Registrare un SP nella Federazione GARR IDEM e in eduGAIN

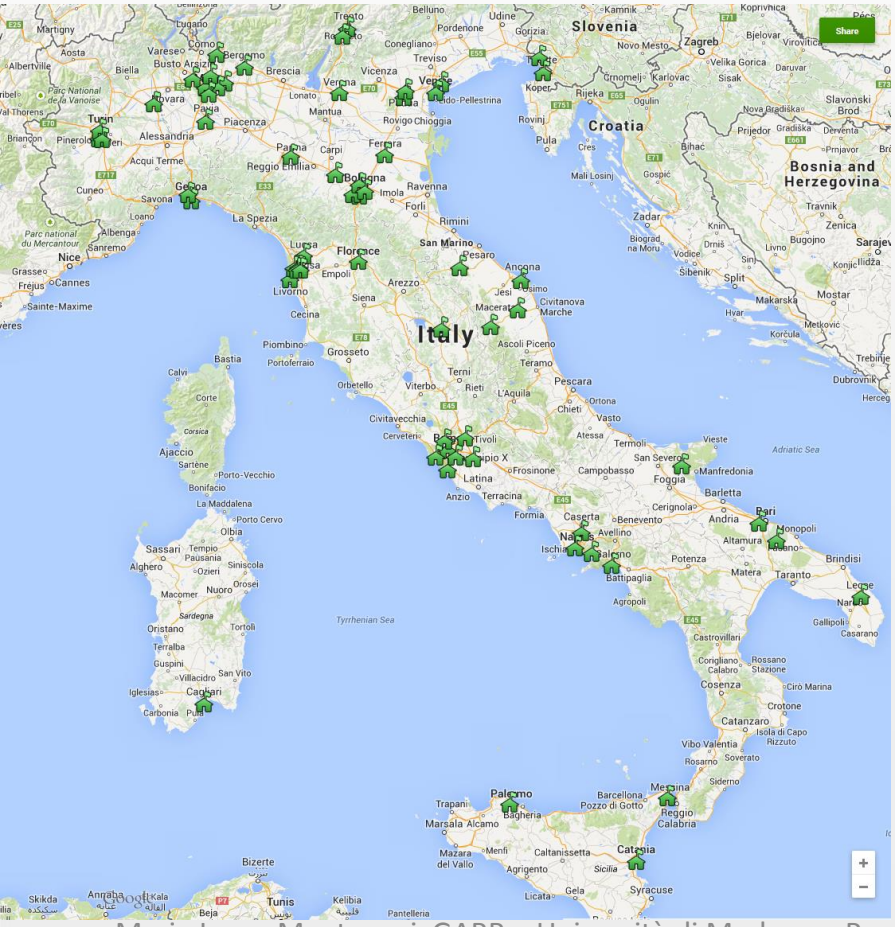
Corso IDEM: Abilitare le applicazioni web al Single Sign-on con strumenti SAML

Roma, 30.09.2014

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

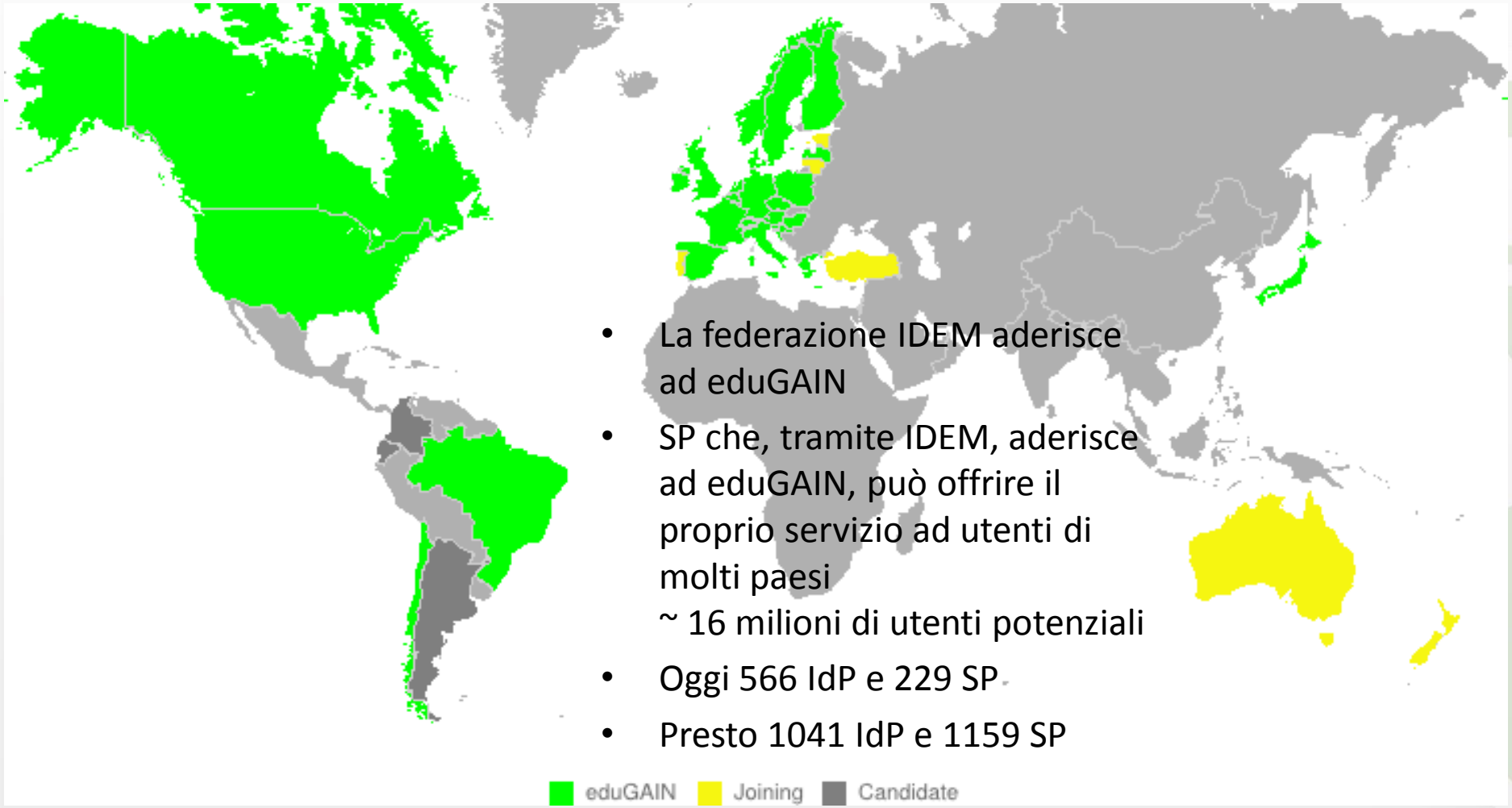
Federazione IDEM: circle of trust in Italia degli IdP e degli SP del settore istruzione e ricerca

