
Login se potete

Altrimenti scegliete

# Register -> Service Provider



# entityID deve essere univoco




The screenshot shows a web browser window displaying the "Service Provider registration form". A red error message at the top states: "The EntityID : 'https://sp1.local/shibboleth' does already exist in the system." Below the error message, there are four numbered steps (1, 2, 3, 4). Step 1 is currently active and shows a "Metadata" field with a text area containing XML code. The XML code is an example of SAML metadata, including an EntityDescriptor and Extensions. To the right of the text area is a "Parse metadata" button. Below the text area is an "Advanced mode" checkbox. At the bottom of the form is a "Next" button.

Service Provider registration form

The EntityID : "https://sp1.local/shibboleth" does already exist in the system.

1 2 3 4

Step1

Metadata (optional) 

```
<!--
This is example metadata only. Do *NOT* supply it as is without review,
and do *NOT* provide it in real time to your partners.
-->
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="66976829043f4b424fb1e61711630e6c35682c"
entityID="https://sp1.local/shibboleth">

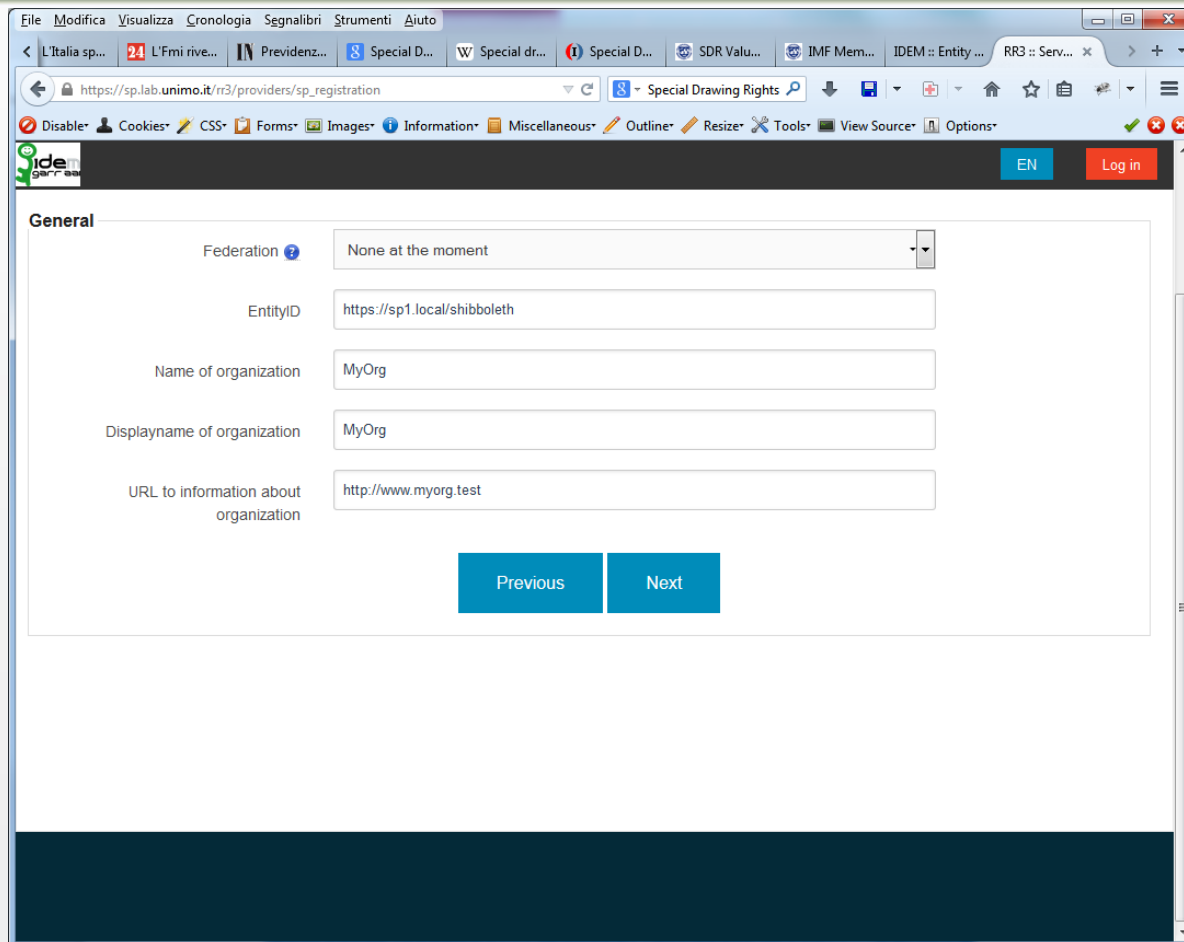
  <md:Extensions
    xmlns:alg="urn:oasis:names:tc:SAML:metadata:alg:support">
    <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha512"/>
    <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha384"/>
    <alg:DigestMethod Algorithm="http://www.w3.org/2001/04
/xmldsig#sha256"/>
    <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha256"/>
    <alg:DigestMethod Algorithm="http://www.w3.org/2000/09
/xmldsig#sha1"/>
    <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha1"/>
  </md:Extensions>
</md:EntityDescriptor>
```

