Lecture no. 5

Register a Service Provider in the IDEM federation and in the eduGAIN inter-federation
IDEM Federation: circle of trust in Italy of IdPs and SPs of the Research & Education sector

https://www.idem.garr.it

- The IDEM GARR AAI service (idem-help@garr.it) keeps up to date the metadata of all IdPs and SPs belonging to the federation.
- At present, 116 SPs and 73 IdPs
- An SP registered in the IDEM federation can offer its services to ~3 million potential users in the R&E sector
eduGAIN inter-federation: circle of trust at global level in the Research & Education sector

http://www.edugain.org

- The IDEM Federation is a member of eduGAIN
- An SP that, through IDEM, is registered in eduGAIN, can offer its services to ~16 million potential users of many countries
- At present, 1459 IdPs and 1001 SPs
Circle of trust: metadata update
How to join

https://www.idem.garr.it/en/join

Are you ready to join the Federation?

Joining the Federation is easy - the IDEM GARR AAI service can provide you with information and assistance at every step of the process.

Who can join?

All organisations connected to GARR, the Italian National Research Network (i.e., Universities and research organizations) can join the Federation as full members. In addition, third-party organisations (i.e., publishers, software service providers, etc.), can join the Federation as partners. In case they provide relevant contents or services to the education and research community. Full membership participation is subject to the IDEM Policy Committee’s approval.

Test environment

Organisations considering joining the IDEM Federation can freely use the Federation's Test Environment to test their identity Provider or Service Provider services. Access to the Test Environment is granted on request by the IDEM GARR AAI service. To activate the service, organisations should send a request to idem-help@garr.it. Joining Test Environment is mandatory before you can register your IDP or SP in the official IDEM Federation, to ensure the service is compliant with Federation requirements.

Signing the Member Accession Form or Memorandum of Understanding

To become a member of the Federation, organisations must sign either the Member Accession Form (for members), or the Memorandum of Understanding (for partners), and send two copies of the signed document to Consortium GARR, Via del Tullio d'Osio 16, 00198 Roma. In addition, a pdf copy should be sent to idem-help@garr.it. Please note that, in order to be valid, the form must be signed by an authorised representative of the organisation. Template forms are available on the IDEM website at Forms.

Approval by the Federation

Once the signed Member Accession Form or the Memorandum of Understanding has been received, your membership application will be submitted to the IDEM Policy Committee for approval. The IDEM Federation will notify applicants about the approval or rejection of their request.

Moving to the Production Environment

Once the membership application has been approved by the IDEM Policy Committee, the IDEM GARR AAI service will be available to assist you with transitioning your services from the test environment to the production mode.
<table>
<thead>
<tr>
<th>An Organisation must</th>
<th>An SP must</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Accept the <strong>Rules of the Federation</strong></td>
<td>• Be compliant with <strong>Technical Specifications</strong></td>
</tr>
<tr>
<td>• Accept the <strong>Rules of Participation</strong></td>
<td>• Be compliant with <strong>Technical Specifications of Attributes</strong></td>
</tr>
<tr>
<td>• Sign and send the <strong>Accession Form</strong> (for Members) or the <strong>Memorandum of Understanding</strong> (for Partners)</td>
<td>• Be compliant with the <strong>Metadata Profile</strong></td>
</tr>
<tr>
<td>• Sign and send the <strong>Resource Registration Request</strong></td>
<td>• Follow the <strong>Best Practices</strong> (Recommended)</td>
</tr>
<tr>
<td></td>
<td>• Be compliant with the <strong>Code of Conduct</strong> (Recommended)</td>
</tr>
</tbody>
</table>
Your SP metadata

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">
...

There are a lot of important things... but as many are missing
Metadata Profile for IDEM