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



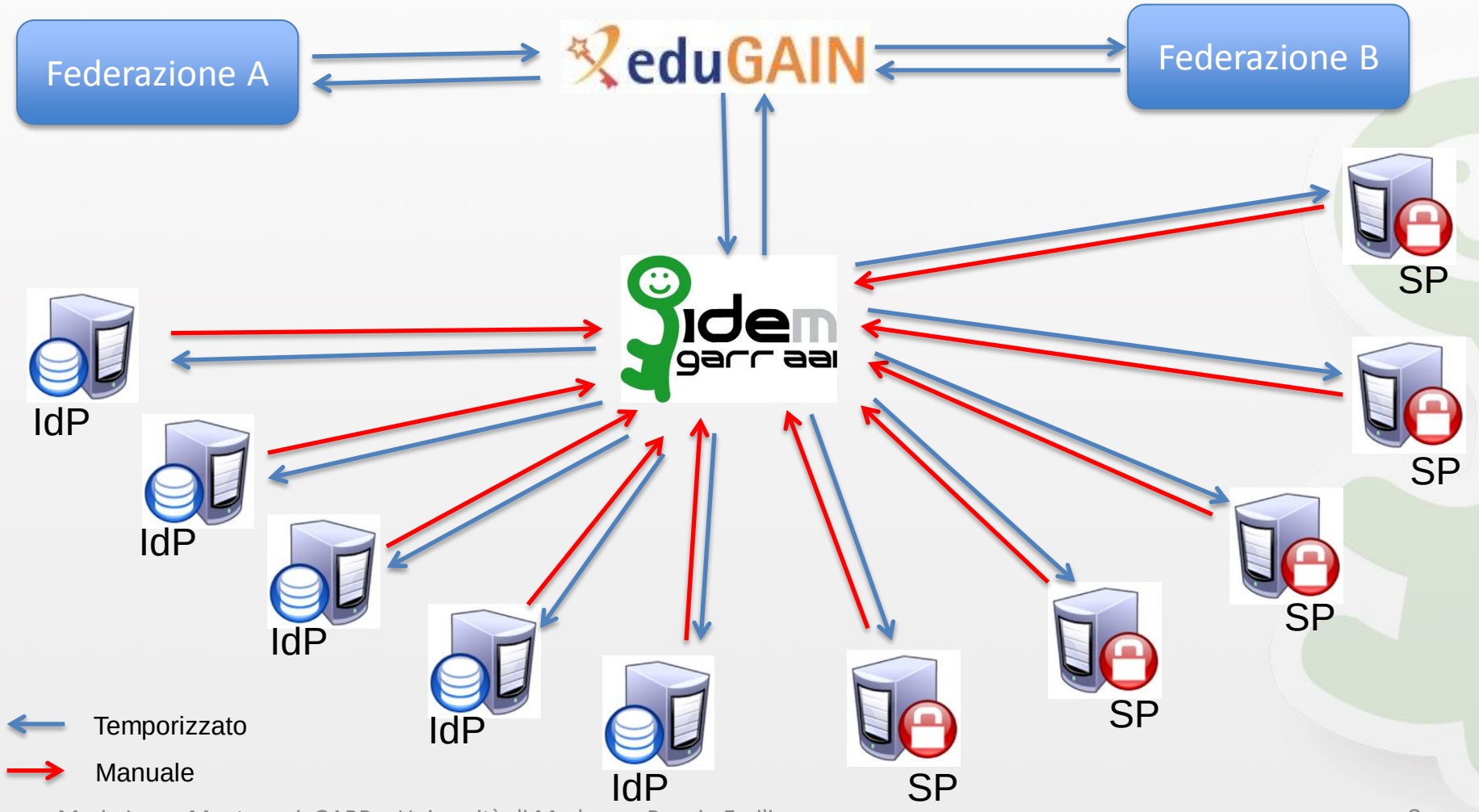
- Servizio IDEM GARR AAI (idem-help@garr.it) mantiene aggiornati quotidianamente i Metadati di tutti gli IdP e SP che hanno chiesto di aderire ad IDEM
- Ad oggi 112 SP e 59 IdP
- SP che aderisce ad IDEM può fornire il proprio servizio ad utenti italiani del settore R&E ~ 3 milioni di utenti potenziali

Federazione eduGAIN circle of trust mondiale nel settore istruzione e ricerca



- La federazione IDEM aderisce ad eduGAIN
- SP che, tramite IDEM, aderisce ad eduGAIN, può offrire il proprio servizio ad utenti di molti paesi
  ~ 16 milioni di utenti potenziali
- Oggi 566 IdP e 229 SP
- Presto 1041 IdP e 1159 SP

Circle of trust aggiornamento dei Metadati



Come partecipare

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

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

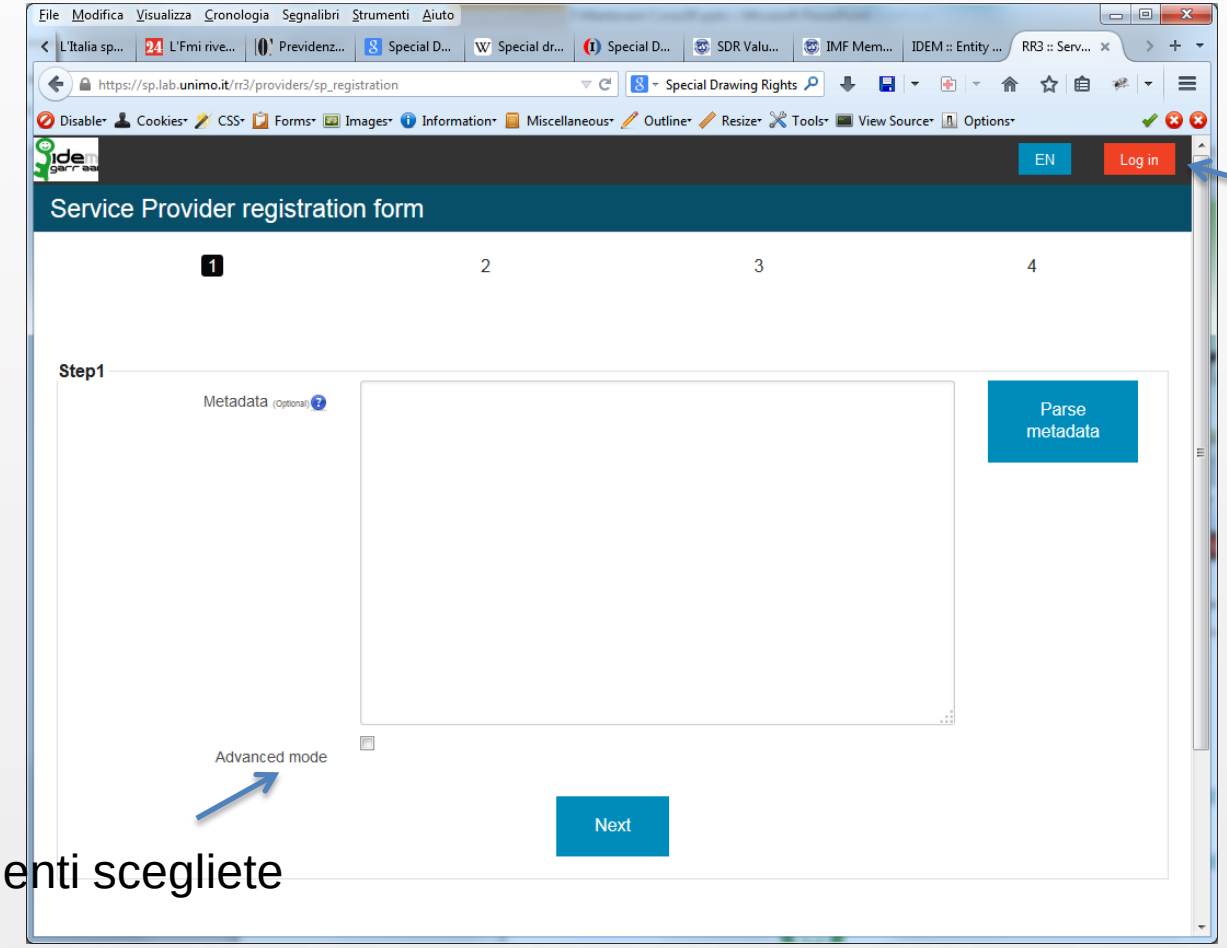
Template metadati per SP:
https://www.idem.garr.it/it/documenti/doc_download/256-sp-metadata-template