Parse metadata

Advanced mode ☐

Next

# Organizzazione: Nome e Info

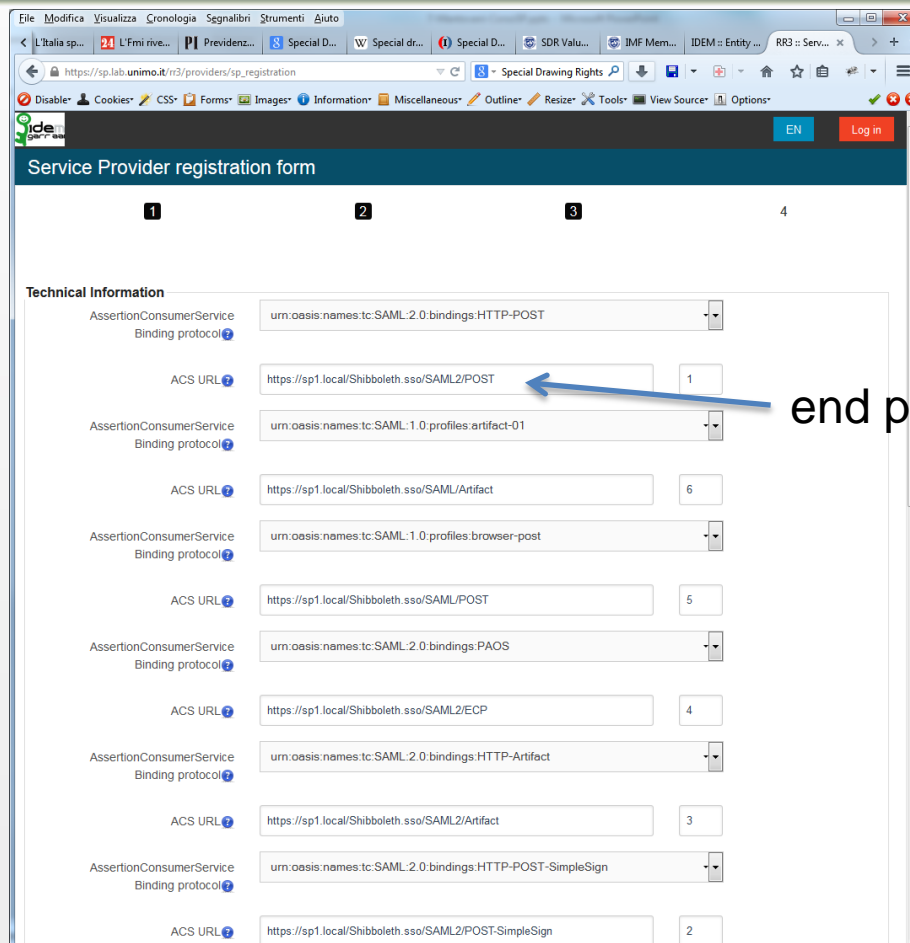


The screenshot shows a web browser window with the URL [https://sp.lab.unimo.it/rr3/providers/sp\\_registration](https://sp.lab.unimo.it/rr3/providers/sp_registration). The page is titled "General" and contains the following fields:

- Federation: A dropdown menu with the selected value "None at the moment".
- EntityID: A text input field containing "https://sp1.local/shibboleth".
- Name of organization: A text input field containing "MyOrg".
- Displayname of organization: A text input field containing "MyOrg".
- URL to information about organization: A text input field containing "http://www.myorg.test".

At the bottom of the form, there are two buttons: "Previous" and "Next".