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

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

Andrea Biancini – Consortium GARR
<table>
<thead>
<tr>
<th>ITALIANO</th>
<th>ENGLISH</th>
</tr>
</thead>
<tbody>
<tr>
<td>L'IDEM Entity Registry è l'applicazione, amministrata dalla Federazione</td>
<td>The IDEM Entity Registry is an application, provided by the IDEM</td>
</tr>
<tr>
<td>IDEM, che si occupa della raccolta, della gestione e della visualizzazione dei suoi Metadati.</td>
<td>Federation, that collects, manages and visualizes the federation's</td>
</tr>
<tr>
<td>Attribuendo di essi gli utenti, amministratori e contatti tecnici, delle</td>
<td>With this application the users, administrators and technical contacts</td>
</tr>
<tr>
<td>varie Organizzazioni potranno gestire le informazioni contenute nei</td>
<td>of different Organisations are able to manage the information</td>
</tr>
<tr>
<td>propri metadati in modo facile e veloce attraverso una pratica</td>
<td>contained in their metadata with a simple, fast and practical</td>
</tr>
<tr>
<td>interfaccia grafica.</td>
<td>Graphics User Interface.</td>
</tr>
<tr>
<td>Per ricevere supporto rivolgersi al IDEM Help</td>
<td>To receive support contact the IDEM Help</td>
</tr>
<tr>
<td>Questo servizio rispetta la seguente Privacy Policy</td>
<td>This service follows this Privacy Policy</td>
</tr>
<tr>
<td>Fai LOG IN per modificare le entità che hai già registrato.</td>
<td>To modify the metadata of your entities, please LOG IN</td>
</tr>
<tr>
<td>Per registrare una nuova entità utilizzare i link sottostanti</td>
<td>To register new entities, use the links below.</td>
</tr>
</tbody>
</table>

**Inserisci un Nuovo Identity Provider nella Federazione IDEM Test**

**Insert a New Identity Provider into the IDEM Test Federation**

**Inserisci un Nuovo Service Provider nella Federazione IDEM Test**

**Insert a New Service Provider into the IDEM Test Federation**
IdP Display and Discovery Service

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

VCONF

Descrizione:
VCONF è il servizio di multivideconferenza del GARR che permette di attivare una o più sole riunioni virtuali.

Organizzazione:
VCONF erogato da GARR-CINECA

Nome: Claudia Allecchie

Politica della Privacy:
Privacy

Sito per le Attività:
Informazioni

Attributi:
eduPersonTargetedID, eduPersonScopedAffiliation, givenName, mail

Attributi Opzionali:
Nessun Attributo opzionale

Use a suggested selection

Log in with local account
Log in via an institution
Select your organization from the list

Please select your organization

Log in with institute account

Terms and Conditions

<mdui:Logo>
<mdui:DisplayName>
etc.
Code of conduct for SPs

- Enables **safe attribute release** between Identity and Service Providers within EU


- **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)
The IDEM-Test Federation

After **having sent the SP Metadata** to IDEM

- through the Entity Registry
- or via email to **idem-help@garr.it**

the **new service is activated** in the IDEM-Test Federation

Service administrators receive an email from **idem-help@garr.it** with the instructions to **configure the SP with the Metadata** (mandatory) and the Discovery Service (optional) of the test federation

---

The transition through the Test Federation is mandatory in order to access the official IDEM Federation
How to officially join the IDEM Federation

• If the Organisation is already connected to GARR (but not yet to IDEM)
  => **Accession Form**
  • [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)

• If the Organisation is NOT connected to GARR
  => **Memorandum of Understanding**
  • [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)

• For each SP => **Resource Registration Request (RRR)**
  • [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)

• Legal Representative, Organisation’s Representative, Technical Representative and Technical Contact Person are responsible towards the Federation
  • [https://www.idem.garr.it/documenti/regolamento](https://www.idem.garr.it/documenti/regolamento)
Approval procedure

The Federation, through the GARR IDEM AAI Service:

- **Receives** the official documentation (RA/AC, RRR)
- **Checks** the Metadata
- **Checks** the certificates of the services for HTTPS connections
- **Checks** the completeness of the information provided about the SP (through the inspection of its website)
- **Checks** the Requested Attribute(s)
- **Controls** the metadata synchronisation time interval
Activation in the official Federation

Once the approval procedure is successfully completed, the SP is moved from the test to the official IDEM Federation

Service administrators receive from idem-help@garr.it the instructions to download the official Metadata

- of IDEM
- and of eduGAIN (if the SP has not «opted-out»)

Instructions are also available at:
https://www.idem.garr.it/informazioni-tecniche/metadati
IDEM Community

• Mailing list: idem-users@garr.it
• Mailto: majordomo@garr.it subscribe idem-users
• Discuss principles and/or technical issues related to:
  • Identity and Access Management,
  • Authentication and Authorisation Infrastructures,
  • The IDEM Federation
• Or just to discuss with other members of the federation
Any questions?