IDEM Entity Registry

https://registry.idem.garr.it

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

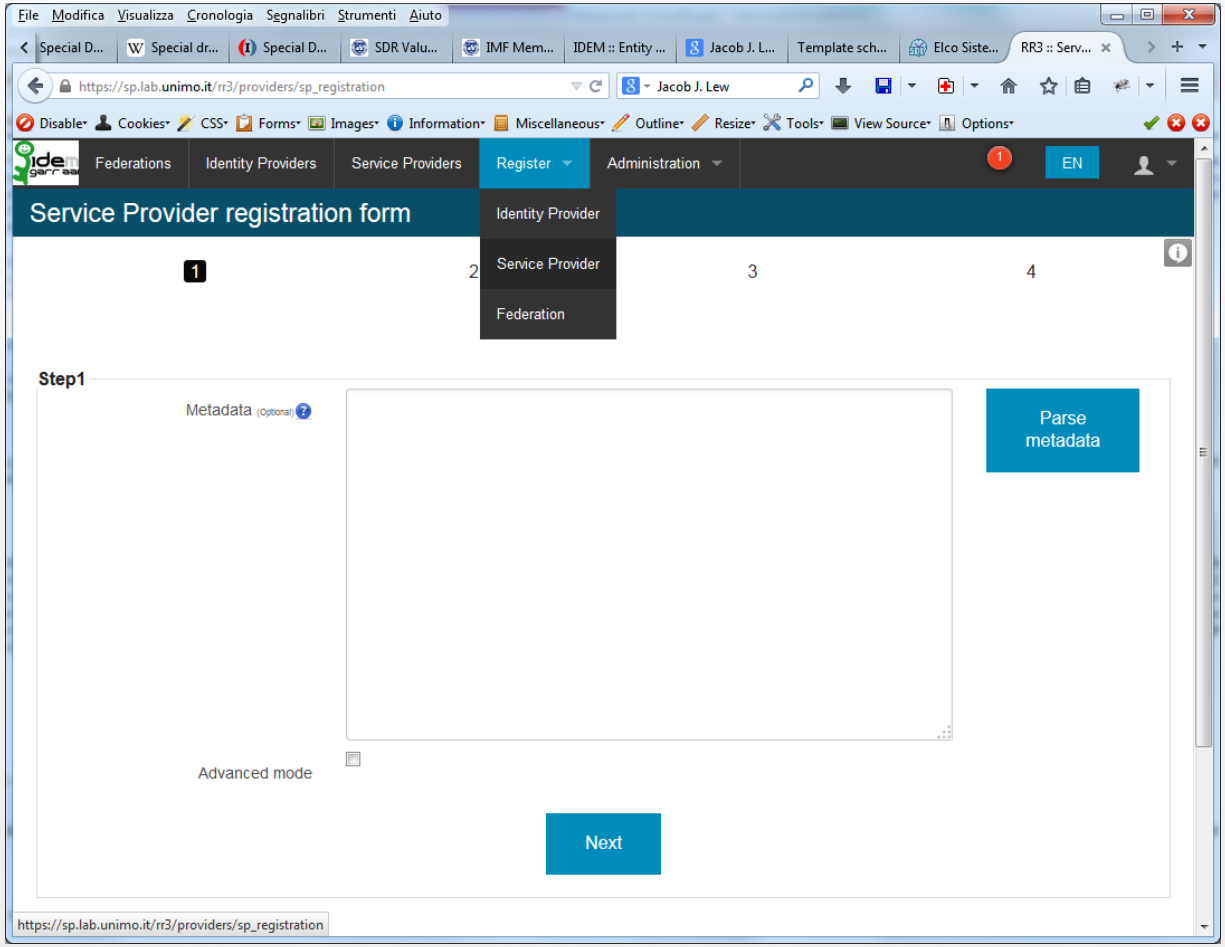
Inserire i metadati creati dal SP



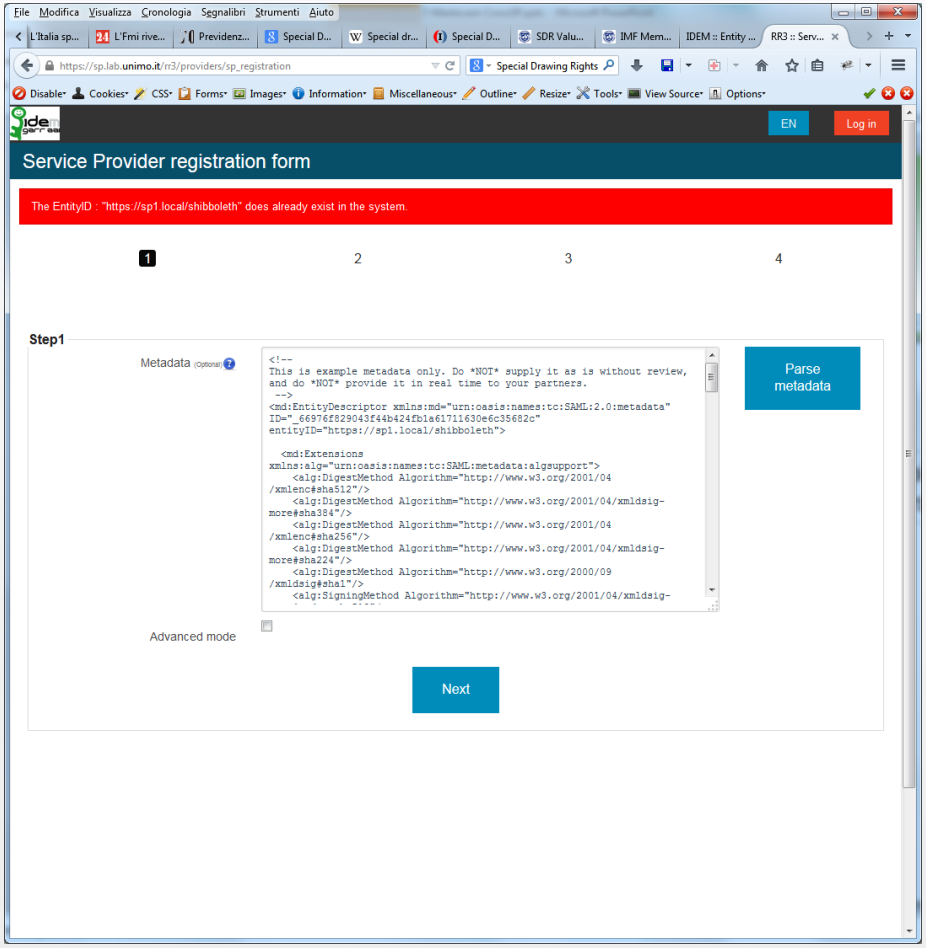
Login se potete

Altrimenti scegliete

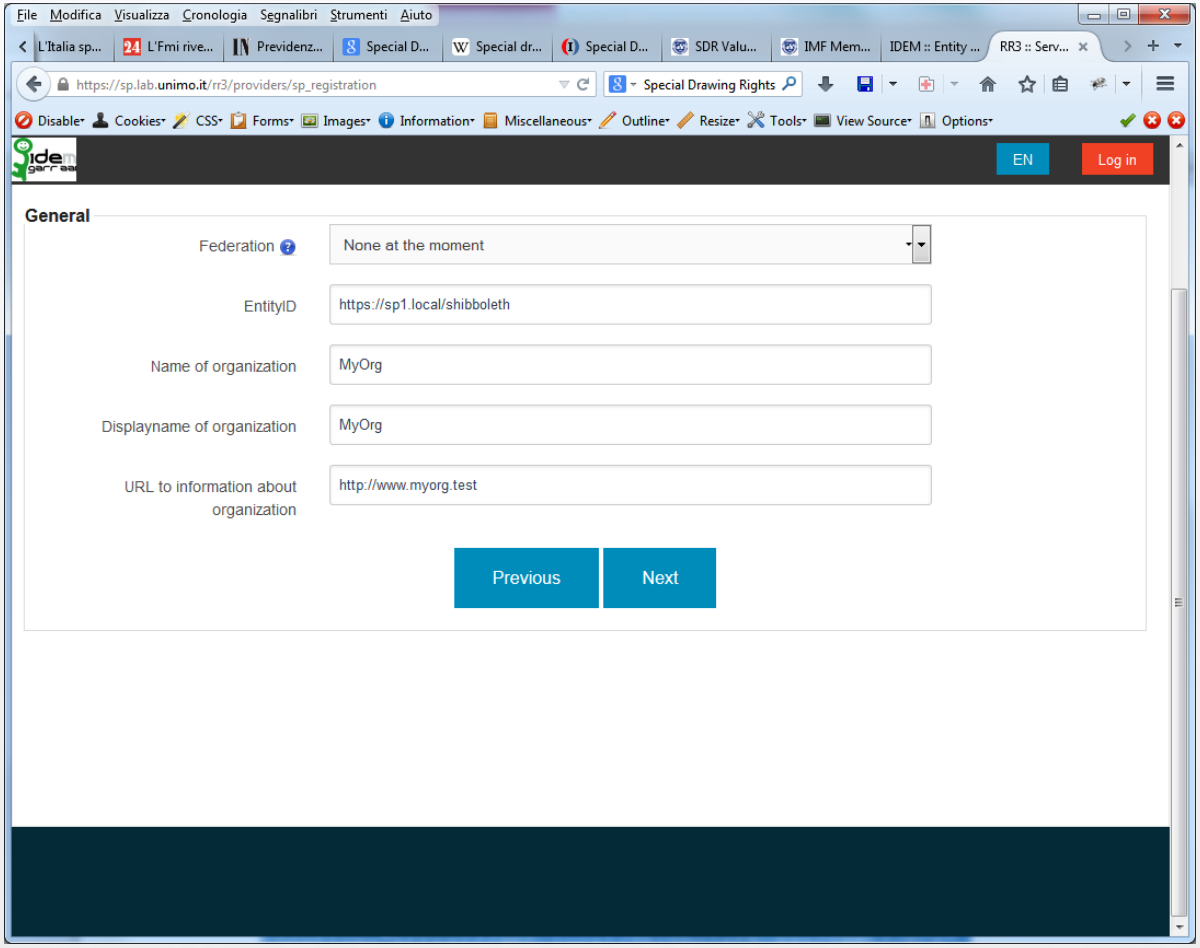
Register -> Service Provider



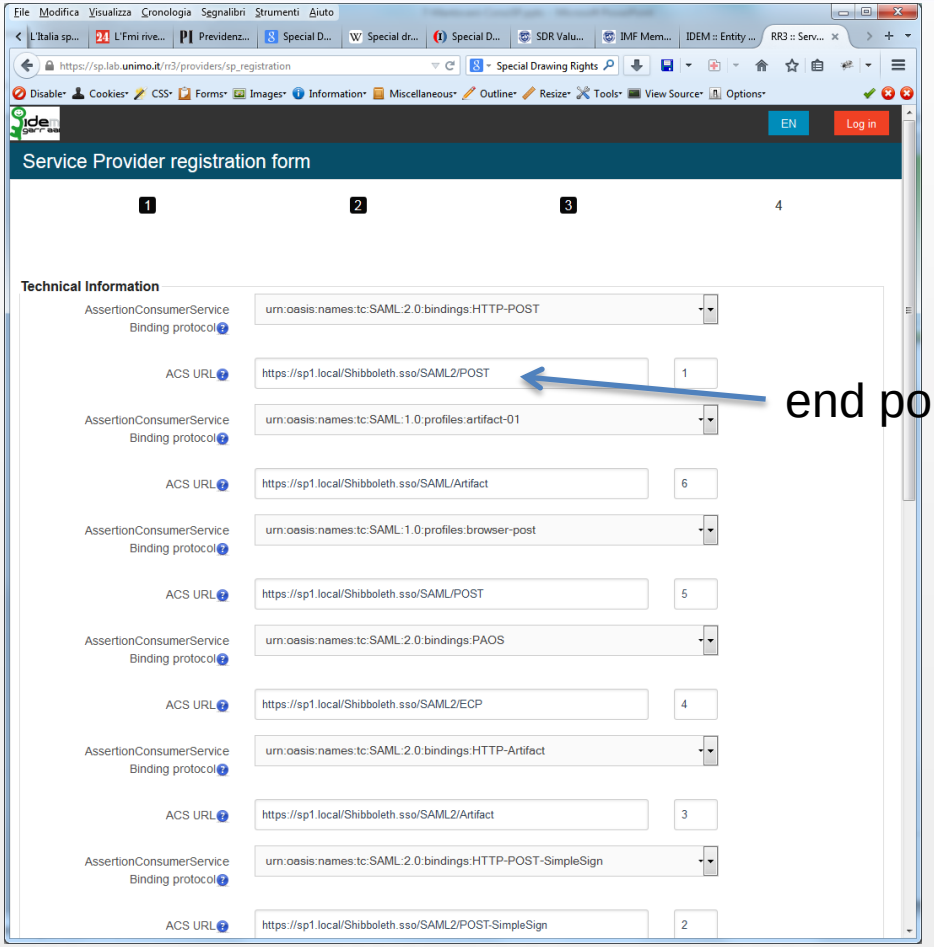
entityID deve essere univoco



Organizzazione: Nome e Info