# End point sicuri



Service Provider registration form

1 2 3 4

**Technical Information**

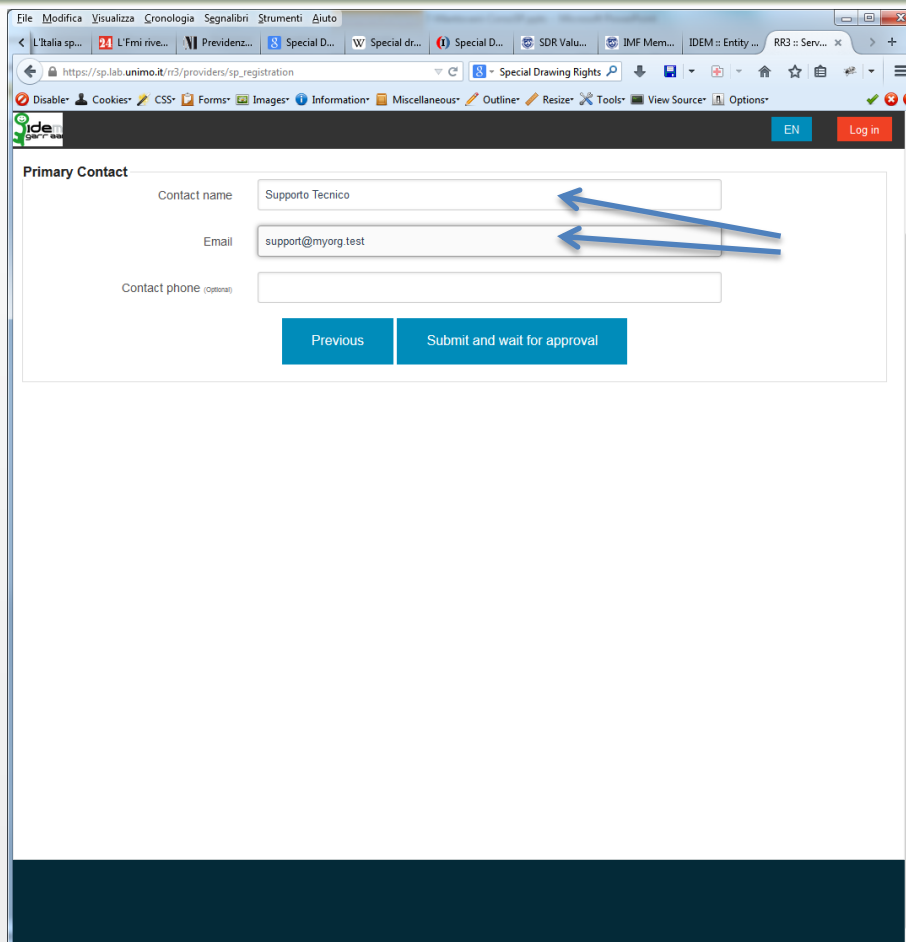
AssertionConsumerService Binding protocol	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	
ACS URL	https://sp1.local/Shibboleth.sso/SAML2/POST	1
AssertionConsumerService Binding protocol	urn:oasis:names:tc:SAML:1.0:profiles:artifact-01	
ACS URL	https://sp1.local/Shibboleth.sso/SAML/Artifact	6
AssertionConsumerService Binding protocol	urn:oasis:names:tc:SAML:1.0:profiles:browser-post	
ACS URL	https://sp1.local/Shibboleth.sso/SAML/POST	5
AssertionConsumerService Binding protocol	urn:oasis:names:tc:SAML:2.0:bindings:PAOS	
ACS URL	https://sp1.local/Shibboleth.sso/SAML2/EC	4
AssertionConsumerService Binding protocol	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact	
ACS URL	https://sp1.local/Shibboleth.sso/SAML2/Artifact	3
AssertionConsumerService Binding protocol	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign	
ACS URL	https://sp1.local/Shibboleth.sso/SAML2/POST-SimpleSign	2

end point deve essere https



Maria Laura Mantovani, GARR e Università di Modena e Reggio Emilia

# Contatti per il Registry



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

https://sp.lab.unimo.it/r3/providers/sp\_registration

Primary Contact

Contact name Supporto Tecnico

Email support@myorg.test

Contact phone (optional)

Previous Submit and wait for approval

## Service Provider: MyOrg

ONS

provider

age membership (joining)

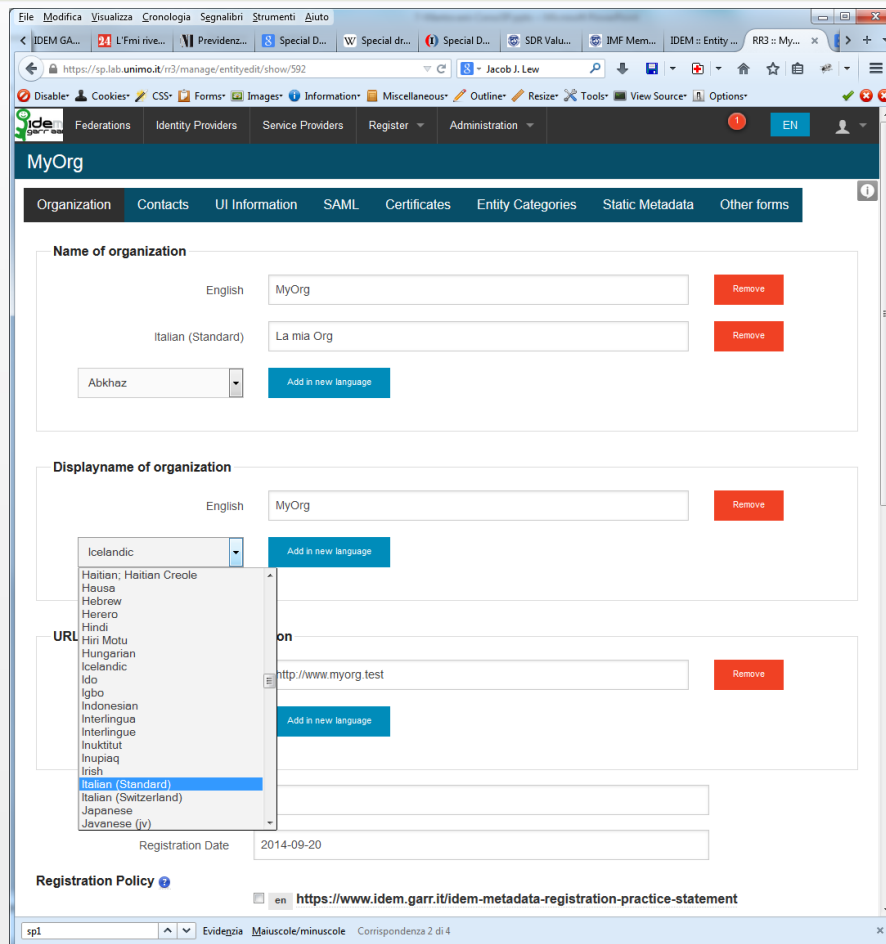
RIBUTES

quired Attributes

Clear cache

	General	Membership	Metadata	Management	Logs/Stats
<b>Status</b> ?	Enabled Managed locally				
<b>Last modification</b>	2014-09-20 15:13:02				
<b>EntityID</b>	https://sp-lalla.local/shibboleth				
<b>Name of organization</b>	en: MyOrg				
<b>Displayname of organization</b>	en: MyOrg				
<b>URL to information about organization</b>	en: http://www.myorg.test				
<b>Registration Authority</b>	It's not set but for metadata generation system will be using http://sp-lalla.local/shibboleth <small>loaded from global config</small>				
<b>Registration Date</b>	2014-09-20				
<b>Registration Policy</b>					
<b>Entity Categories</b>	not set				
<b>Valid From/Until</b>	unlimited -- unlimited				

# Info multilingue: Organizzazione



The screenshot shows the 'MyOrg' web application interface. The browser window displays the URL <https://sp.lab.unimo.it/n3/manage/entityedit/show/592>. The application has a dark blue header with the 'MyOrg' logo and a navigation bar with tabs: Organization, Contacts, UI Information, SAML, Certificates, Entity Categories, Static Metadata, and Other forms. The 'Organization' tab is active.

The main content area is titled 'Name of organization' and contains two input fields for different languages:

- English: MyOrg (with a 'Remove' button)
- Italian (Standard): La mia Org (with a 'Remove' button)

Below these fields is a dropdown menu for 'Abkhaz' and a button 'Add in new language'.

The next section is 'Displayname of organization', which has an input field for 'English' with the value 'MyOrg' and a 'Remove' button. Below this is a dropdown menu for 'Icelandic' and a button 'Add in new language'.