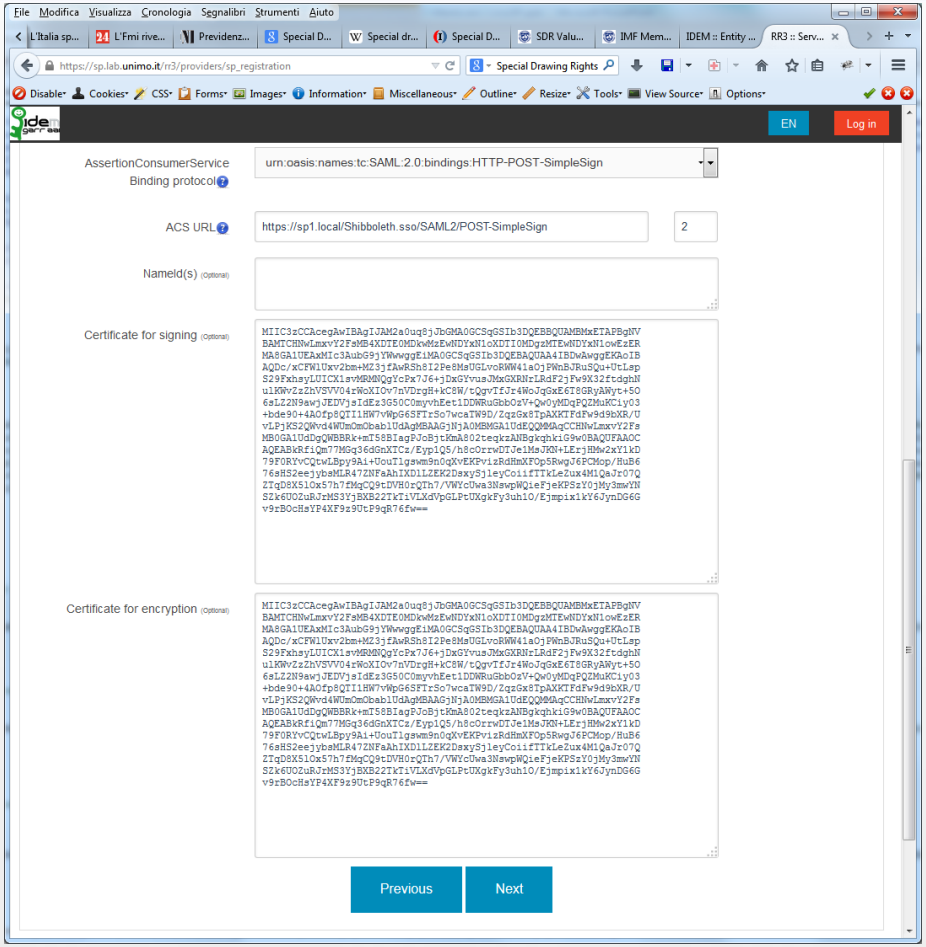


End point sicuri

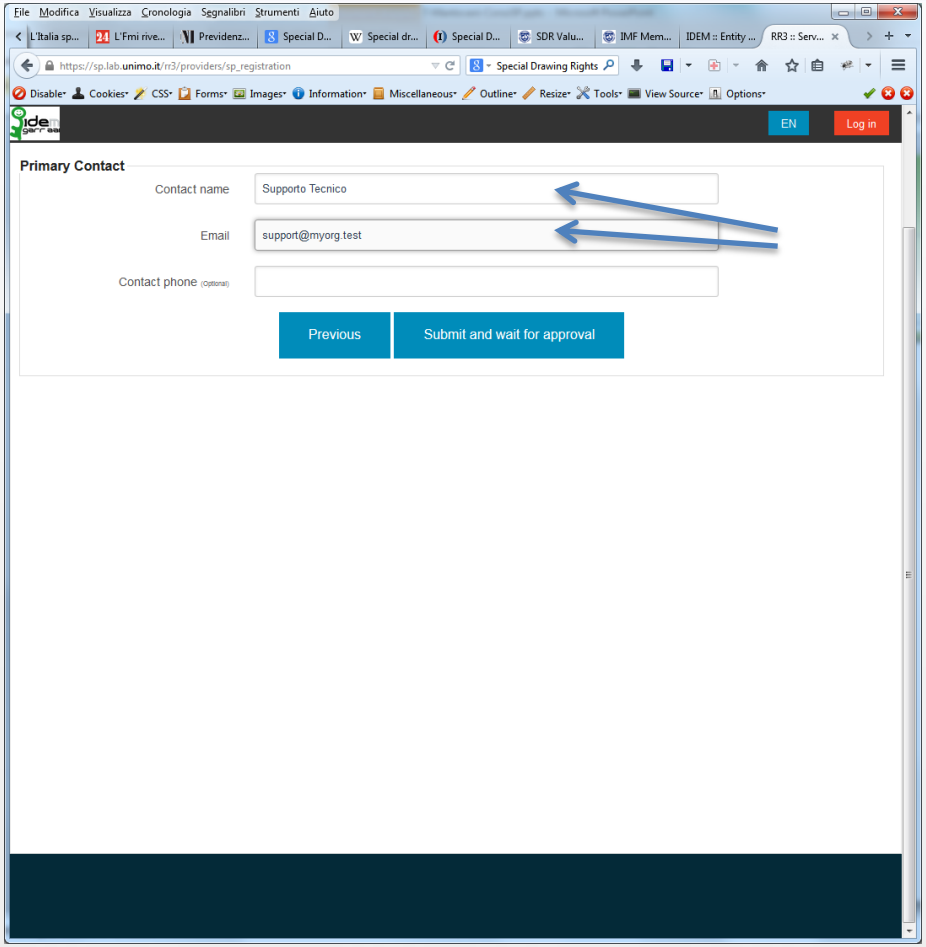


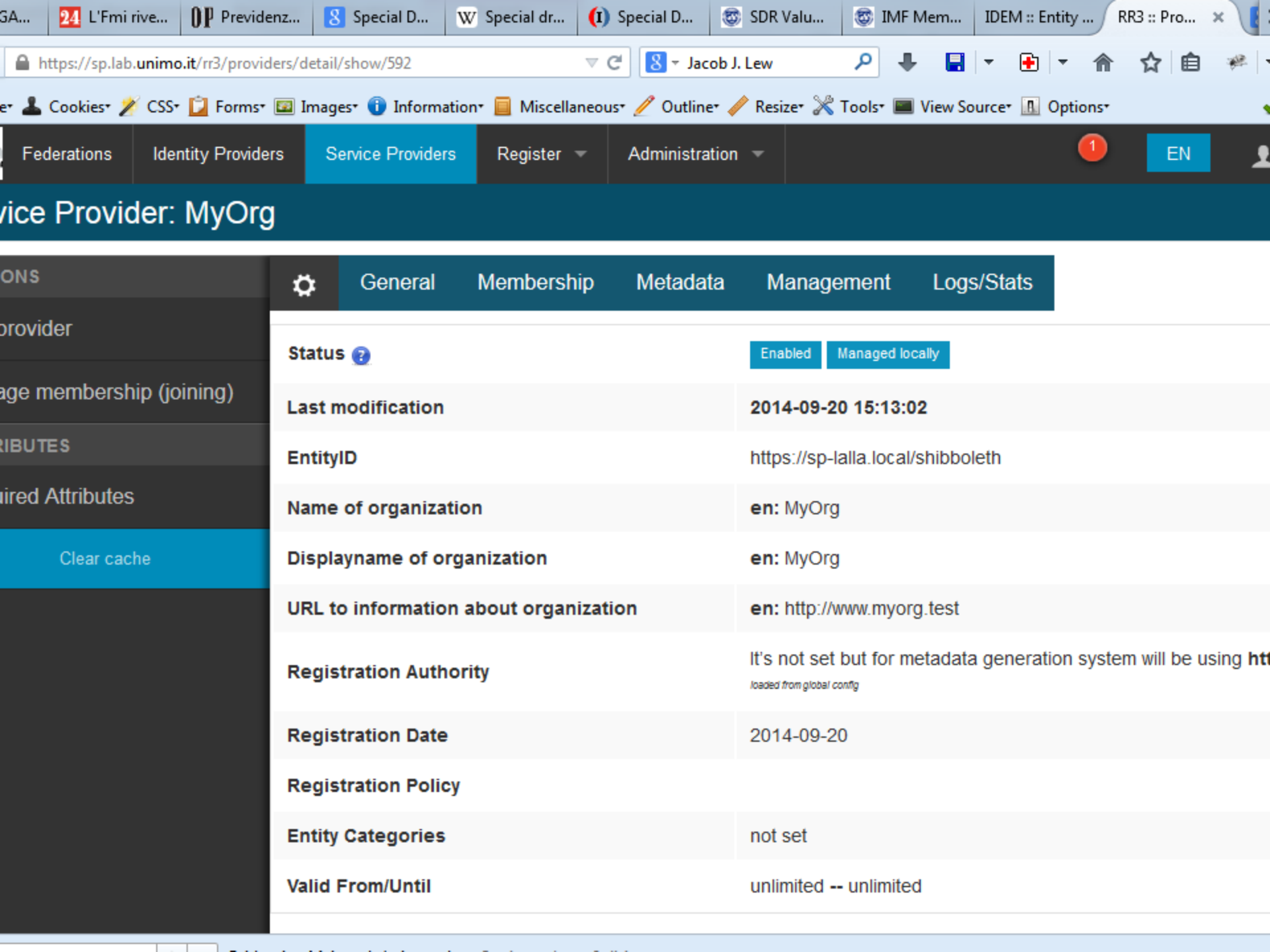
end point deve essere https

Autocompilazione certificati e ACS

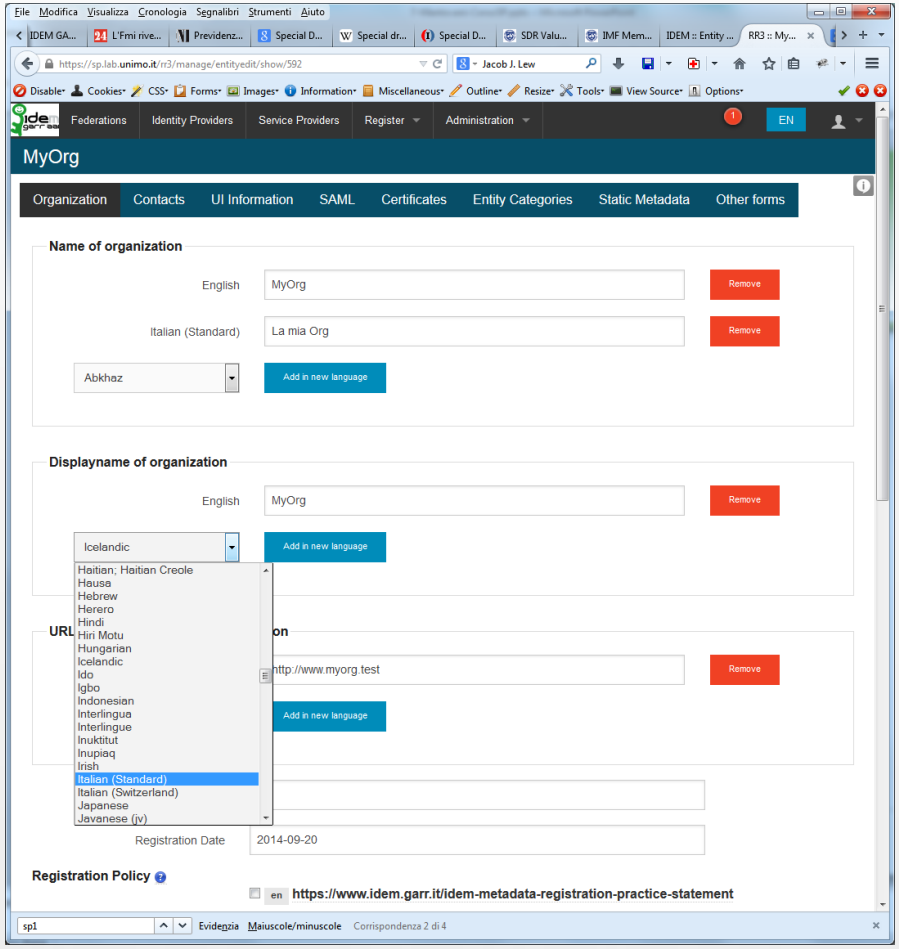


Contatti per il Registry

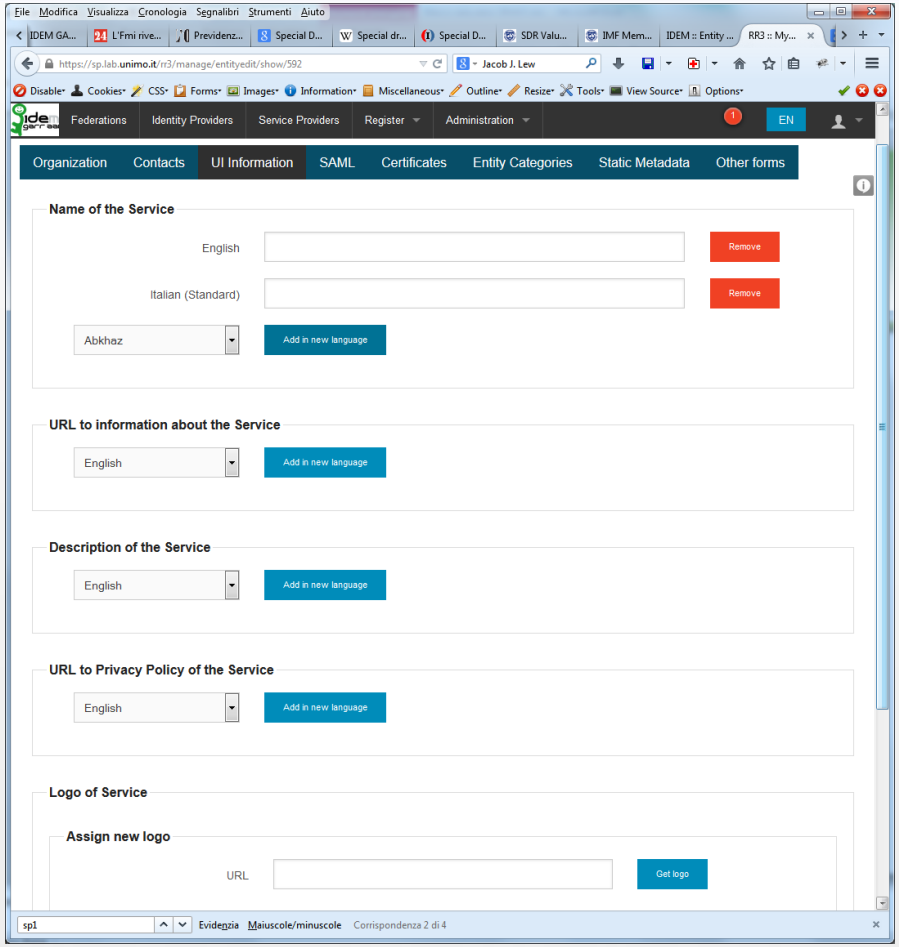



GA...
L'Fmi rive...
Previdenz...
Special D...
Special dr...
Special D...
SDR Valu...
IMF Mem...
IDEM :: Entity ...
RR3 :: Pro...
https://sp.lab.unimo.it/rr3/providers/detail/show/592
Jacob J. Lew
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
Federations
Identity Providers
Service Providers
Register
Administration
1
EN
vice Provider: MyOrg
ONS
provider
age membership (joining)
RIBUTES
ired Attributes
Clear cache
General
Membership
Metadata
Management
Logs/Stats
Status
Enabled
Managed locally
Last modification
2014-09-20 15:13:02
EntityID
https://sp-lalla.local/shibboleth
Name of organization
en: MyOrg
Displayname of organization
en: MyOrg
URL to information about organization
en: http://www.myorg.test
Registration Authority
It's not set but for metadata generation system will be using htt
loaded from global config
Registration Date
2014-09-20
Registration Policy
Entity Categories
not set
Valid From/Until
unlimited -- unlimited