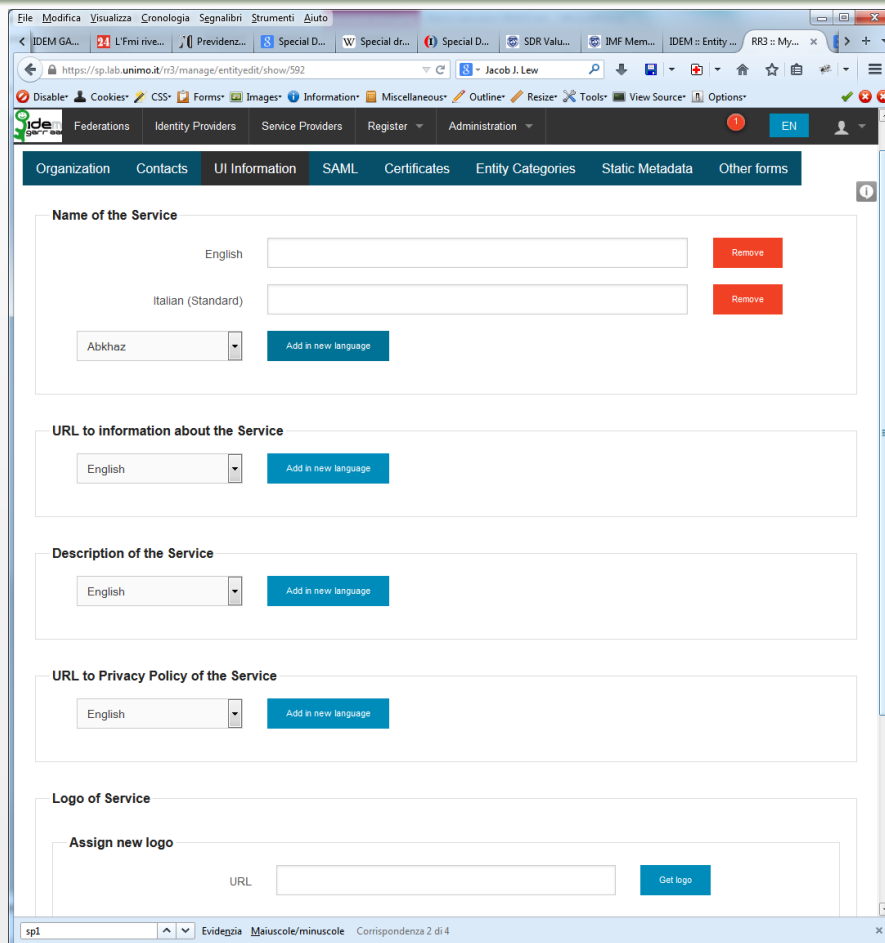
The 'URL' section has an input field with the value 'http://www.myorg.test' and a 'Remove' button. Below this is a button 'Add in new language'.

The 'Registration Date' is set to '2014-09-20'.

The 'Registration Policy' section shows a dropdown menu for 'en' and a link to <https://www.idem.garr.it/idem-metadata-registration-practice-statement>.

The footer of the application shows the text 'spl' and 'Evidenza Maiuscole/minuscole Corrispondenza 2 di 4'.

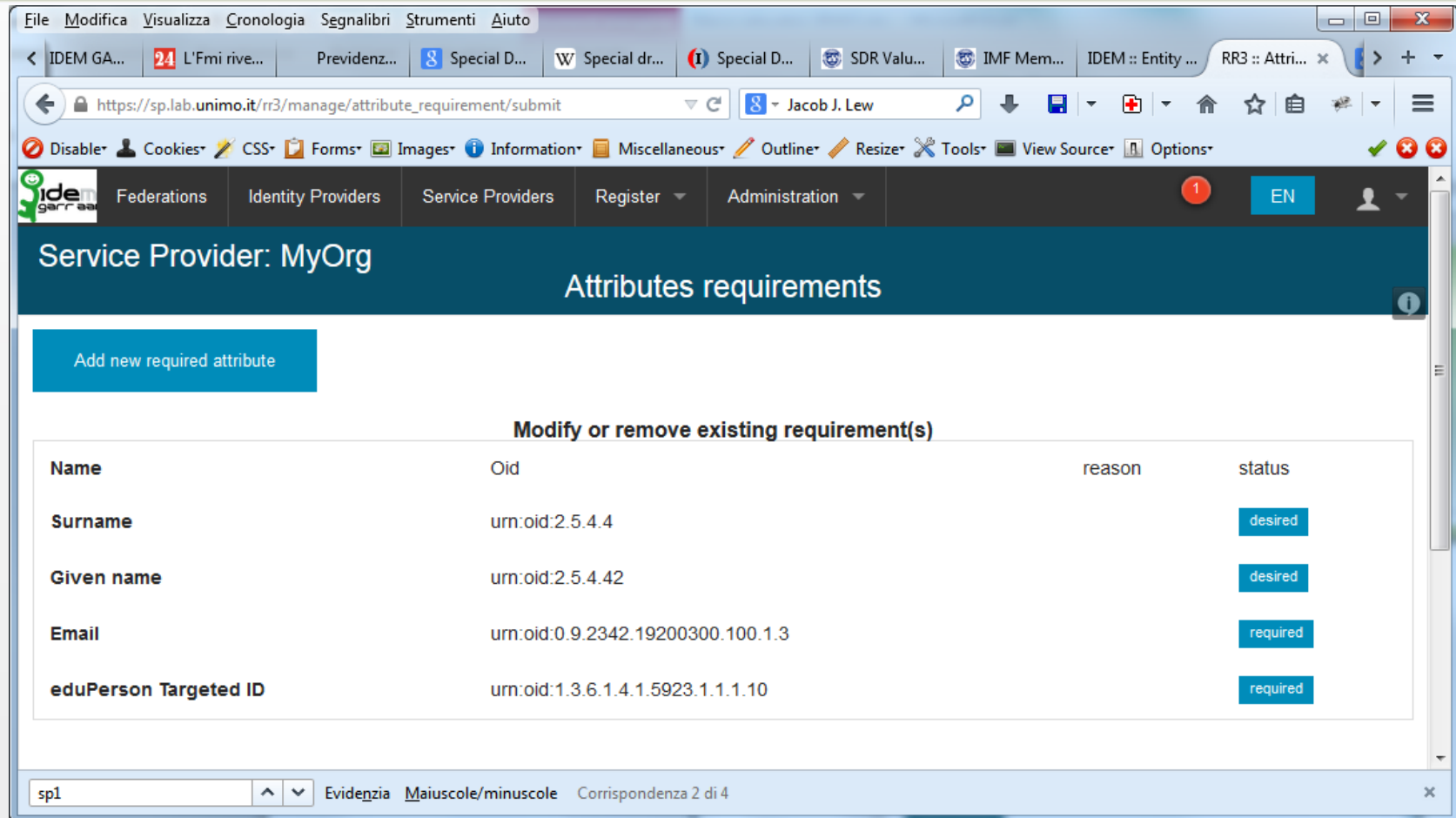
# Info multilingue: Servizio



The screenshot shows a web browser window with the URL <https://sp.lab.unimo.it/n3/manage/entityedit/show/592>. The page title is "IDEM GA...". The browser's address bar shows the URL. The page has a navigation bar with tabs: "Organization", "Contacts", "UI Information", "SAML", "Certificates", "Entity Categories", "Static Metadata", and "Other forms". The "UI Information" tab is selected. The main content area is titled "Name of the Service" and contains a form with two language entries: "English" and "Italian (Standard)". Each entry has a text input field and a "Remove" button. Below these entries is a dropdown menu for "Abkhaz" and an "Add in new language" button. The form also includes sections for "URL to information about the Service", "Description of the Service", "URL to Privacy Policy of the Service", and "Logo of Service". Each of these sections has a language dropdown menu and an "Add in new language" button. The "Logo of Service" section has a text input field for the "URL" and a "Get logo" button. The browser's status bar at the bottom shows the page is "Corrispondenza 2 di 4".



# Attributi richiesti dal SP



Service Provider: MyOrg

## Attributes requirements

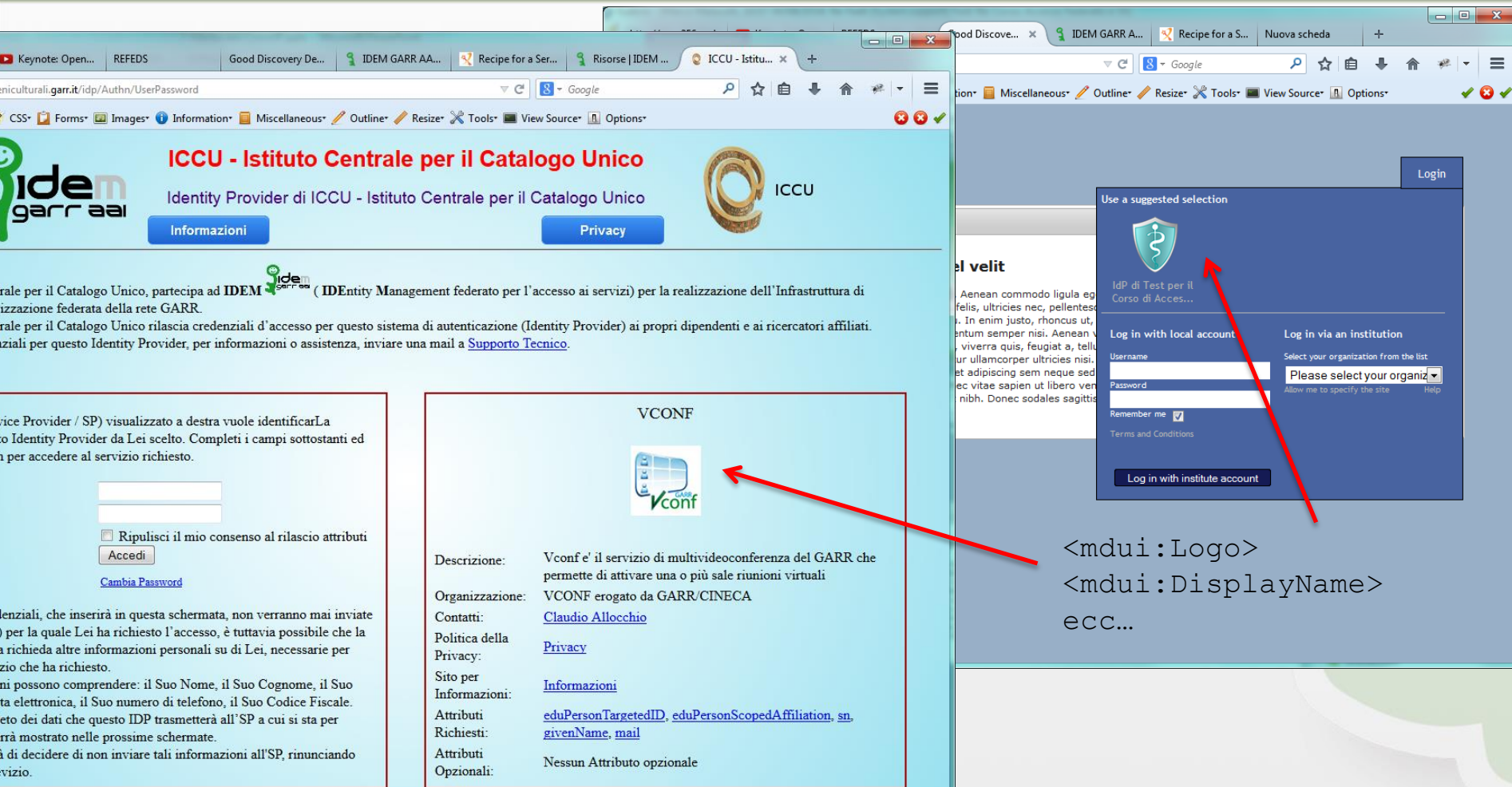
[Add new required attribute](#)