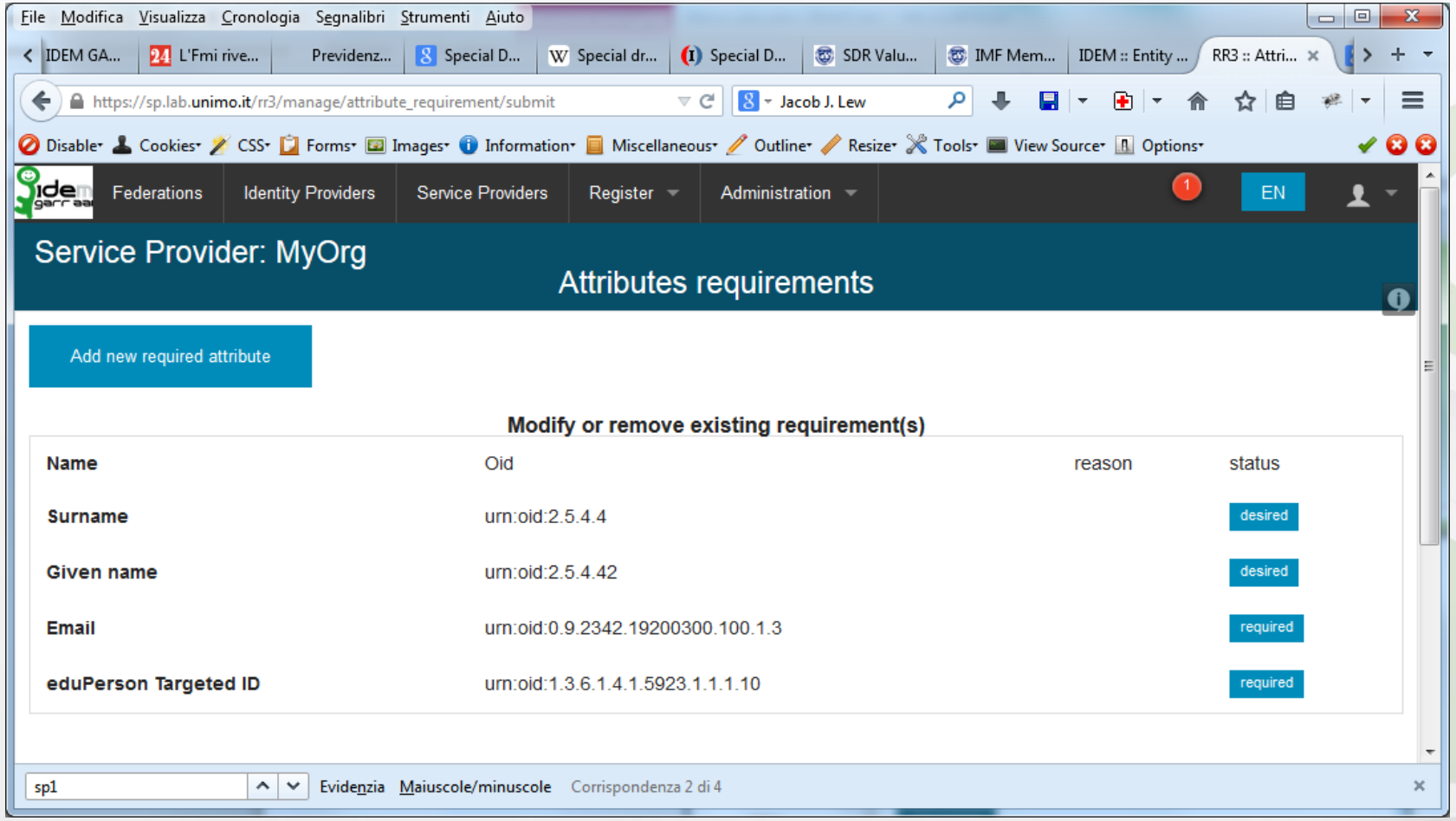
Info multilingue: Organizzazione



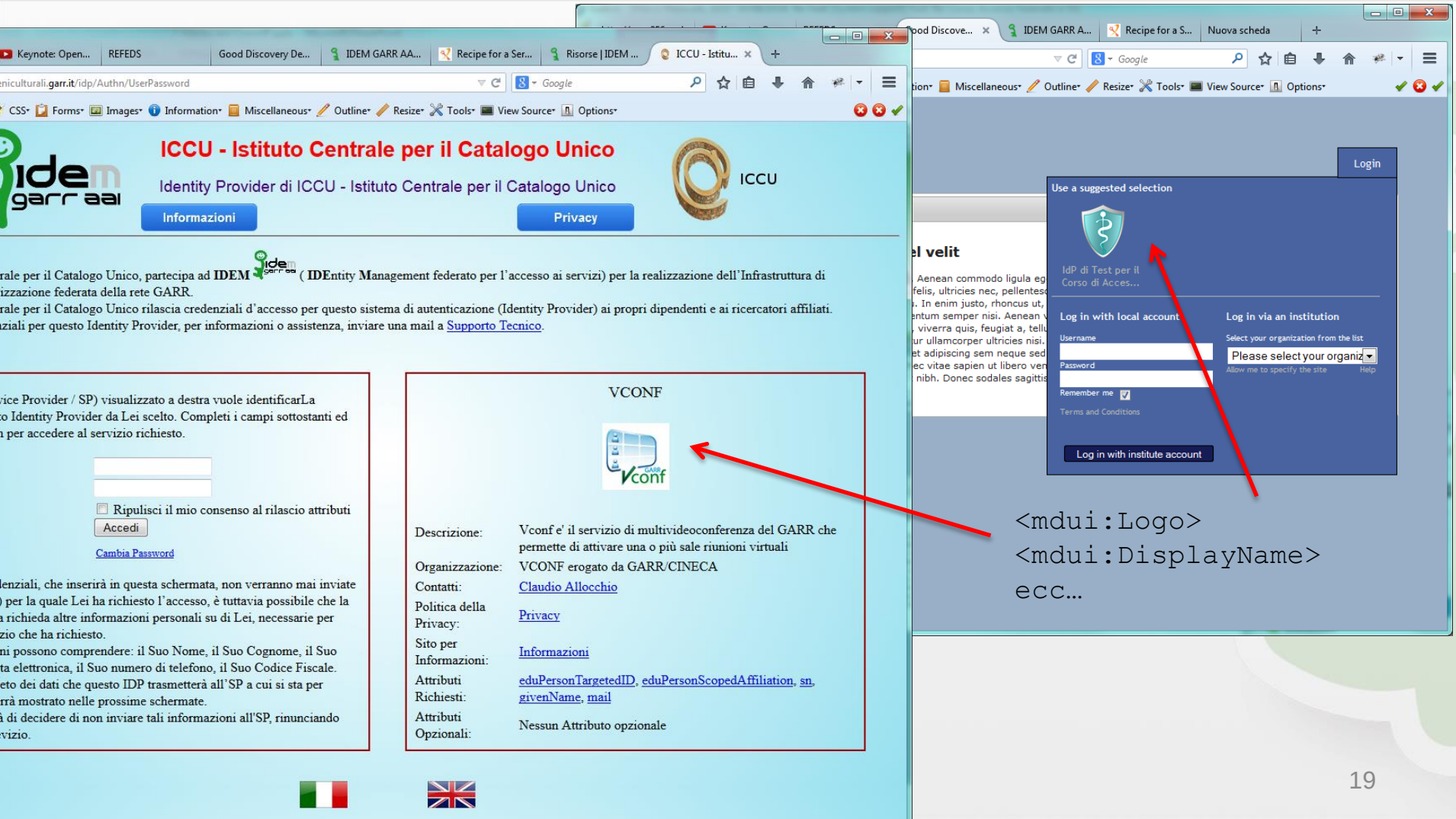
Info multilingue: Servizio



Attributi richiesti dal SP

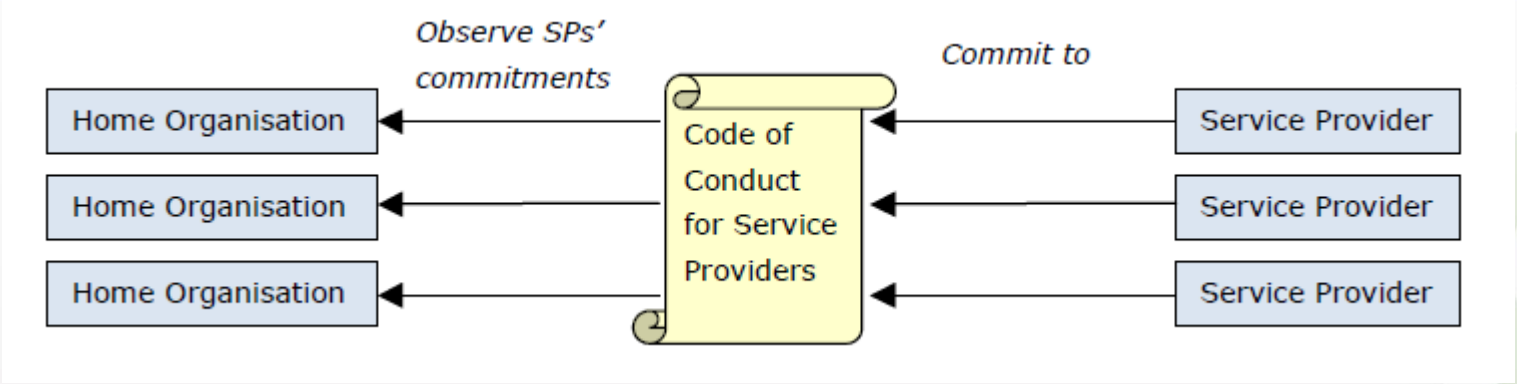


Display in IDP e DS



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
- 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

Venite attivati nella federazione IDEM-TEST

Riceverete una email da 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

Se l'Organizzazione NON è collegata a GARR

=> **Accordo di collaborazione**

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

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 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: 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