**Modify or remove existing requirement(s)**

Name	OID	reason	status
Surname	urn:oid:2.5.4.4		<a href="#">desired</a>
Given name	urn:oid:2.5.4.42		<a href="#">desired</a>
Email	urn:oid:0.9.2342.19200300.100.1.3		<a href="#">required</a>
eduPerson Targeted ID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10		<a href="#">required</a>

sp1 Evidenzia Maiuscole/minuscole Corrispondenza 2 di 4

# Display in IDP e DS



**ICCUI - Istituto Centrale per il Catalogo Unico**  
Identity Provider di ICCU - Istituto Centrale per il Catalogo Unico

[Informazioni](#) [Privacy](#)

IdP di Test per il Corso di Acces...

Log in with local account  
Username  
Password  
Remember me ☒  
Terms and Conditions  
Log in with institute account

Log in via an institution  
Select your organization from the list  
Please select your organization  
Allow me to specify the site  
Help

**VCONF**

Descrizione: Vconf e' il servizio di multivideoconferenza del GARR che permette di attivare una o più sale riunioni virtuali

Organizzazione: VCONF erogato da GARR/CINECA

Contatti: [Claudio Allocchio](#)

Politica della Privacy: [Privacy](#)

Sito per Informazioni: [Informazioni](#)

Attributi: [eduPersonTargetedID](#), [eduPersonScopedAffiliation](#), [sn](#), [givenName](#), [mail](#)

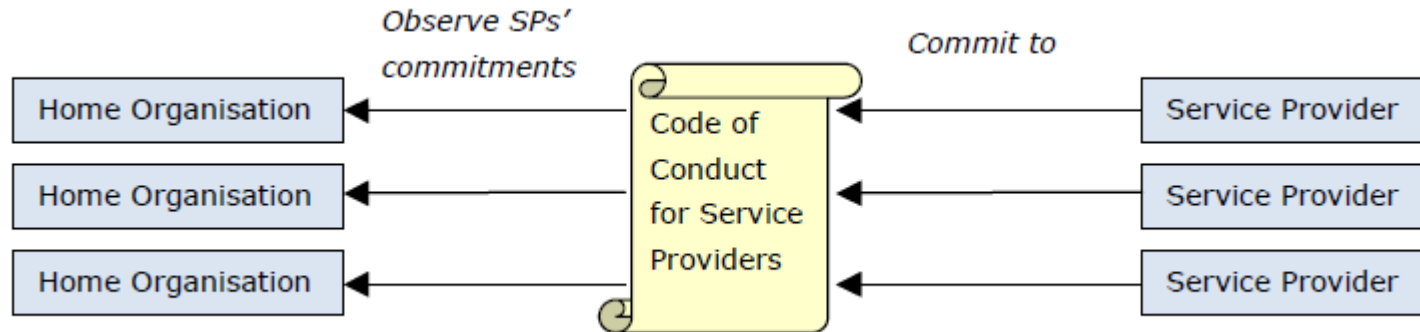
Richiesti:

Attributi Opzionali: Nessun Attributo opzionale

`<mdui:Logo>`  
`<mdui:DisplayName>`  
ecc...

# Codice di Condotta per SP

enables safe attribute release between Identity and Service Providers within EU



- [http://www.geant.net/uri/dataprotection-code-of-conduct/V1/Documents/GEANT\\_DP\\_CoC\\_ver1.0.pdf](http://www.geant.net/uri/dataprotection-code-of-conduct/V1/Documents/GEANT_DP_CoC_ver1.0.pdf)
- template: [Privacy Policy Guidelines for Service Providers](#)
- Metadata:
  - Entity Category attribute for the Code of Conduct
  - mdui:PrivacyStatementURL
  - list of md:RequestedAttributes
  - mdui:Displayname (recommended)
  - mdui:Description (recommended)

# La federazione IDEM-TEST

Dopo aver inviato i vostri Metadati ad IDEM

- Tramite l'Entity Registry
- Oppure via email a [idem-help@garr.it](mailto:idem-help@garr.it)

Venite attivati nella federazione IDEM-TEST

Riceverete una email da [idem-help@garr.it](mailto:idem-help@garr.it) con le istruzioni per configurare il vostro SP con i Metadati della federazione di test e il DS (facoltativo) della federazione di test.

**Il passaggio per la Federazione IDEM-TEST è obbligatorio prima di poter accedere alla Federazione IDEM ufficiale**

# Aderire ufficialmente alla Federazione

<https://www.idem.garr.it/come-partecipare/regole-e-procedure>

Se l'Organizzazione è collegata a GARR (e non ancora in IDEM)

=> **Richiesta di Adesione**

[https://www.idem.garr.it/documenti/doc\\_download/111-richiestadiadesione-v1-2-20100223](https://www.idem.garr.it/documenti/doc_download/111-richiestadiadesione-v1-2-20100223)

Se l'Organizzazione NON è collegata a GARR

=> **Accordo di collaborazione**

[https://www.idem.garr.it/documenti/doc\\_download/156-accordodicollaborazione-v1-3-20110218](https://www.idem.garr.it/documenti/doc_download/156-accordodicollaborazione-v1-3-20110218)

Per ogni SP => **Modulo per la Registrazione di un SP**

(Resource Registration Request)

Qui dichiarate se volete  
entrare anche in eduGAIN

[https://www.idem.garr.it/documenti/doc\\_download/261-resourceregistrationrequest-v2-0-20130523](https://www.idem.garr.it/documenti/doc_download/261-resourceregistrationrequest-v2-0-20130523)

Responsabile legale, Referente Organizzativo, Referente Tecnico  
e Contatto Tecnico assumono responsabilità verso la federazione  
(<https://www.idem.garr.it/documenti/regolamento> )



# La procedura di approvazione

La Federazione, per mezzo del Servizio IDEM GARR AAI:

- Riceve la documentazione ufficiale (RA/AC, RRR)
- Verifica la completezza dei Metadati
- Verifica la sicurezza dei certificati e degli end point (https)
- Completezza delle informazioni fornite (via URL)
- Verifica Requested Attribute
- Tempo di sincronizzazione metadati

# Attivazione nella Federazione di Produzione

Superata la procedura di approvazione  
la vostra entità viene spostata nella federazione  
ufficiale

Riceverete da [idem-help@garr.it](mailto:idem-help@garr.it) le istruzioni per  
riconfigurare lo scaricamento dei metadati ufficiali

- di IDEM
- o eventualmente di eduGAIN (se opt-in)

le istruzioni si trovano anche:

<https://www.idem.garr.it/informazioni-tecniche/metadati>

# Community IDEM

- Mailing list [idem-users@garr.it](mailto:idem-users@garr.it)
- Mailto: [majordomo@garr.it](mailto:majordomo@garr.it) subscribe idem-users
- Per discutere di problematiche teoriche/tecniche relative
  - all'Identity and Access Management,
  - alle Infrastrutture di Autenticazione e Autorizzazione,
  - alla Federazione IDEM
- con gli altri partecipanti alla Federazione IDEM

# Q&A



# Bibliografia

- Federazione IDEM: <https://www.idem.garr.it/>
- Documenti normativi IDEM: <https://www.idem.garr.it/come-partecipare/regole-e-procedure>
- Metadati: <https://www.idem.garr.it/informazioni-tecniche/metadati>
- eduGAIN status:  
<http://www.edugain.org/technical/status.php>
- Documenti normativi eduGAIN:  
<http://www.geant.net/service/eduGAIN/resources/Pages/home.aspx>
- Code of Conduct cookbook:  
[https://wiki.edugain.org/Data\\_Protection\\_Code\\_of\\_Conduct\\_Cookbook](https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook)