



Authentication and Authorisation for Research and Collaboration

INTERNAZIONALIZZAZIONE CON EDUGAIN:

Verso un rilascio più scalabile e sicuro degli attributi degli utenti

Maria Laura Mantovani, Simona Venuti, Marco Malavolti

NA2, AARC

IDEM GARR AAI Service, GARR

IDEM DAY 2016, Roma

7 June 2016



Agenda

9:00-10:30

- Introduction to new federated technologies
 - eduGAIN needs IdP collaboration to work
 - The attribute release problem
- Entity categories as a solution
 - Research & Scholarship EC
 - GÉANT Data Protection Code of Conduct EC
- -----

• 10:30-11:00 BREAK

• -----

11:00-12:30

- Legal ground for ECs
- Attribute release process, easy IdP configuration if supported by federation
 - Fill missing values
 - Easy configuration for entity category support
 - Federation registry: a valid helper in attribute release configuration

Evolution of Identity Techniques

Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in once
- Users sign in 'once'
- Applications cannot see the user's password

Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

Evolution of Identity Techniques

Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own

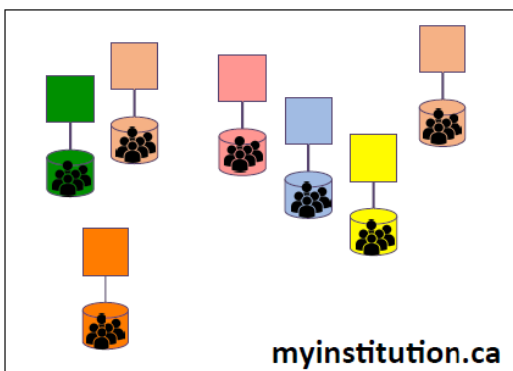
Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in 'once'
- Applications cannot see the user's password

Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

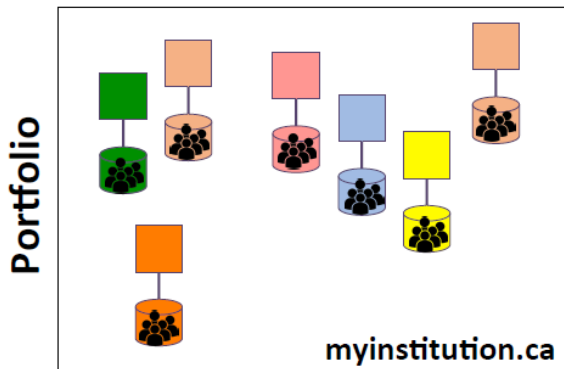
Portfolio



Evolution of Identity Techniques

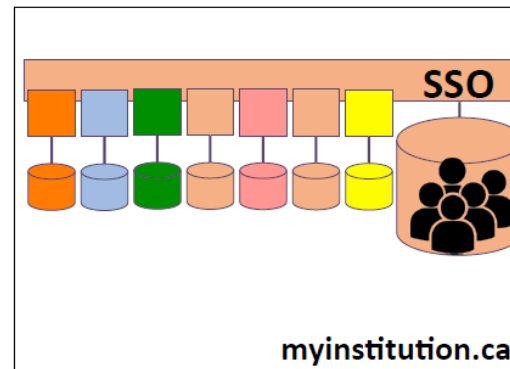
Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own



Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in 'once'
- Applications cannot see the user's password



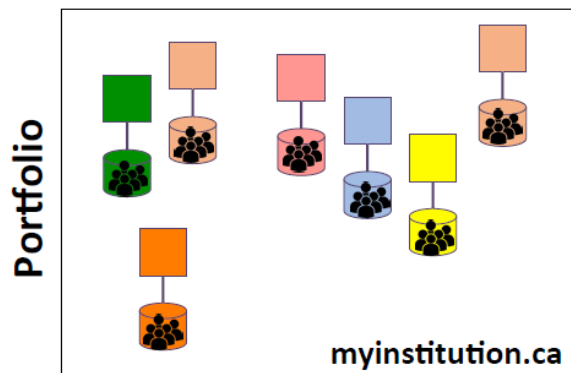
Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled

Evolution of Identity Techniques

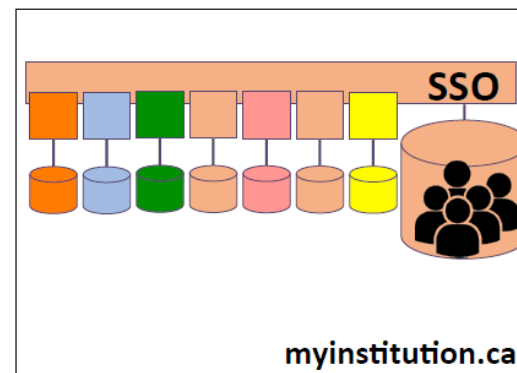
Application Centric IdM

- Services activated, but little interaction between them
- Applications have distinct userID/password pairs of their own



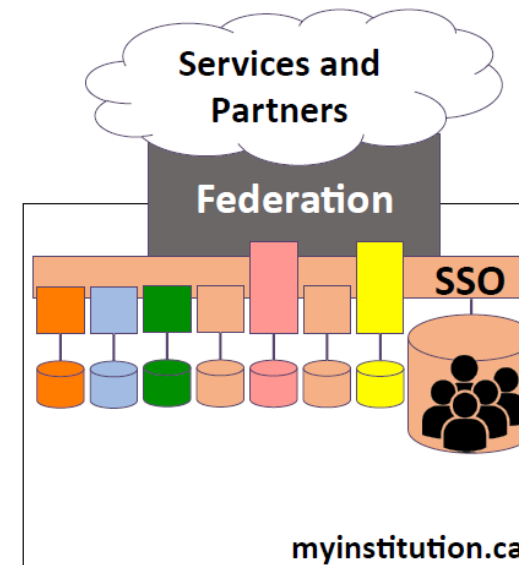
Centralizing Campus Directory & Sign-On

- Services are easier to turn on
- Users are using same password
- Campus SSO users sign in 'once'
- Applications cannot see the user's password

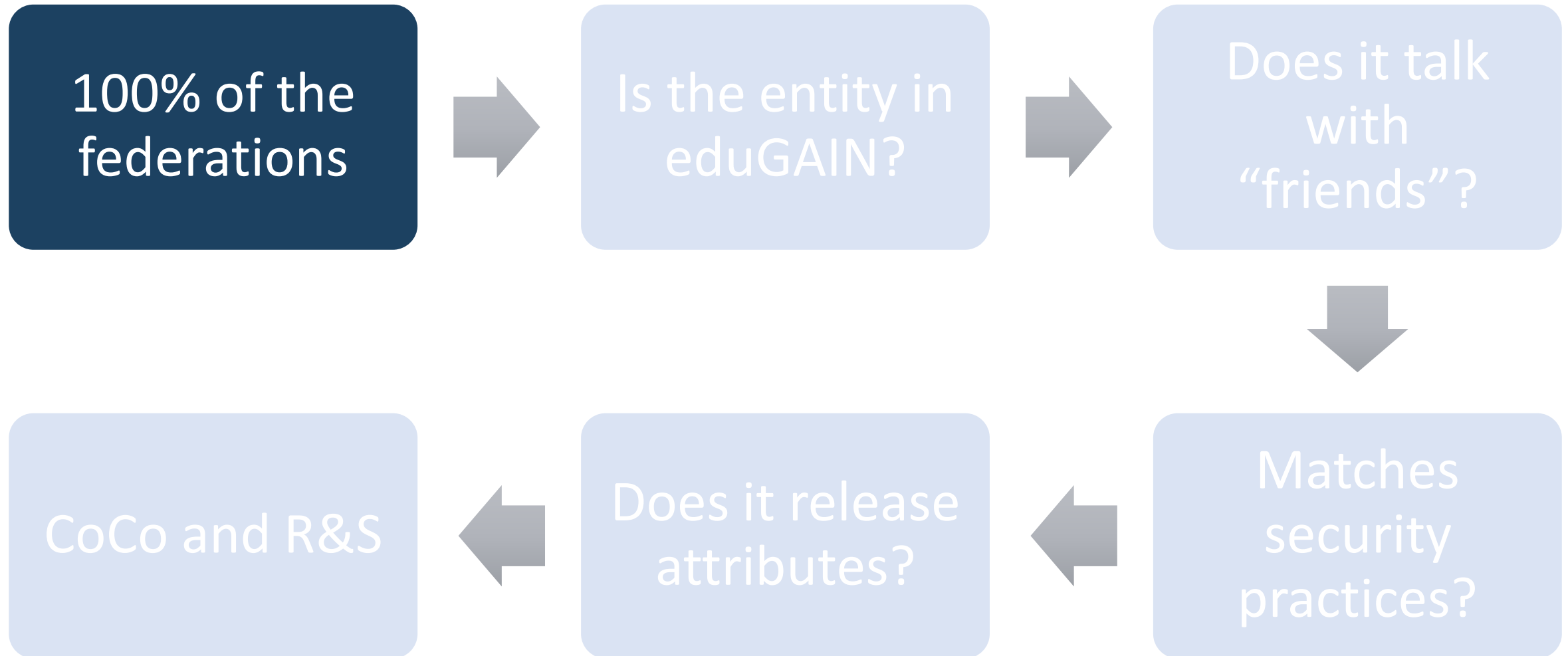


Federated SSO

- Faster service turn-up time – config and go
- Minimized attack/risk surface inherent in design
- Services outside your domain more easily enabled



Campaigns for “eduGAIN works”



eduGAIN & Federation Status

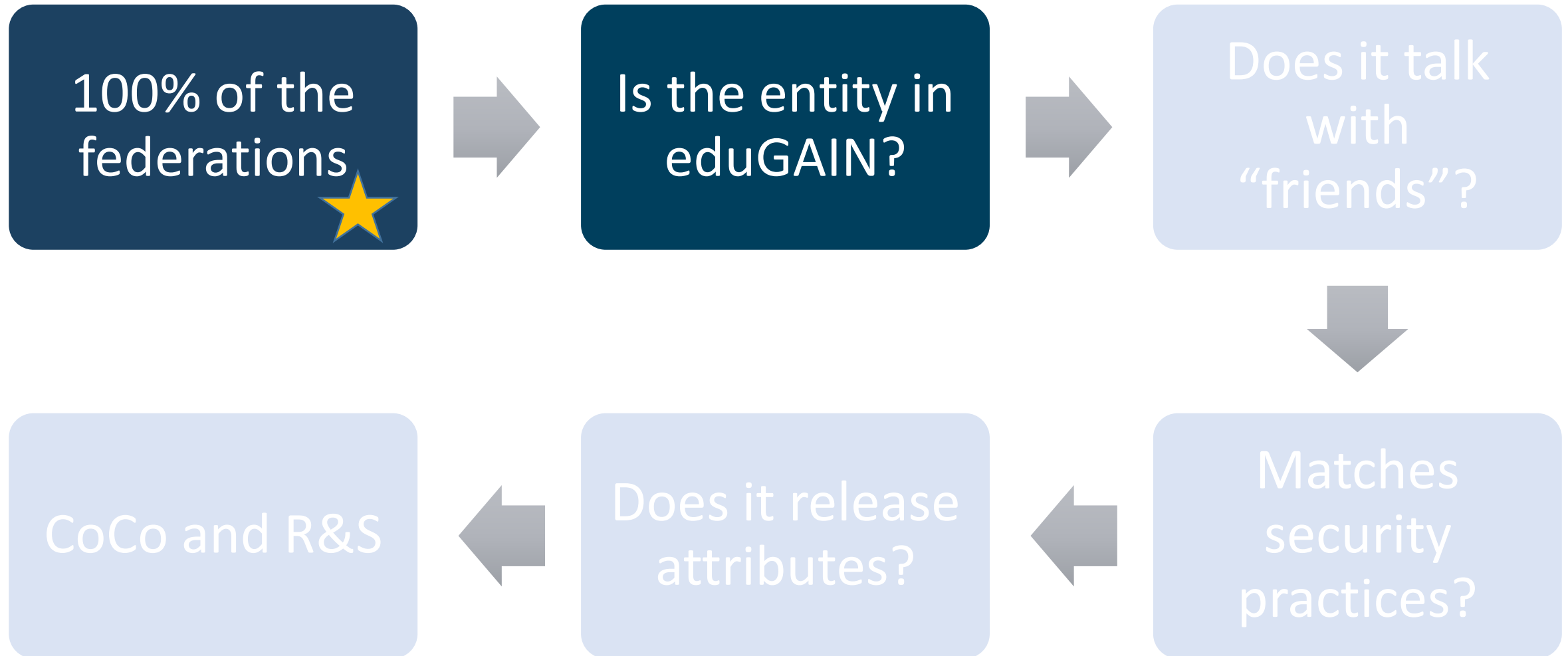


24/06/2013

March 2016

- 38 eduGAIN Members
- 5 Joining eduGAIN
- 8 Candidate Federations
- 10 Known Federations

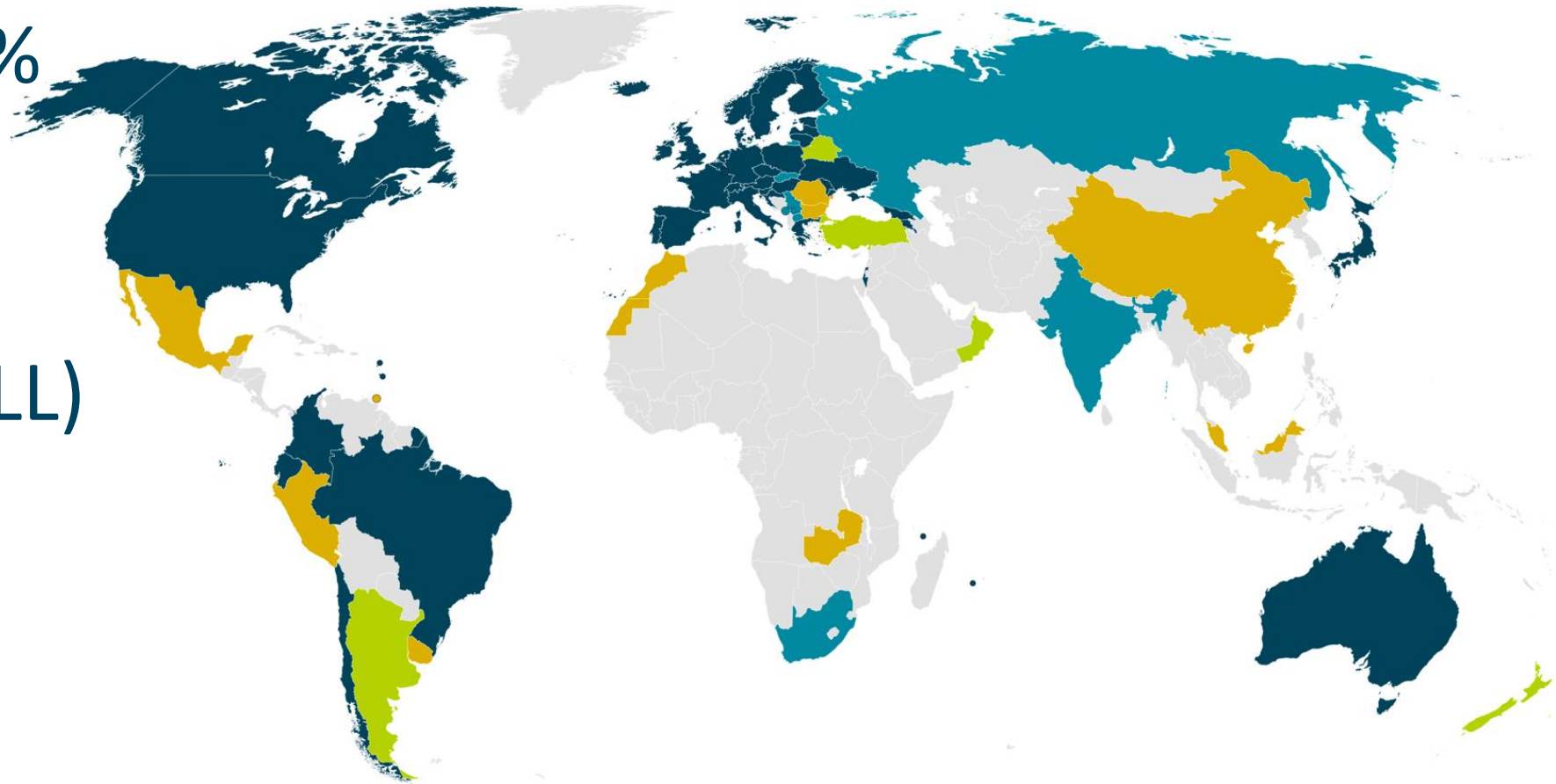
Campaigns for “eduGAIN works”



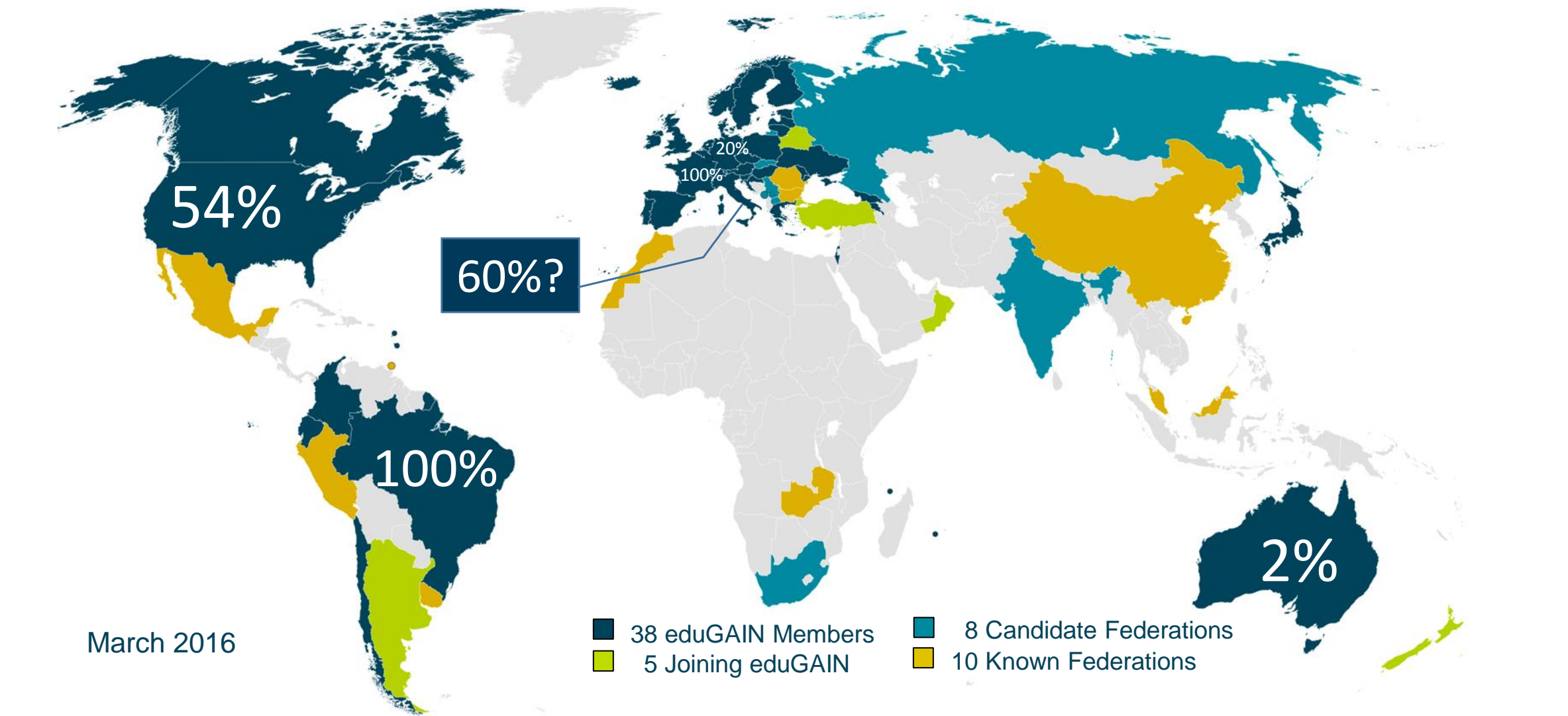
eduGAIN vs the World!

Federations: 63%
+ joining: 70%

Entities: 27% (ALL)
IdPs: 57%
SPs: 14%



eduGAIN & Federation Status (% of entities)



Is the entity in eduGAIN?

YES, THANKS
TO OPT-OUT
POLICY FOR
IDPS

Highlights



Completata eduGAIN opt-out policy per gli IdP

Ultima modifica il Lunedì, 11 Gennaio 2016 14:34

Pubblicato Venerdì, 09 Gennaio 2015 11:04

Visite: 2388



IDEM ha completato la transizione della policy di ingresso in eduGAIN da opt-in a opt-out per i propri IdP. Dal 11/01/2015

ogni nuovo IdP che è entrato in IDEM, in forza della policy opt-out è stato aggiunto di default al flusso eduGAIN. Abbiamo ora terminato anche il passaggio ad eduGAIN di tutti gli IdP registrati in passato, raggiungendo il numero di 62 IdP italiani pubblicati nel flusso eduGAIN. Per ottenere questo risultato lo staff tecnico di IDEM esegue alcuni test di conformità sugli IdP prima di pubblicarli in eduGAIN:

[Leggi tutto: Completata eduGAIN opt-out policy per gli IdP](#)

Da OPT-IN a OPT-OUT, così è cambiata la policy applicata agli IdP per entrare in eduGAIN

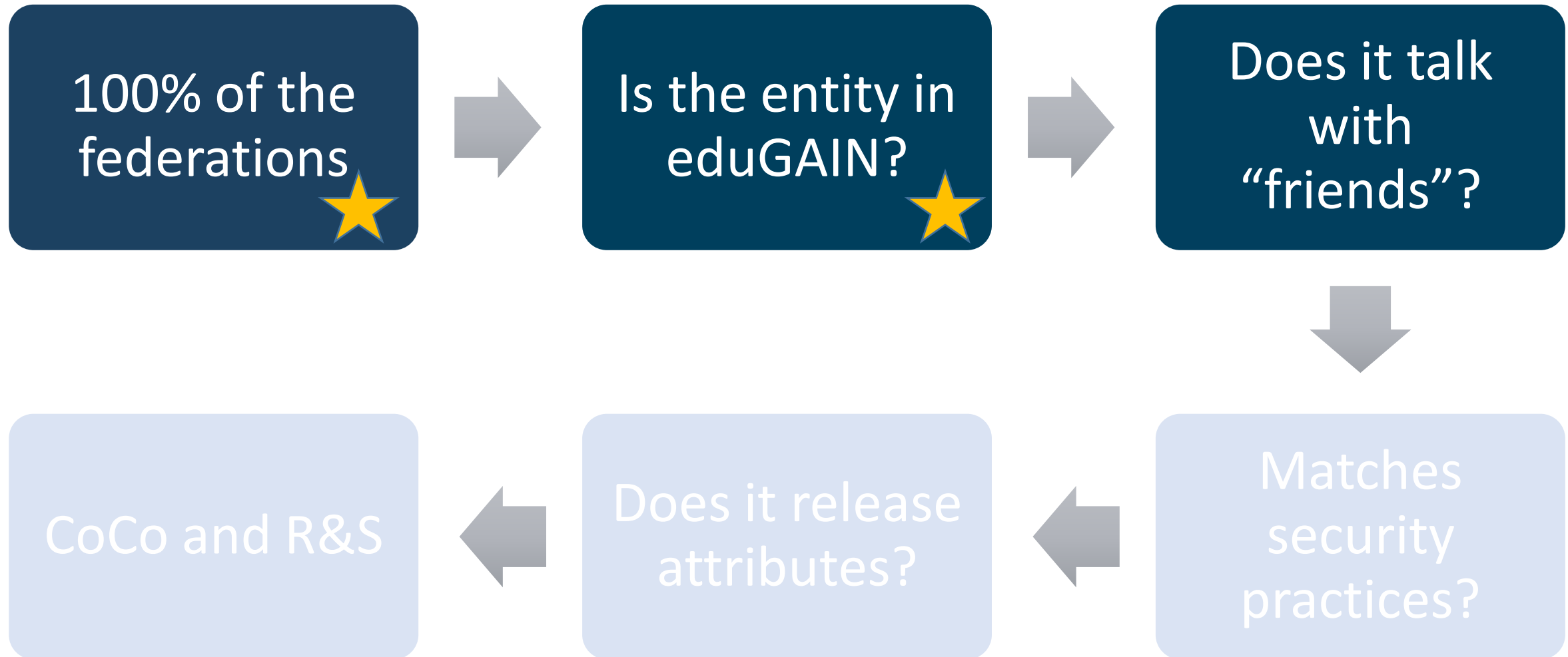
Ultima modifica il Martedì, 29 Aprile 2014 12:47

Pubblicato Venerdì, 11 Aprile 2014 16:13

Visite: 5659



Campaigns for “eduGAIN works”



Does it talk with “friends”?

<https://technical.edugain.org/eccs/>



eduGAIN Connectivity Check Service

[Identity Providers](#) | [All IdP Test Results](#) | [Instructions](#) | [Contacts](#)

Show IdPs with status: **Error** | **Warning** | **OK** | **Disabled** | [Show all](#)

Display Name ▾	entityID ▾	Registration Authority ▾	Contacts	Last Test ▾	Current Result ▾	Tests
<input type="text"/>	<input type="text"/>	<input type="text" value="idem"/>	T: Technical, S: Support		All ▾	<input type="button" value="Search"/>
IdP data				Last test results		
CNR Bologna Research Area	https://biblio.bo.cnr.it/idp/shibboleth	http://www.idem.garr.it/	T: biblio-idem@area.bo.cnr.it T: biblio-idem@area.bo.cnr.it	2016-05-31 03:01:47	OK	View
IDP in the Cloud Project (GARR)	https://garr-idp-prod.irccs.garr.it/idp/shibboleth	http://www.idem.garr.it/	T: system.support@garr.it	2016-05-31 03:01:42	OK	View
University of Verona (nuovo)	https://giasso.univr.it/idp/idem	http://www.idem.garr.it/	T: sistemi@ateneo.univr.it	2016-05-31 03:20:11	OK	View
CNR Institute of Clinical Physiology	https://idea.ifc.cnr.it/idp/shibboleth	http://www.idem.garr.it/	T: idem@ifc.cnr.it	2016-05-31 03:01:47	OK	View
CNR Institute for Computational Linguistics "Antonio Zampolli"	https://idem-idp.ilc.cnr.it/idp/shibboleth	http://www.idem.garr.it/	T: idem@ilc.cnr.it T: idem@ilc.cnr.it S: idem@ilc.cnr.it	2016-05-31 03:01:55	OK	View
IMT Institute for Advanced Studies Lucca	https://idem-idp.imtlucca.it/idp/shibboleth	http://www.idem.garr.it/	T: webmaster@imtlucca.it	2016-05-31 03:01:43	OK	View
National Institute for Astrophysics - INAF	https://idem.ced.inaf.it/idp/shibboleth	http://www.idem.garr.it/	T: m.nanni@ira.inaf.it T: f.tinarelli@ira.inaf.it T: inaf-idem@ced.inaf.it	2016-05-31 03:01:57	OK	View
Second University of Naples	https://idem.unina2.it/idp/shibboleth	http://www.idem.garr.it/	T: csi@unina2.it	2016-05-31 03:02:01	OK	View

Does it talk with “friends”?

YES, THANKS
TO THE NEW
METADATA
DISTRIBUTION

IDEM Metadata distribution UPDATE

Published on Tuesday, 04 March 2014 13:52

Hits: 1945

Dear Italy-IDEM Federation Participants,

according to the new standards and security assessment/upgrade, and the inter-federation agreements, in order to reach a higher security standard level and a major inter-operability between federations, Italy-IDEM Federation set a new distribution system for its Federation metadata.

In the meantime we have a new metadata signing key due to the expiration of the metadata signing certificate in use.

New certificate available at https://www.idem.garr.it/documenti/doc_download/321-idem-metadata-signer-2019

1- Idem Federation metadata will be distributed in four different forms:

- a) with SHA-256 hash signed
- b) with SHA-1 hash signed (NEW key). Please keep in mind that SHA-1 is becoming obsolete during the current year (2014), so you are kindly asked to upgrade your systems as soon as possible.
- c) with SHA-1 hash signed (OLD key, expiring on the 17th of April 2014). Please keep in mind that SHA-1 is becoming obsolete during the current year (2014), so you are kindly asked to upgrade your systems as soon as possible.
- d) not signed available only until the 15th of January 2015

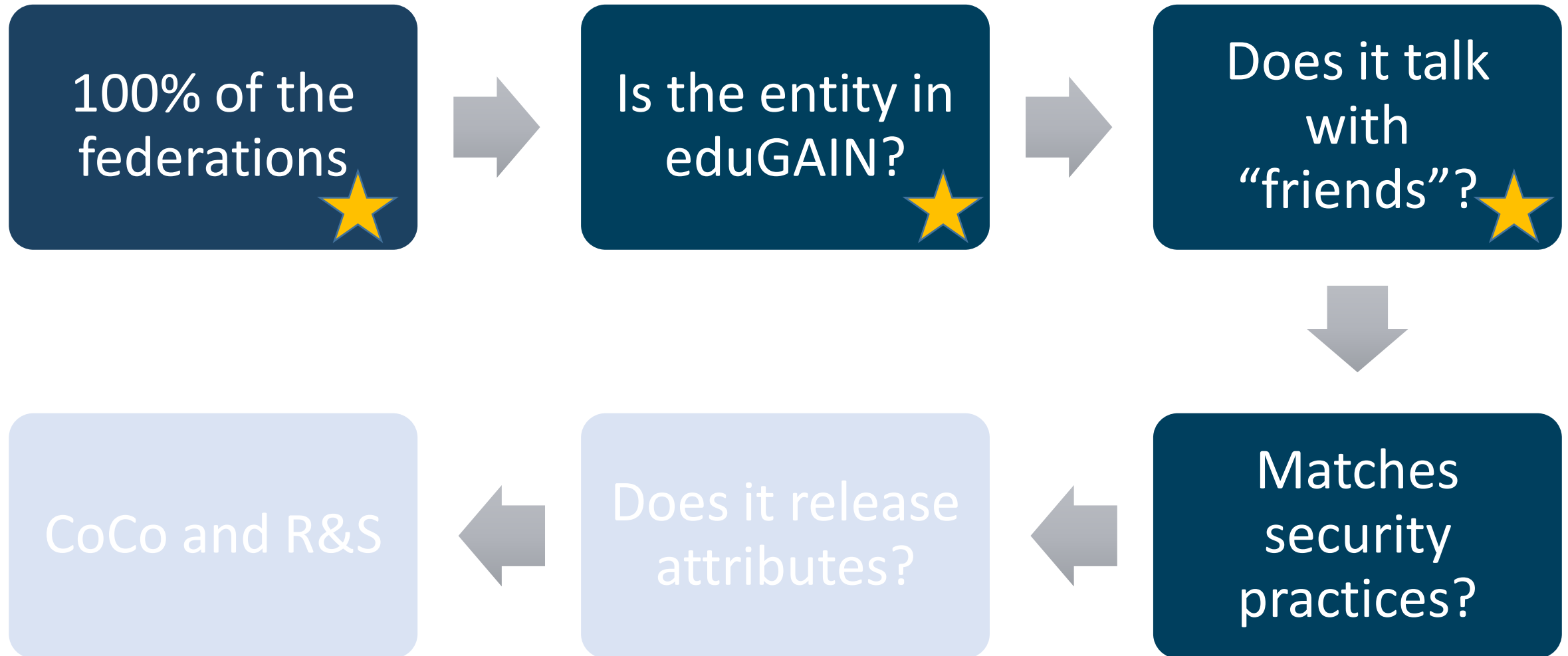
The new locations of Italy-IDEM metadata are:

Italy-IDEM Federation (Production):



04/03/2014

Campaigns for “eduGAIN works”



We have experienced the severity of the problem

07/04/2014

A very serious bug in OpenSSL 1.0.1 was announced this afternoon:

<http://heartbleed.com/>

The actual direct impact on the Shibboleth software packages is relatively minimal in comparison with the fallout from this. The only distribution of OpenSSL included with any Shibboleth software is the Windows SP.

I'm not waiting to produce an actual advisory on this before saying something because this is a major, major bug and it's public.

I am working to prepare a patch for this (I had no advance warning) and it will be done as soon as I can produce it. It will **only** apply to the supported SP version, which is 2.5.3. Anything older than 2.5.0 didn't include an affected OpenSSL version, but **any 2.5.x version will need to be updated to 2.5.3 and then patched.**

Any other SP version is still vulnerable if used with OpenSSL 1.0.1, but I don't control the process of obtaining an update, so that will depend on your OS or local build.

On the IdP side, this is really a matter for deployment considerations. We don't provide the actual web server and TLS implementation for the IdP, so you would need to evaluate your choices there and determine whether OpenSSL 1.0.1 is implicated. Obviously pure Java solutions hosting the IdP are not, though some Java containers can be configured to use OpenSSL as a TLS stack for performance reasons.

As to the implications, this is a very severe bug, and has apparently been shown to leak the private key used on the server or client. In the case of an IdP, that usually means the potential exposure of **the** signing key because that key usually doubles as a server key for SOAP traffic on a second port.

In the case of the SP, there is, I think, somewhat less risk because the SP doesn't generally contact arbitrary servers that might be used to attack it, but that doesn't guarantee safety.

In the security parlance, keys at risk are basically considered compromised and the official advice would have to be to revoke and replace them. **I would imagine that federations will be moving on this to help people understand and react to this, but I felt an obligation to say something in the interim, given the gravity of the bug.**

-- Scott Cantor
Shibboleth Project/Consortium

Matches security practices?

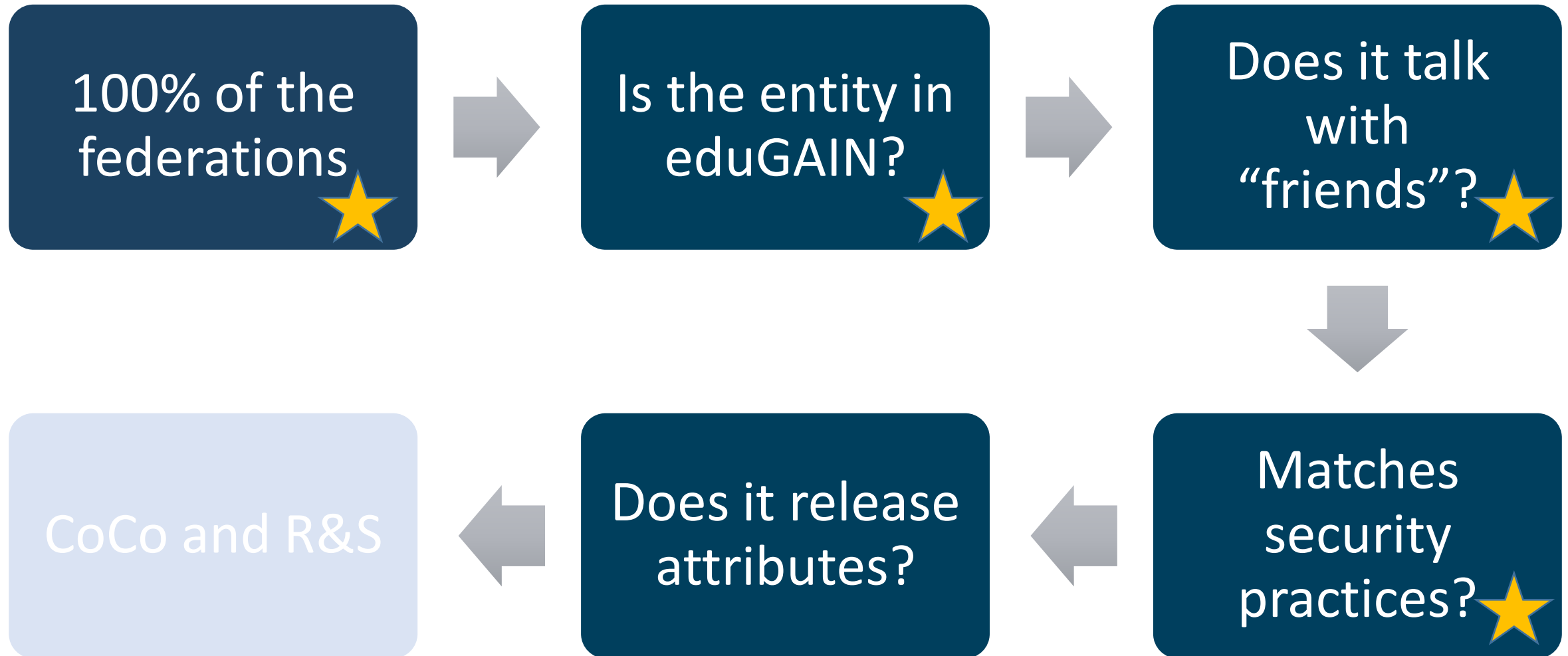
IDEM help desk performs this audit every 2 months

<https://www.ssllabs.com/ssltest/>

Answers here:

<https://goo.gl/6prNMg>

Campaigns for “eduGAIN works”



Trust and Identity today

Classic Identity Federations interoperating via eduGAIN



Identity Provider (IdP) asserts authentication and information about users.

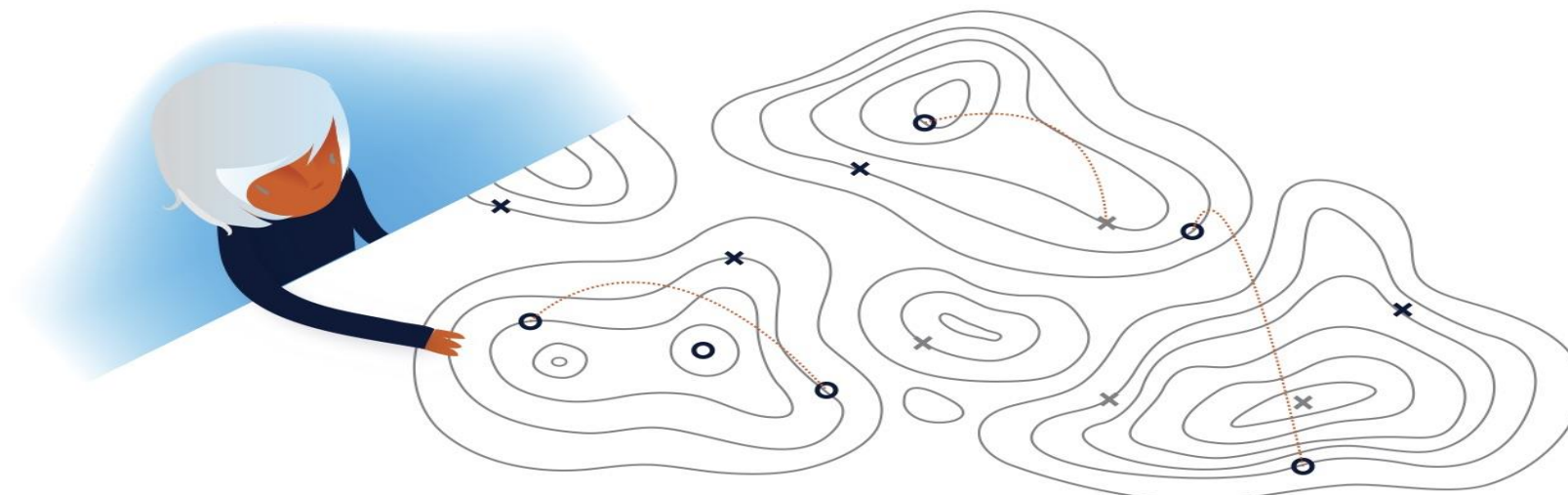


Service Providers (SP) check and consume this information for authorization and make it available to an application

A group of organizations running IdPs and SPs that agree on a common set of rules and standards that build trust

- <https://technical.edugain.org/status>
- <https://technical.edugain.org/entities>
- Many SPs in eduGAIN want to collaborate with our users

No researcher works in isolation




 **Neelie Kroes** ✓
@NeelieKroesEU

Following

At @CERN, "a single paper can easily have 3,000 authors" - @RHDijkgraaf
ec.europa.eu/commission_201 ...
#opendigitalscience #EUDigitalMinds
#research

RETWEETS 17 FAVORITES 5

4:51 PM - 30 Oct 2014

 **Ewan Birney**
@ewanbirney

I'm always really impressed at the intelligence, drive and diversity of students we get @emblebi across Europe and the world.

9:19am · 17 Feb 2016 · Twitter for iPad

1 RETWEET 7 LIKES

e-Research Trust and Identity Infrastructures

GENERIC



Campus

- Hundreds of thousands of users



- Thousands of services



Individual Experiments

- Tens to hundreds of individuals *

SPECIFIC

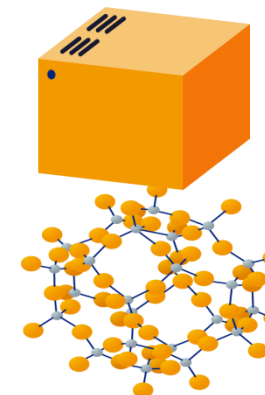
Federation

- Tens of thousands of services



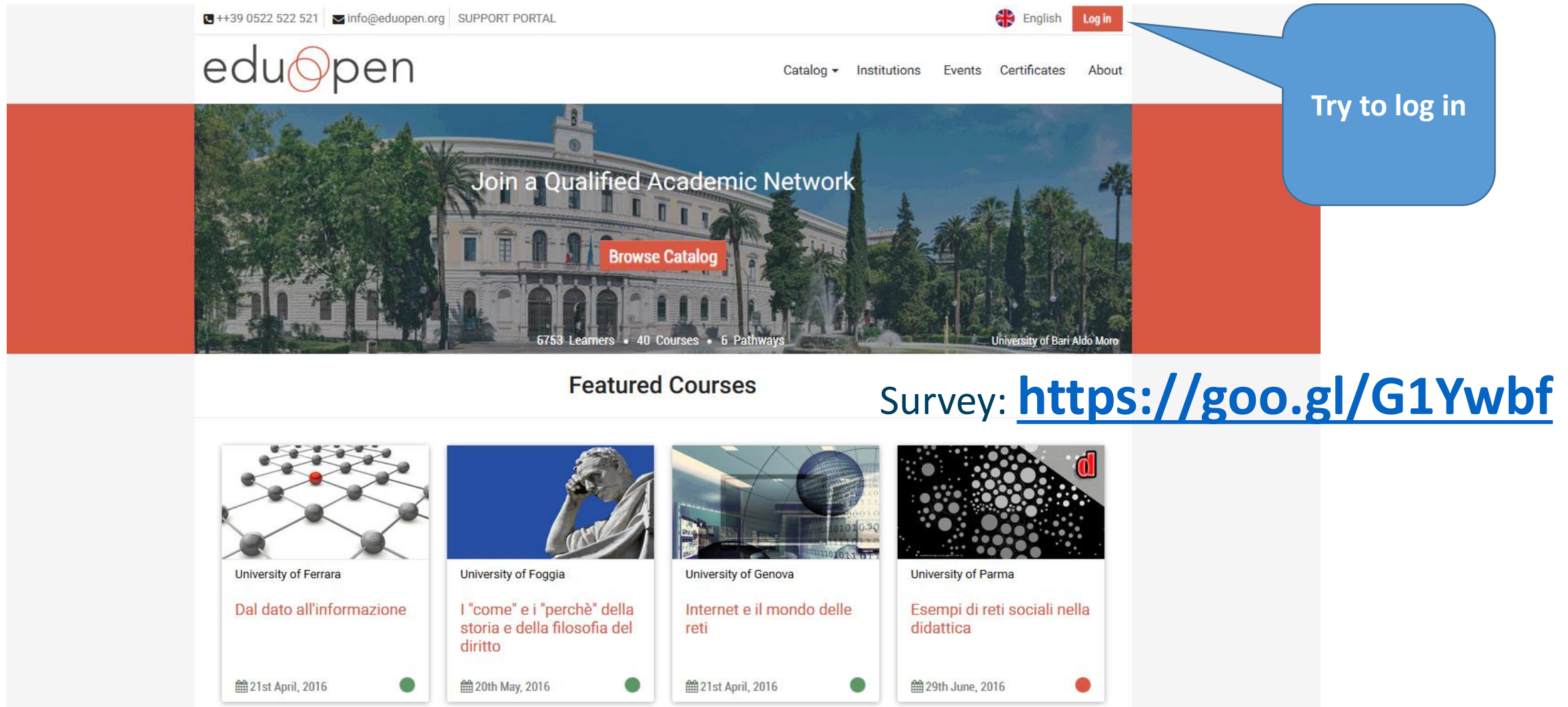
General and Specific e-Research Infrastructures

- Hundreds of services



Understand how hard for a SP to be happy in the interfederation

EduOpen Example - <https://learn.eduopen.org>



++39 0522 522 521 | info@eduopen.org | SUPPORT PORTAL

English Log in

eduopen

Catalog Institutions Events Certificates About

Join a Qualified Academic Network

Browse Catalog

6753 Learners • 40 Courses • 6 Pathways

University of Bari Aldo Moro

Featured Courses

Survey: <https://goo.gl/G1Ywbf>

University	Course Title	Date	Status
University of Ferrara	Dal dato all'informazione	21st April, 2016	Green
University of Foggia	I "come" e i "perchè" della storia e della filosofia del diritto	20th May, 2016	Green
University of Genova	Internet e il mondo delle reti	21st April, 2016	Green
University of Parma	Esempi di reti sociali nella didattica	29th June, 2016	Red



Image credit: The SXS (Simulating eXtreme Spacetimes) Project

Gravitational Waves Detected 100 Years After Einstein's Prediction

News Release • February 11, 2016

Visit The Detection Portal

See also: [LIGO Hanford Press Release](#)

LIGO Opens New Window on the Universe with Observation of Gravitational Waves from Colliding Black Holes

WASHINGTON, DC/Cascina, Italy

For the first time, scientists have observed ripples in the fabric of spacetime called gravitational waves, arriving at the earth from a cataclysmic event in the distant universe. This confirms a major prediction of Albert Einstein's 1915 general theory of relativity and opens an unprecedented new window onto the cosmos.

Gravitational waves carry information about their dramatic origins and about the nature of gravity that cannot otherwise be obtained. Physicists have concluded that the detected gravitational waves were produced during the

RELATED MEDIA

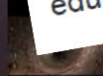


Gravitational Waves Detected 100 Years After Einstein's Prediction
News Release



InCommon
11 febbraio

Congrats to our friends at the #LIGO Scientific Collaboration on this discovery. InCommon is proud to have provided a small part of the infrastructure for collaboration, and excited to help further the reach of all scientific collaborations using federated identity technology and eduGAIN.



Two Black Holes Merge into One
Simulation Image



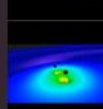
Massive Bodies Warp Space-Time
Artwork Image



LIGO Detects Gravitational Waves - announcement at press conference (part 2)
Education Video



Journey of a Gravitational Wave
Education Video



Warped Space and Time Around Colliding Black Holes
Simulation Video



The Sound of Two Black Holes Colliding
Science Video

Does your IdP works with LIGO?

LIGO Example



Survey: <https://goo.gl/2zPqvl>

LIGO needs to collaborate with you

Italian Login Providers (IdPs)



These Italian login providers (identity providers or IdPs) are of particular interest to the gravitational-wave community since there are groups of astronomers from those institutions that need to collaborate with LIGO.

This is not a static list and is expected to evolve. If you have suggestions or changes for the list please send email to [the LIGO IdP project](#).

Federated IdPs

- Dipartimento di Fisica, Università di Siena (entityID <https://shibboleth.unisi.it/idp/shibboleth>)
- INAF - National Institute for Astrophysics (entityID <https://idem.ced.inaf.it/idp/shibboleth>)
- University of Milano Bicocca (entityID <https://idp.unimib.it/idp/shibboleth>)
- Università di Padova (entityID <https://shibidp.cca.unipd.it/idp/shibboleth>)
- University of Perugia (entityID <https://idp.unipg.it/idp/shibboleth>)
- Università di Pisa (entityID <https://idp.unipi.it/idp/shibboleth>)
- INFN (all institutes) (entityID <https://idp.infn.it/saml2/idp/metadata.php>)

Not federated at this time

- ASDC - ASI Science Data Center
- Brera Observatory Milan
- Istituto Universitario di Studi Superiori of Pavia
- Università dell'Insubria
- Università di Udine



<https://wiki.ligo.org/AuthProject/EMFollowUpOrganizationsForIdMIItaly>

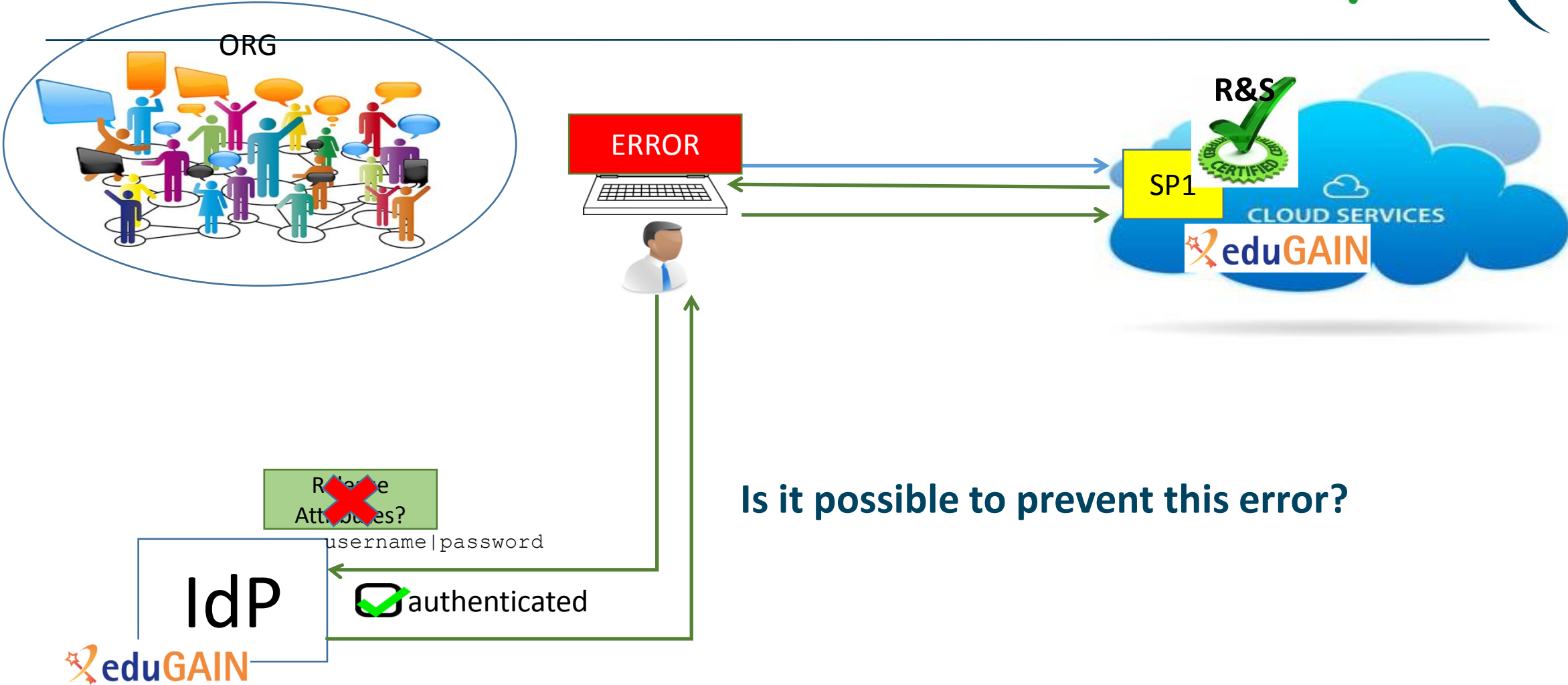
<https://wiki.ligo.org/AuthProject/EMFollowUpOrganizationsForIdM>

*Now can LIGO have some attributes please?
We have many more years of gravitational-wave astronomy
discoveries to come and realizing the full science potential
will require close collaboration with astronomers and
astrophysicists from around the world. eduGAIN and your
national federations can help make that happen.*

- Scott Koranda, lead architect for the Laser Interferometer Gravitational-Wave Observatory Identity and Access Management

- Read more about releasing attributes for Science <https://refeds.org/a/1154>

The real world of interederation



ERROR AFTER SUCCESSFUL LOGIN: Frustration of user



- The user doesn't understand the error
- The user doesn't know to whom complain
- User feels that things must work

ERROR AFTER SUCCESSFUL LOGIN: Frustration of the SP



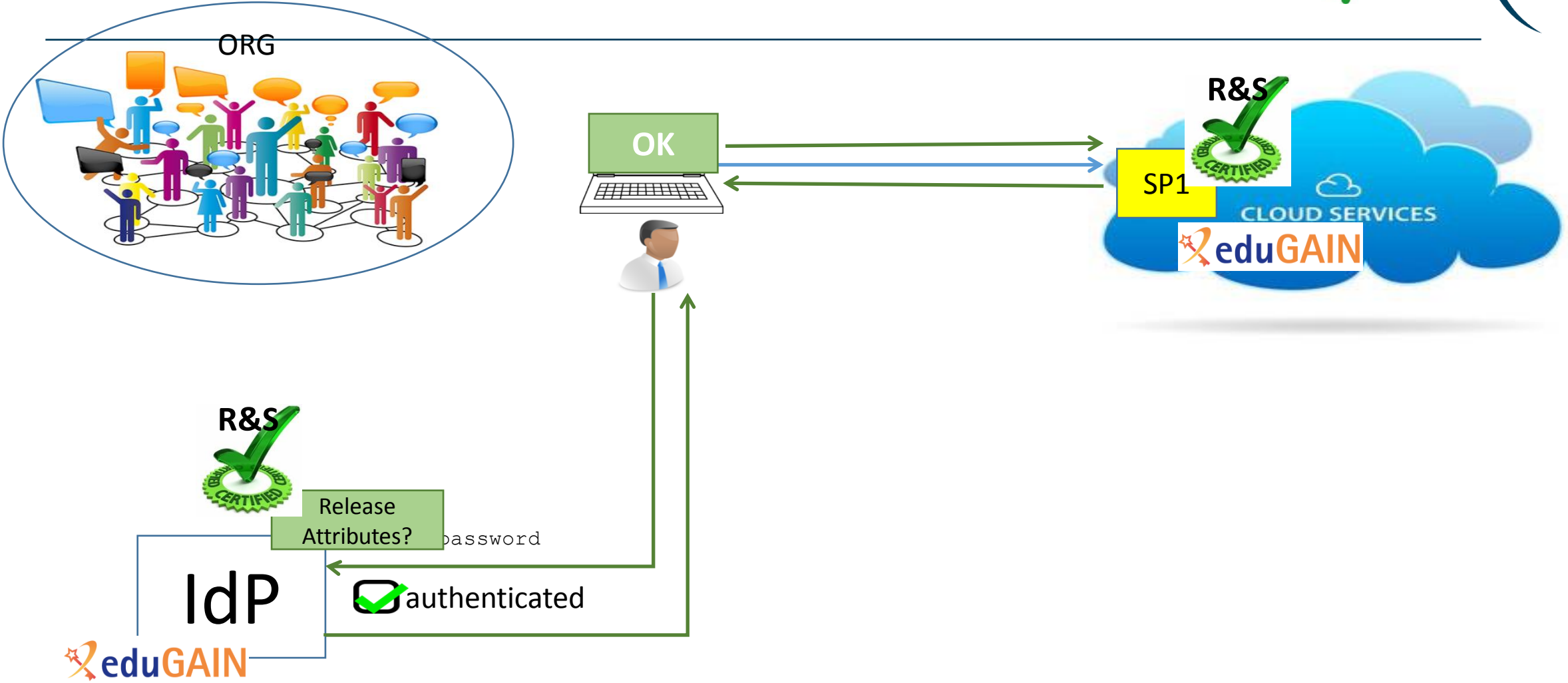
- SP has done a lot of work to domesticate the application
- SP has done a lot of work to join and be compliant with a national federation
- SP has done a lot of work to join and be compliant with eduGAIN
- The SP require attributes.
- Likely the SP comply with R&S and/or CoCo and has done a lot of work for this compliance.
- Now the SP expects that all works as desired with logins coming from 1 thousands of IdPs.
- But the real world makes all the effort spent by a SP to be able to work in the interfederation a vain effort, because nothing works automatically as expected.
- It's hard for the SP to get in touch with the IdP and, in any case, is too late.

ERROR AFTER SUCCESSFUL LOGIN: doesn't the IdP care?



- Seems that IdP operators don't care about this until they receive complains from the user

The desired world of interfederation



What is the desired world of interfederation

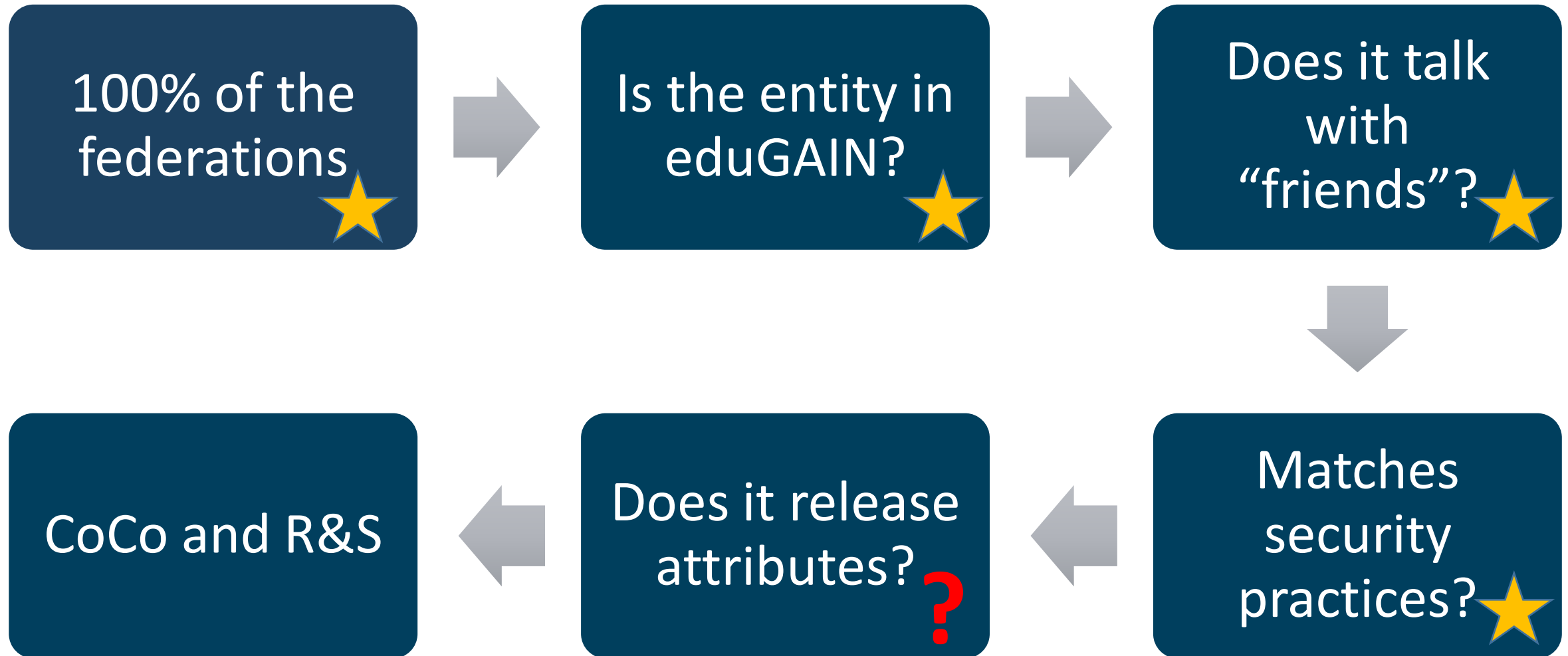


- When a new SP appears suddenly in the eduGAIN metadata aggregate
- the IdP dynamically and automatically configure the attribute-filter (ARP: attribute release policy)
 - in the way requested by the SP and
 - in compliance with the policy of the IdP home organisation.

ERROR AFTER SUCCESSFUL LOGIN: doesn't the FedOp care?

- The role of the Federator operator SHOULD BE proactive or passive? (in order to help to reach the desired world)
- Here follows our proposal, as Federation Operator, to help in solving the issue

Campaigns for “eduGAIN works”



Everytime a new SP joins a federation, the IdP manager has to

Edit and modify the attribute release policy (attribute-filter.xml or module_attributepolicy_prod.php file)

- Add the new entityID
- Add the list of the RequestedAttributes (if they are compliant with the Organization policy)
- For a Shibboleth IdP - Restart the IdP services!

... And problems

As we all know, manually editing files is a big time consuming activity...

... And stressing activity....

... And it is very easy to make mistakes

Everytime it is

- Easy to make mistakes
- Easy to forget
- Difficult to implement if there are many SPs

... And more problems....

In a inter-federated enviroment it could be even more difficult:

The IdP manager often is not aware of new SPs joining for example eduGAIN and for this reason

- He will never add the new SP to his configuration file
- He will never release the correct attributes to make them work
- The new SP will never work with his IdP until one or more users complain about a SP that is not working

IdP managers need something

- Simple to configure
- Simple to implement
- Automatic!! (or at least semi-automatic)
- Compliant with the Organization privacy policy for the users

A possible approach

There is one thing that could help the IdP managers to solve many of the problems discussed
the EntityCategory feature

The produced simplification consists in a federation service categorization of homogeneous services

The scope of EntityCategory is that the attribute release policy will not be configured for each SP but only once-for the whole category

Each category will contain a set of homogeneous entities (in our case a set of SPs) that meet the requirements of the category itself

IdPs can configure a rule for the category. The rules will remains unchanged (scalable) even if further SPs subscribe that category in the future.

How Entity Category works



A federation agrees with its members to

- Introduce one or more categories for its federated IdP and SP
- Define a set of criteria to belong to the category
- Establish procedures, both for SPs and IdPs, to be member
- Membership to a category is written in the single entity metadata

- Since the SP must satisfy a set of requirements
- Since the Federation Operator has to control that those requirements are compliant and satisfied

Once the Federation or the Registration Authority accepted the SP in a category

The IdP can trust every SP in that category, and be sure that all the requirements are satisfied and certified by the Registration Authority, or by the Federation

EntityCategory attribute

To obtain the entity category attribute a SP MUST satisfy the requirements for the category and ASK for the certification to the Registrar.

To certify that a SP is member of a category the Registrar (after any necessary control) adds this fragment to the SP entity metadata

<AttributeName>**<http://macedir.org/entity-category>**</AttributeName>

<AttributeValue><http://refeds.org/category/research-and-scholarship></AttributeValue>

<AttributeValue><http://www.geant.net/uri/dataprotection-code-of-conduct/v1></AttributeValue>

The EntityCategory support attribute

A categorised SP needs to know the supporter IdPs of the category, in order to work easier.

IdPs are asked to claim explicitly that they are supporting the category, by inserting a proper tag in the IdP metadata

<AttributeName>**<http://macedir.org/entity-category-support>**</AttributeName>

<AttributeValue><http://refeds.org/category/research-and-scholarship></AttributeValue>

<AttributeValue><http://www.geant.net/uri/dataprotection-code-of-conduct/v1></AttributeValue>

The Research & Scholarship (R&S) EntityCategory is a category that applies only to SP and IdP that are operated for the purpose of supporting research and scholarship interaction, collaboration or management

Examples:

- Wiki
- Blog
- Collaborative tools
- Learning management system
- Research collaborations (LIGO, ELIXIR, CLARIN, etc)

Not any licensed content like e-journals

An SP part of R&S category has to

- Claim that it will not use attributes for purpose that fall outside of the service definition
- Request a minimal subset of R&S attributes that represent only those attributes that the SP requires to operate its service

R&S relies on the legitimate interest approach

Metadata example for an R&S SP

```
<EntityAttributes>
```

```
<Attribute Name="http://macedir.org/entity-category" >
```

```
<AttributeValue>http://refeds.org/category/research-and-scholarship</:AttributeValue>
```

```
</Attribute>
```

```
</EntityAttributes>
```


Research & Scholarship IdP support attribute



An IdP that support R&S entity category MUST release the following attributes to the SPs in this category

- eduPersonPrincipalName
 - eduPersonTargetedID
 - displayName
 - givenName
 - sn
 - mail
-
- Populate the user directory with the attributes to release
 - An IdP that support R&S entity category is **STRONGLY ENCOURAGED** to release eduPersonScopedAffiliation

After the IdP configured its attribute-filter file for R&S it has to explicitly claim its support to the category, by inserting this fragment in its metadata:

```
<EntityAttributes>
```

```
<Attribute Name="http://macedir.org/entity-category-support"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
```

```
<AttributeValue>http://refeds.org/category/research-and-scholarship</:AttributeValue>
```

```
</Attribute>
```

```
</EntityAttributes>
```


Research & Scholarship IdP filter

Example of attribute-filter.xml file for a IdP supporting R&S

```
<AttributeFilterPolicy id="releaseDynamicSubsetRandSAttributeBundle">  <PolicyRequirementRule
xsi:type="EntityAttributeExactMatch"      attributeName="http://macedir.org/entity-category"
attributeValue="http://refeds.org/category/research-and-scholarship"/>
<AttributeRule attributeID="eduPersonPrincipalName">
<PermitValueRule xsi:type="AttributeInMetadata"onlyIfRequired="false"/>  </AttributeRule>
<AttributeRule attributeID="email">
<PermitValueRule xsi:type="AttributeInMetadata"onlyIfRequired="false"/>  </AttributeRule>
</AttributeRule>
[... prosegue con tutti gli attributi: eduPersonTargetetID, displayName, sn, givenName]
</AttributeFilterPolicy>
```


GÉANT Data Protection Code of Conduct (DP_CoCo)

- Created to meet the requirements of the EU Data Protection Directive in federated identity management
- It's a formal agreement about how user data will be treated in order to respect user privacy
- It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct.

To be member of DP_CoCo entity category a SP has to

- Be located in EU/EEA and obey to EU laws
 - It is not allowed to send the user data to third parties
 - It must ask only for the minimal set of required attributes
- Ask its necessary attributes in its RequestedAttribute statement as «isRequired="true"»
- Inform the user about the processing his personal data in a PrivacyPolicy page linked to its primary service page

The SP is member of DP_CoCo category if the Registrar certifies it (after any necessary control) by adding this fragment to the SP entity metadata

<EntityAttributes>

<Attribute Name="http://macedir.org/entity-category"

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

<AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</:AttributeValue>

</Attribute>

</EntityAttributes>

DP_CoCo IdP support attribute

To support DP_CoCo entity category an IdP has to

- Release only the requested attributes with the «isRequired="true"» value
- If the SP requires a particular value for a multivalue attribute the IdP has to release only that value
- Inform the user about the treatment for every single attribute in its PrivacyStatementURL
- To support DP_CoCo EntityCategory the IdP has to explicitly claim it in its metadata by adding:

```
<EntityAttributes>
```

```
<Attribute Name="http://macedir.org/entity-category-support"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
```

```
<AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</AttributeValue>
```

```
</Attribute>
```

```
</EntityAttributes>
```

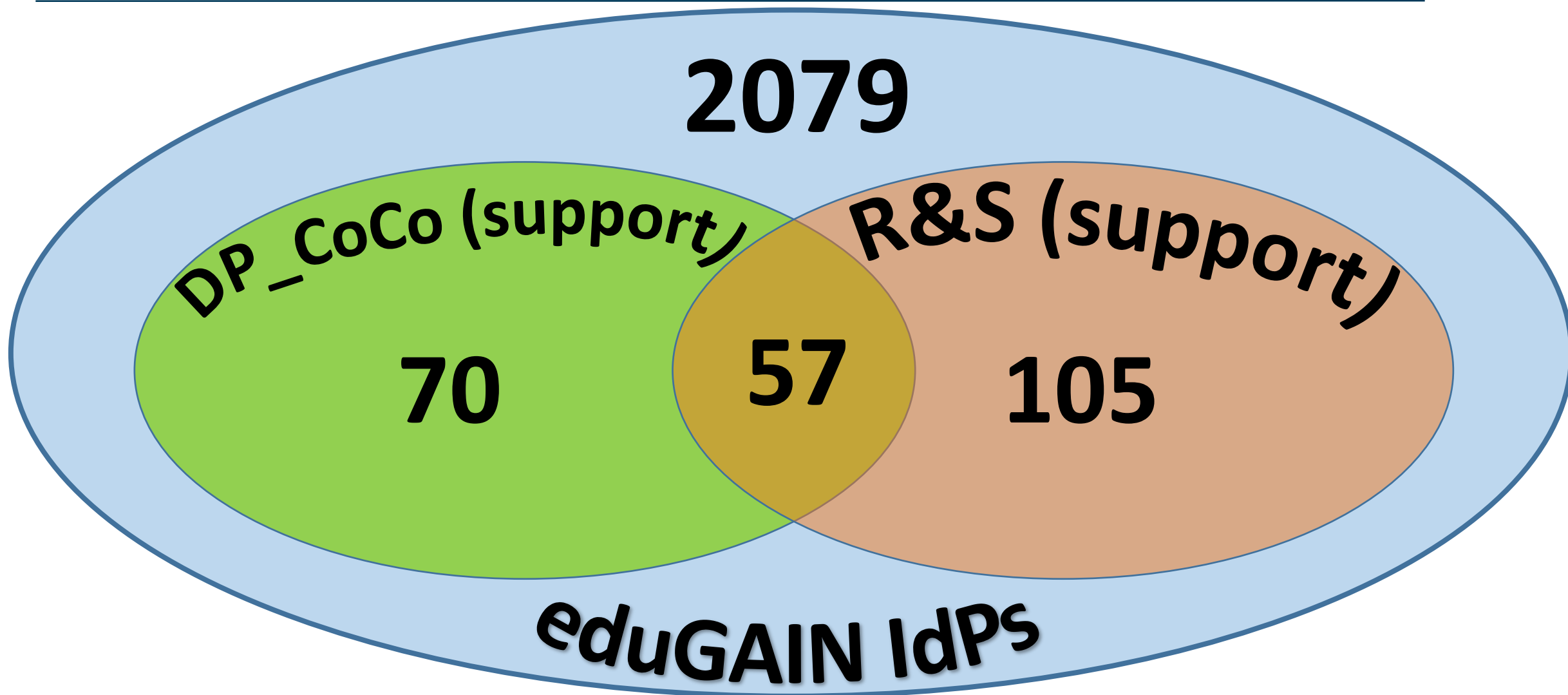


```
<AttributeFilterPolicy id="releaseToCoCo">  
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"  
    attributeName="http://macedir.org/entity-category"  
    attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1" />  
  <AttributeRule attributeID="sn">  
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />  
  </AttributeRule>  
  <AttributeRule attributeID="givenName">  
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true" />  
  </AttributeRule>  
  [... Per tutti gli attributi]  
</AttributeFilterPolicy>
```


- Release only Attributes that are **adequate, relevant and not excessive** for the Service Provider flagged as requested in SAML metadata (see SAML 2 Profile for the Code of Conduct for details on how this is done)
- If the Service Provider requests only a **particular Attribute value**, release only that value and no other values for instance, if the Service Provider requests only eduPersonAffiliation="member", do not release eduPersonAffiliation="faculty"
- **Inform the end user** on the Attribute
 - for each Attribute, the Attribute name, description and value an easily understood label can be displayed instead of displaying several closely related Attributes (eg the various name Attributes)
- If use the **data controller's legitimate interests** as the legal grounds for attribute release, release only attributes that are flagged as NECESSARY

BREAK



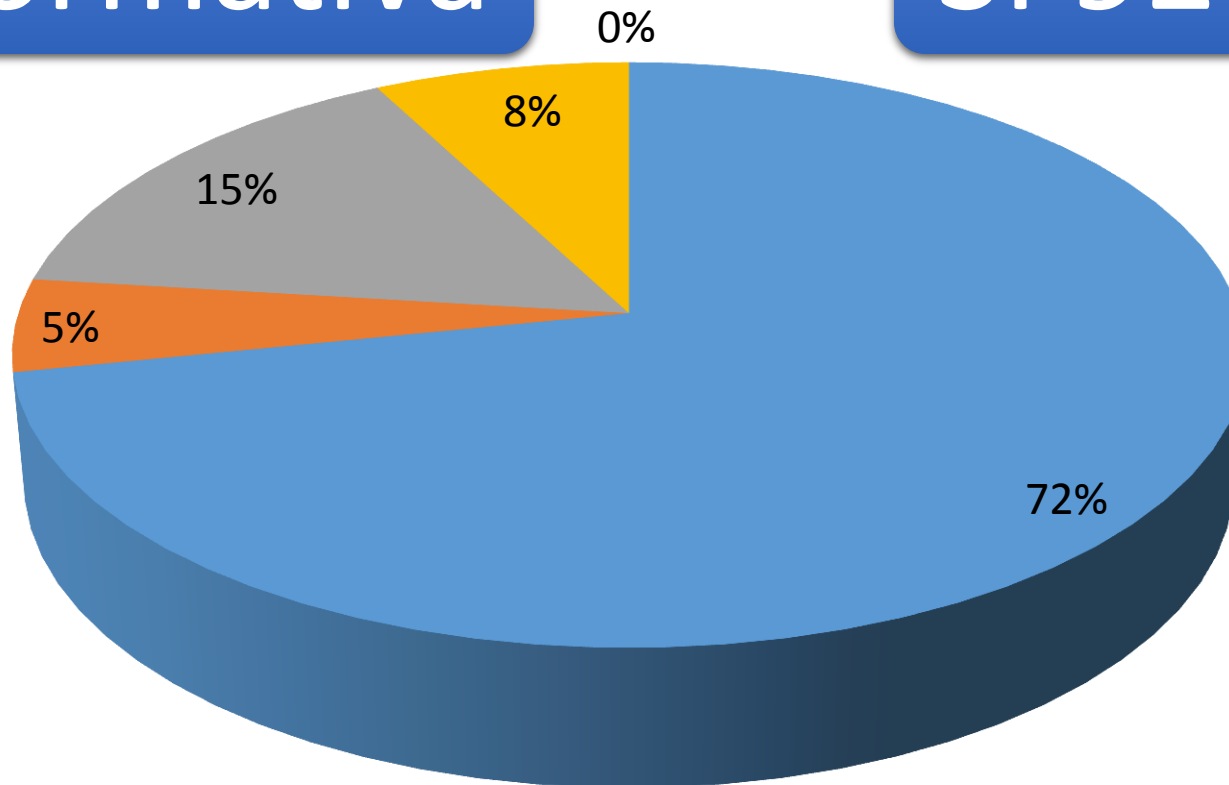


DOPAU and LEGAL GROUND

2.1.3 L'OdA informa gli utenti, anche in maniera semplificata, dei meccanismi di funzionamento dei sistemi federati (ad es. rilascio degli attributi da IdP a SP, eventuali rischi connessi, ecc.)? (più risposte possibili)

informativa

SÌ 92%

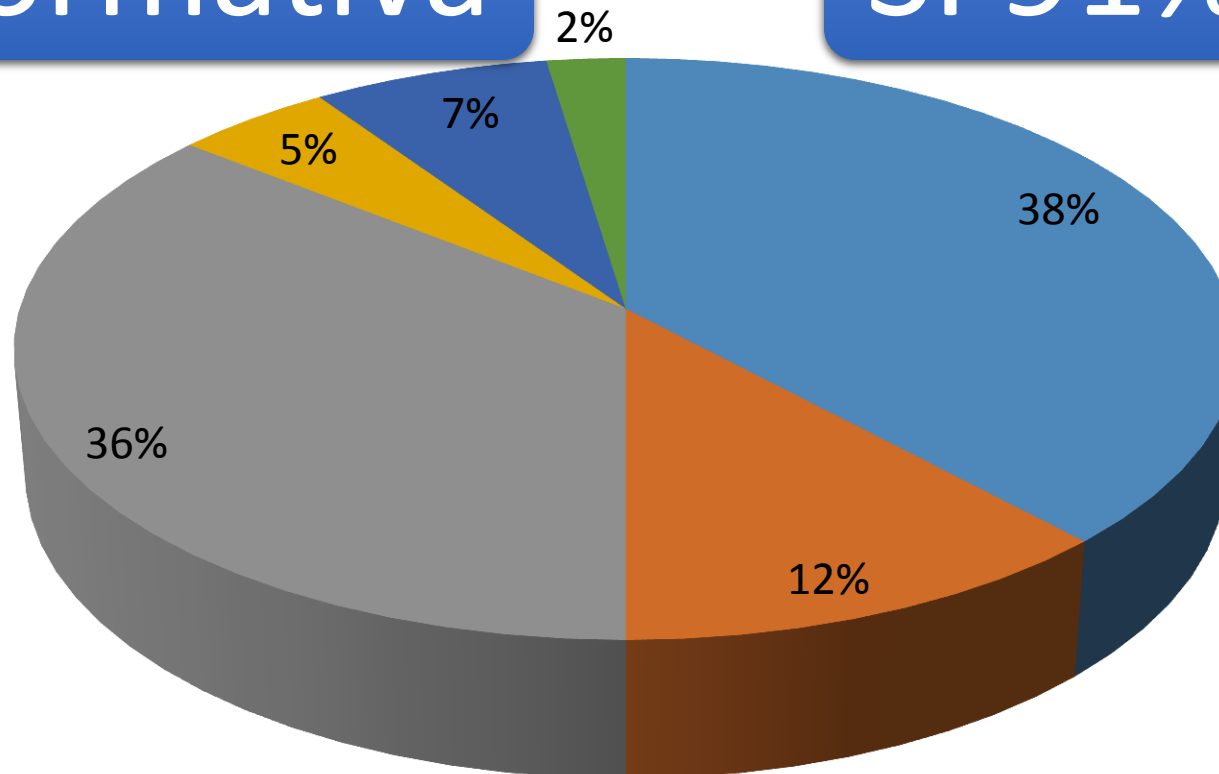


- a. Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- b. Si, mediante la distribuzione di materiale cartaceo informativo/divulgativo
- c. Si, mediante eventi informativi/divulgativi
- d. No
- e. Altro

2.1.4. L'OdA informa l'utente sui dati personali che l'Identity Provider trasferirà ad uno specifico Service Provider di interesse per l'utente stesso? (più risposte possibili)

informativa

Sì 91%

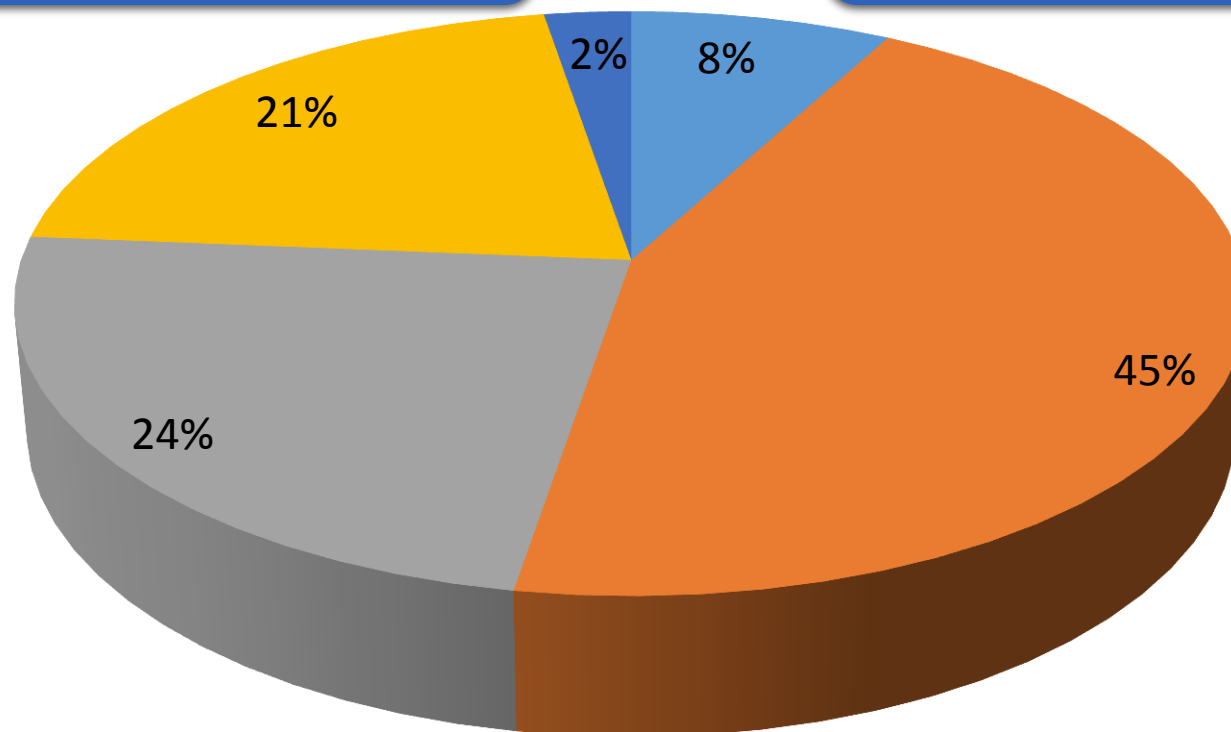


- a. Si, mediante un' informativa disponibile su di una pagina web dedicata ai servizi di autenticazione federata
- b. Si, mediante un' informativa su di una pagina web dedicata raggiungibile dalla pagina di login dell'Identity Provider o direttamente disponibile su quest'ultima
- c. Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- d. Si, distribuendo agli utenti un'informativa cartacea
- e. No
- f. Altro

2.1.5. L'OdA, ove questo sia previsto dal D.Lgs. 196/2003, chiede all'utente il consenso al trasferimento dei suoi dati personali dall'Identity Provider ai Service Provider federati di interesse per l'utente stesso? (più risposte possibili)

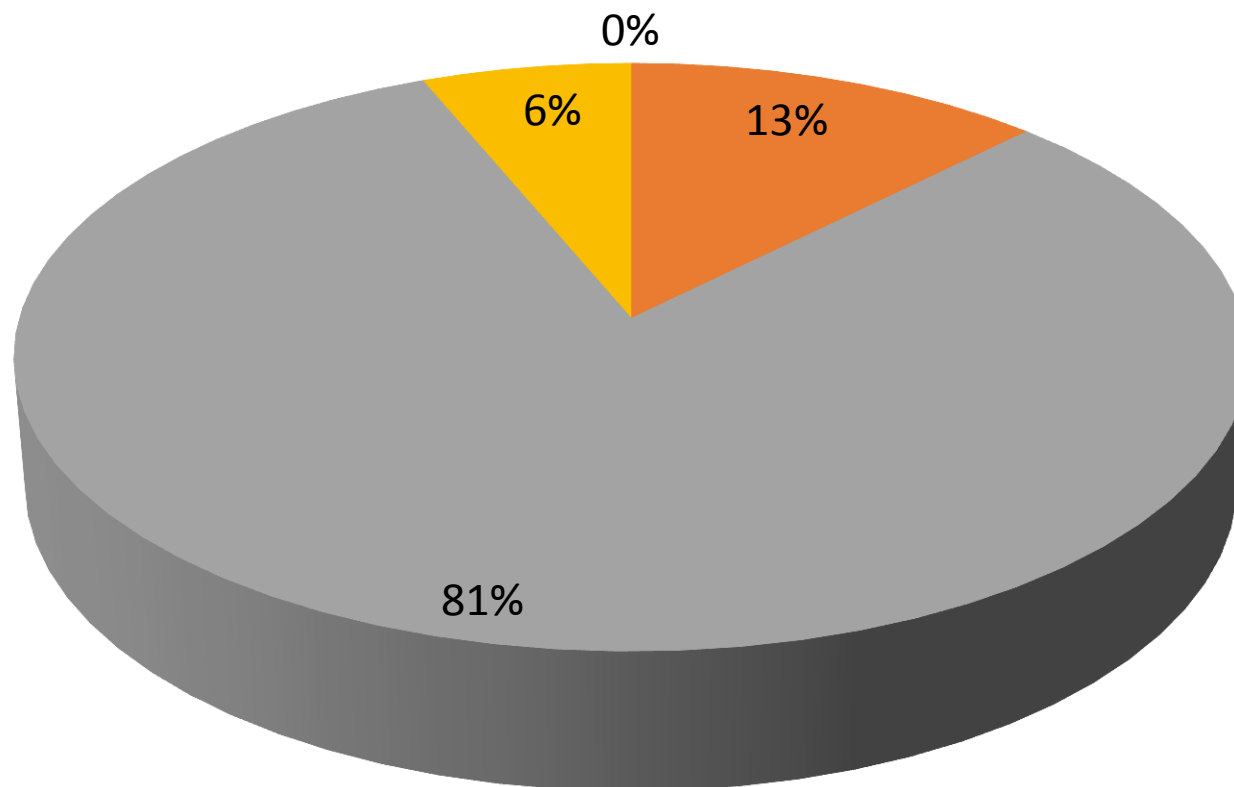
consenso

Sì 77%



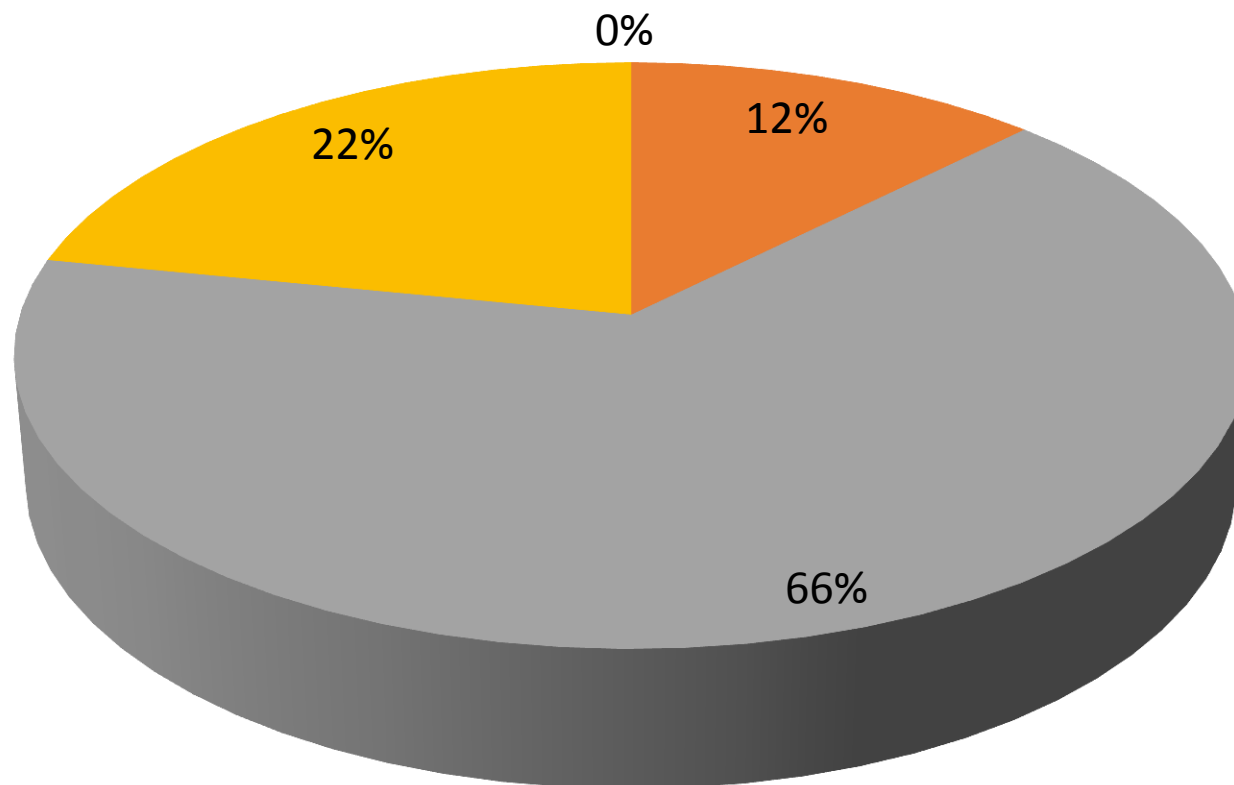
- a. Si, mediante un'accettazione esplicita rilasciata on line tramite applicazione web con accesso autenticato
- b. Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- c. Si, facendo firmare agli utenti un modulo di consenso cartaceo
- d. No
- e. Altro

2.2.1 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano necessari al funzionamento del servizio?



- a. si, se il servizio viene erogato dall'Italia
- b. si, se il servizio viene erogato dall'Europa
- c. si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
- d. no

2.2.2 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano non necessari (opzionali) al funzionamento del servizio?



- a. si, se il servizio viene erogato dall'Italia
- b. si, se il servizio viene erogato dall'Europa
- c. si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
- d. no

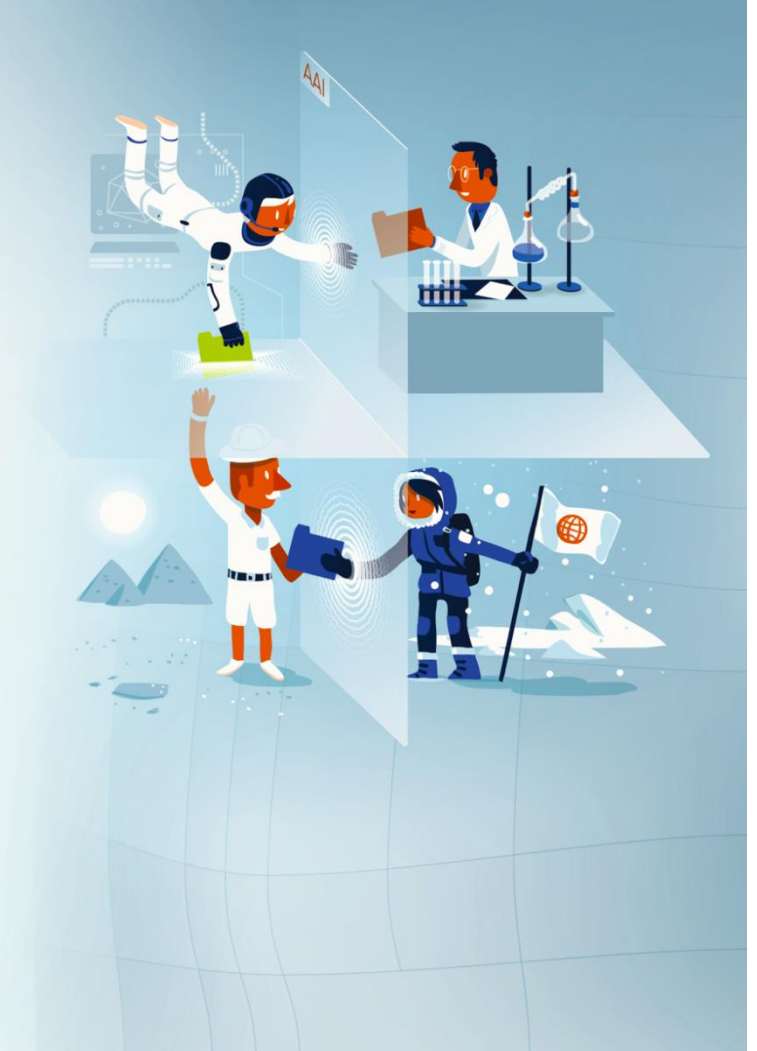
Unlocking Attributes

I am not a lawyer...

Most of eduGAIN is under EU
Data protection directive or
equivalent

The objective of the directive is to
protect a person's fundamental
rights while guaranteeing the free
flow of personal data between
member states

Member States shall provide that the controller must implement **appropriate** technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.



Balancing Risk



In Focus - Attribute Release

Tools to automate risk-analysis-based support of e-Research



Entity Categories group federation entities that share common criteria.

Facilitate IdP decisions to release a defined set of attributes to SPs without the need for detailed local review for each SP

Check with your Federation Operator for advice on which best suits your needs

Research and Scholarship Entity Category relies on the legitimate interest approach

- Safeguards of data minimisation, privacy enhancing tech
- Limits the types of services that are allowed to claim this category and focusing on low-risk, high benefit services that have a clearly identifiable need for personal information
- Each SP is considered on a case-by-case basis by the federation in question and reviewed annually.

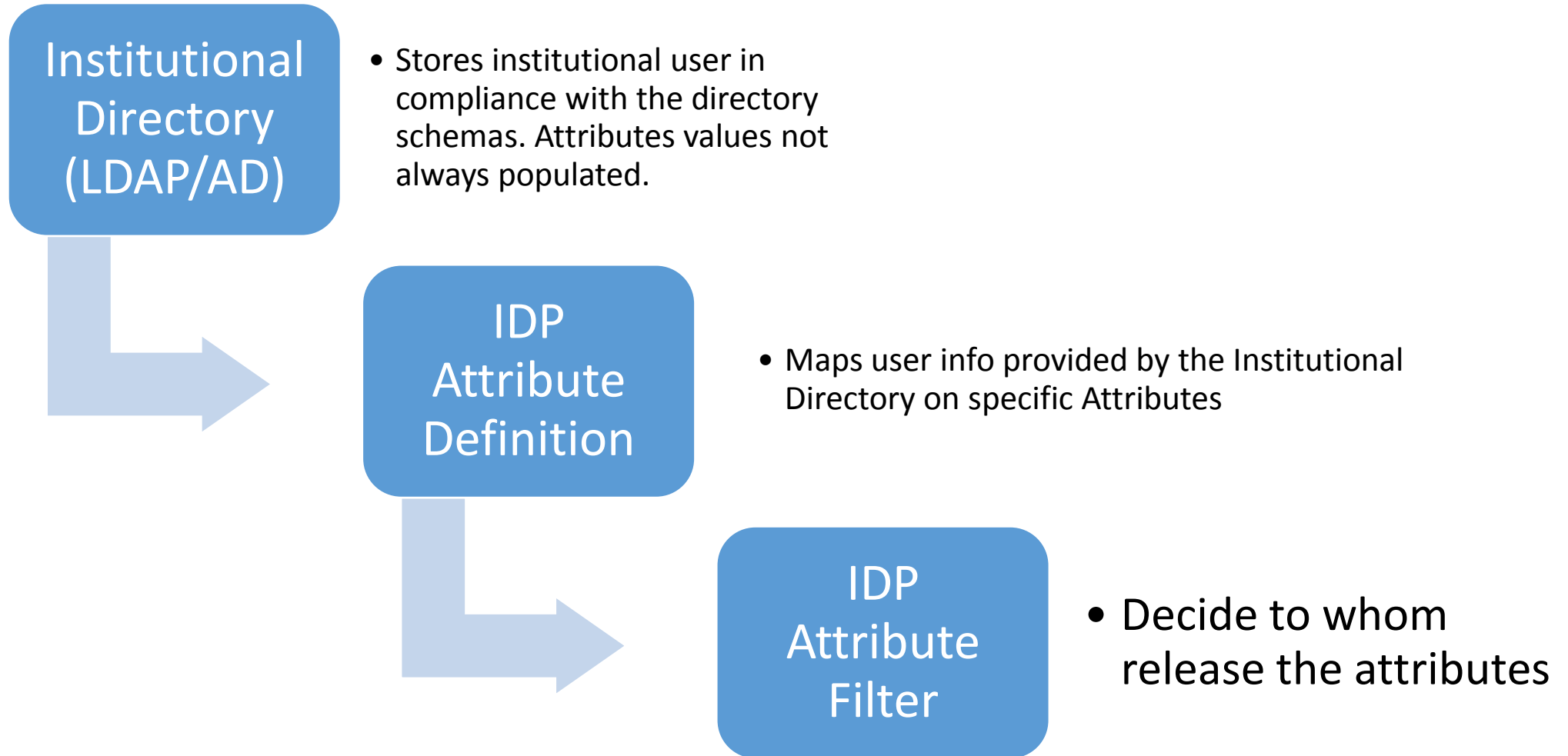
GÉANT Code of Conduct approach aims to minimise the risk that arises from depending on each other.

- Legitimate interest is also fundamental
- Signals that the Home Organisation and Service Provider are aware of the legal requirements
- Based on Directive 95/46/EC 1995

PROBLEM

**Federated Users can't access to the
Federated Resources because their
federated IdP doesn't release all the
needed attributes**

Attribute Release Process



- Importance of using international defined schemas
 - We need to share international schemas in order to be able to exchange attributes in an international context (eduGAIN)
- Private/national schemas are irrelevant in the international context (SP should be aware they cannot pretend to obtain private/national defined attributes).
 - Could be taken in consideration at national level.

Does your IdP manage these attributes?



<https://goo.gl/rOMQiP>

attribute management

FriendlyName	OID	Count
email, mail, rfc822Mailbox	urn:oid:0.9.2342.19200300.100.1.3	282
eduPersonPrincipalName, eppn	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	277
displayName	urn:oid:2.16.840.1.113730.3.1.241	148
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	144
givenName, gn, FirstName	urn:oid:2.5.4.42	144
sn, surname, LastName	urn:oid:2.5.4.4	141
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	126
cn, commonName	urn:oid:2.5.4.3	85
eduPersonScopedAffiliation, eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	62
schacHomeOrganization, shacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	35
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	33
o, organizationName	urn:oid:2.5.4.10	32
schacHomeOrganizationType	urn:oid:1.3.6.1.4.1.25178.1.2.10	22
preferredLanguage	urn:oid:2.16.840.1.113730.3.1.39	17
uid	urn:oid:0.9.2342.19200300.100.1.1	15
eduPersonPrimaryAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.5	13
eduPersonOrgDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.3	10
ou	urn:oid:2.5.4.11	8
title	urn:oid:2.5.4.12	7
telephoneNumber	urn:oid:2.5.4.20	7
mobile	urn:oid:0.9.2342.19200300.100.1.41	6
eduPersonNickname, Nickname	urn:oid:1.3.6.1.4.1.5923.1.1.1.2	6
eduPersonOrgUnitDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.4	6
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11	5
eduPersonPrimaryOrgUnitDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.8	5
postalAddress	urn:oid:2.5.4.16	5
l, localityName	urn:oid:2.5.4.7	5

- Which are the attributes that my IdP is able to manage?
 - Complete your list
- Which are the attributes that SPs require?
- ← Most requested attributes from SPs in eduGAIN
- Are the two lists compatible? Overlapping?
- Is my IdP able to release the attributes that could be requested?
- At the end:
 - If I want/need, I'm in the position to be able to release attributes

Attributes are missing in the Directory (openLDAP/AD)

SOLUTION: Define dynamically the missing attributes on the IdP side

- Fast solution
- Simply like a JavaScript script
- Directory Manager independent
- Used only if the attribute is not already present on the directory

What the IdP Operator needs to do

Fill values missing in the directory

Dynamic Attributes Definitions Examples

Attribute Name	IDEM Attribute Value composed by	IDEM Implementation for IdP with Java 7 (Rhino)	IDEM Implementation for IdP with Java 8 (Nashorn)
schacHomeOrganization	domain.org	<u>schacHomeOrganization</u>	<u>schacHomeOrganization</u>
organizationName	schacHomeOrganization	<u>organizationName</u>	<u>organizationName</u>
organizationalUnit	organizationName	<u>organizationalUnit</u>	<u>organizationalUnit</u>
eduPersonOrgDN	organizationName + schacHomeOrganization	<u>eduPersonOrgDN</u>	<u>eduPersonOrgDN</u>
eduPersonOrgUnitDN	eduPersonOrgDN	<u>eduPersonOrgUnitDN</u>	<u>eduPersonOrgUnitDN</u>
displayName	commonName OR givenName + surname OR givenName OR surname	<u>displayName</u>	<u>displayName</u>

Attributes Filters are misconfigured

WHY:

- IdP Manager is not always focused on the IdP problems.
- IdP Manager doesn't have enough technical knowledge.
- IdP Manager doesn't want to change those things that seems working.
- The person who installed the IdP software has left the institution without passing all the needed knowledge.

Attributes Filters are misconfigured

SOLUTION:

Federation Operator supports IdP Manager on the definition of the needed attribute release policy.

What your institutional policy allows to do?



1. Provides a set of attributes to all federated resources without doing differences?
2. Provides the support to the R&S Entity Category?
3. Provides the support to the Data Protection CoCo Entity Category?
4. Allows an user to access to any kind of free federated resource available?

Attribute Release Policy (ARP)

How to address the attribute release to the federated resources



1. ARP Entity Category(EC) based:

attribute release policy based on static rules that don't require changes once created to satisfy the attribute requests coming from old and new federated resources.

2. ARP Registry based:

attribute release policy based on rules built dynamically through easy-to-use tools (like a registry) that allow to an IDP Manager to change them easily and satisfy the attribute requests coming from the federated resources.

ARP EC based VS ARP Registry based

PRO & CONS

<u>EC ARP</u>		<u>REGISTRY ARP</u>	
PRO	CONS	PRO	CONS
Scalable (it needs less or no changes in the long time period)	Low number of IdP compliant with the existing Entity Categories	It can satisfy all federated resources without limit. The IdP Manager can change the rules as he want.	Not Scalable (but it is easy to add new resources with the GUI)
Simple and fast to apply on IdP (download and use it)	The current Entity Categories are not sufficient	Simple and fast to apply on IdP (download and use it)	
		A simple GUI replaces heavy manual operations (metadata management, ARP, know all resources available, ...)	

IDEM Federation choice: EC ARP + Registry ARP



IDEM GARR AAI has chosen to use both, plus its Default ARP:

1. Default ARP:

- **Default Federation ARP:** attribute filter that releases a very small set of attributes to all resources and allows to use only few essential federation resources.

2. EC ARP:

- **R&S EC ARP:** attribute filter that implement the rules established for all resources compliant with Research and Scholarship entity category.
- **CoCo EC ARP:** attribute filter that implement the rules established for all resources compliant with Code Of Conduct entity category.

3. Registry ARP:

- **Custom IdP ARP:** An IdP Manager maintains the decisional power to release or not the attributes to the SPs by building his attribute filter with the help of IDEM Entity Registry.

General Steps to apply a new Attribute Filter on a Shibboleth IdP



- Create or Retrieve the attribute filter
- Add it to «services.xml»
- Reload the attribute filter service (or entire Tomcat if it fails)

IDEM Default ARP + R&S + CoCo

HOW TO Retrieve and Use IDEM Default and EC ARPs

1. Download the IDEM ARPs:

- `cd /opt/shibboleth-idp/conf`
- `wget http://www.garr.it/idem-conf/attribute-filter-v3-idem.xml`
- `wget http://www.garr.it/idem-conf/attribute-filter-v3-rs.xml`
- `wget http://www.garr.it/idem-conf/attribute-filter-v3-coco.xml`

2. Modify the «services.xml» file:

- `vim /opt/shibboleth-idp/conf/services.xml`

```
<util:list id="shibboleth.AttributeFilterResources">
    <value>{%idp.home}/conf/attribute-filter-v3-idem.xml</value>
    <value>{%idp.home}/conf/attribute-filter-v3-rs.xml</value>
    <value>{%idp.home}/conf/attribute-filter-v3-coco.xml</value>
</util:list>
```

3. Restart the Attribute Filter Service of the Shibboleth IdP:

- `cd /opt/shibboleth-idp/bin`
- `./reload-service.sh -id shibboleth.AttributeFilterService`


IDEM Registry ARP

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 1 - Log in via federated identity to the IDEM Entity Registry:

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






EN

Log in

Log In to the Registry

IDEM Entity Registry

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



HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 1 - Log in via federated identity to the IDEM Entity Registry



ENLog in

Log in with local account

Username

Password

Sign in

Login via IDEM

Log In via Federated Identity

L'IDEM Entity Registry è un sistema di raccolta, della...

Attraverso di esso è possibile gestire le informazioni dell'interfaccia grafica...

Per ricevere su...

Questo servizio...

Fai LOG-IN per modificare le entità che hai già registrato.

Per registrare una nuova entità utilizza i link sottostanti

Inserisci un Nuovo Identity Provider nella Federazione IDEM Test

Inserisci un Nuovo Service Provider nella Federazione IDEM Test

collects,

rganisations are practical

To modify the metadata of your entities, please LOG-IN.

To register new entities, use the links below.

Insert a New Identity Provider into the IDEM Test Federation

Insert a New Service Provider into the IDEM Test Federation

idem garr aai

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 1 - Log in via federated identity to the IDEM Entity Registry



The screenshot shows the IDEM Entity Registry dashboard. At the top, there is a navigation bar with the following items: Federations, Identity Providers, Service Providers, Register, and Administration. A red arrow points to the 'Identity Providers' menu item. Below the navigation bar is a 'Quick access' section. On the left, there is a 'DASHBOARD' label. In the center, there are four large buttons: 'Identity Providers', 'Service Providers', 'Federations', and 'Queue'. The 'Queue' button is highlighted with a blue border. Below the 'Queue' button, there is a table with the following columns: Date, Requester, and Request type.

Date	Requester	Request type
------	-----------	--------------

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 2 – Declare which attributes are supported by the IdP



FederationsIdentity ProvidersService ProvidersRegisterAdministration

0EN

List Of Identity Providers

DASHBOARD / IDENTITY PROVIDERS

Display 10 records per page

external/importedlocally managedColumn visibility

Showing 1 to 1 of 1 entries (filtered from 156 total records)

Search: idp.dir.garr.it

OPEN IDP MAIN PAGE BY CLICKING HERE

Name of organization	URL to information about organization	Registration Date	status
GARR IdP https://idp.dir.garr.it/idp/shibboleth	http://www.garr.it/b/eng	2010-09-30	

Showing 1 to 1 of 1 entries (filtered from 156 total records)

Previous1Next

WRITE IDP FQDN HERE

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 2 – Declare which Entity Category will be supported by the IdP



CLICK ON THIS GEAR WHEEL TO OPEN IDP SETTINGS →

Identity Provider: GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP

General Membership Metadata Management Logs/Stats

Status	Enabled Managed locally
Last modification	2016-02-29 17:27:36
EntityID	https://idp.dir.garr.it/idp/shibboleth
Name of organization	it: GARR en: GARR
Displayname of organization	it: GARR en: GARR
URL to information about organization	it: http://www.garr.it en: http://www.garr.it/b/eng
Registration Authority	http://www.idem.garr.it/
Registration Date	2010-09-30 15:00:00
Registration Policy	en: https://www.idem.garr.it/idem-metadata-registration-practice-statement
Entity Categories	
Valid From/Until	unlimited -- unlimited

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 2 – Declare which Entity Category will be supported by the IdP

Federations Identity Providers Service Providers Register Administration

Identity Provider: GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP

EDIT IDP METADATA INFO BY CLICKING HERE →

ACTIONS

- Edit provider
- Manage membership (joining)
- Manage membership (leaving)

ATTRIBUTES

- SPs excluded from ARP
- Attribute Policy
- Clear cache

General Membership Metadata Management Logs/Stats

Status **Enabled** Managed locally

Last modification 2016-06-03 21:50:25

EntityID https://idp.dir.garr.it/idp/shibboleth

Name of organization
it: GARR
en: GARR

Displayname of organization
it: GARR
en: GARR

URL to information about organization
it: http://www.garr.it
en: http://www.garr.it/b/eng

Registration Authority http://www.idem.garr.it/

Registration Date 2010-09-30 15:00:00

Registration Policy
en: https://www.idem.garr.it/idem-metadata-registration-practice-statement

Entity Categories

Valid From/Until unlimited -- unlimited

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 2 – Declare which Entity Category will be supported by the IdP



GARR IdP EDIT YOUR METADATA INFO ABOUT EC BY CLICKING HERE

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / EDIT

Organization | Contacts | UI Information | UI Hints | SAML | Certificates | Entity Categories | Static Metadata

Name of organization

Italian (it)	<input type="text" value="GARR"/>	<button>Remove</button>
English (en)	<input type="text" value="GARR"/>	<button>Remove</button>
<div>English (en) ▾</div>	<button>Add in new language</button>	

Displayname of organization

Italian (it)	<input type="text" value="GARR"/>	<button>Remove</button>
--------------	-----------------------------------	-------------------------

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 2 – Declare which Entity Category will be supported by the IdP



GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / EDIT

Organization Contacts UI Information UI Hints SAML Certificates **Entity Categories** Static Metadata

CHOOSE WHICH AVAILABLE EC SUPPORT

- ☒ Research and Scholarship Entity Category for IdPs
- ☒ Code of Conduct v1 for IdPs

UPDATE IDP METADATA

Cancel Save draft **Update**

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 2 – Declare which Entity Category will be supported by the IdP



CLICK ON THIS GEAR WHEEL TO OPEN IDP SETTINGS

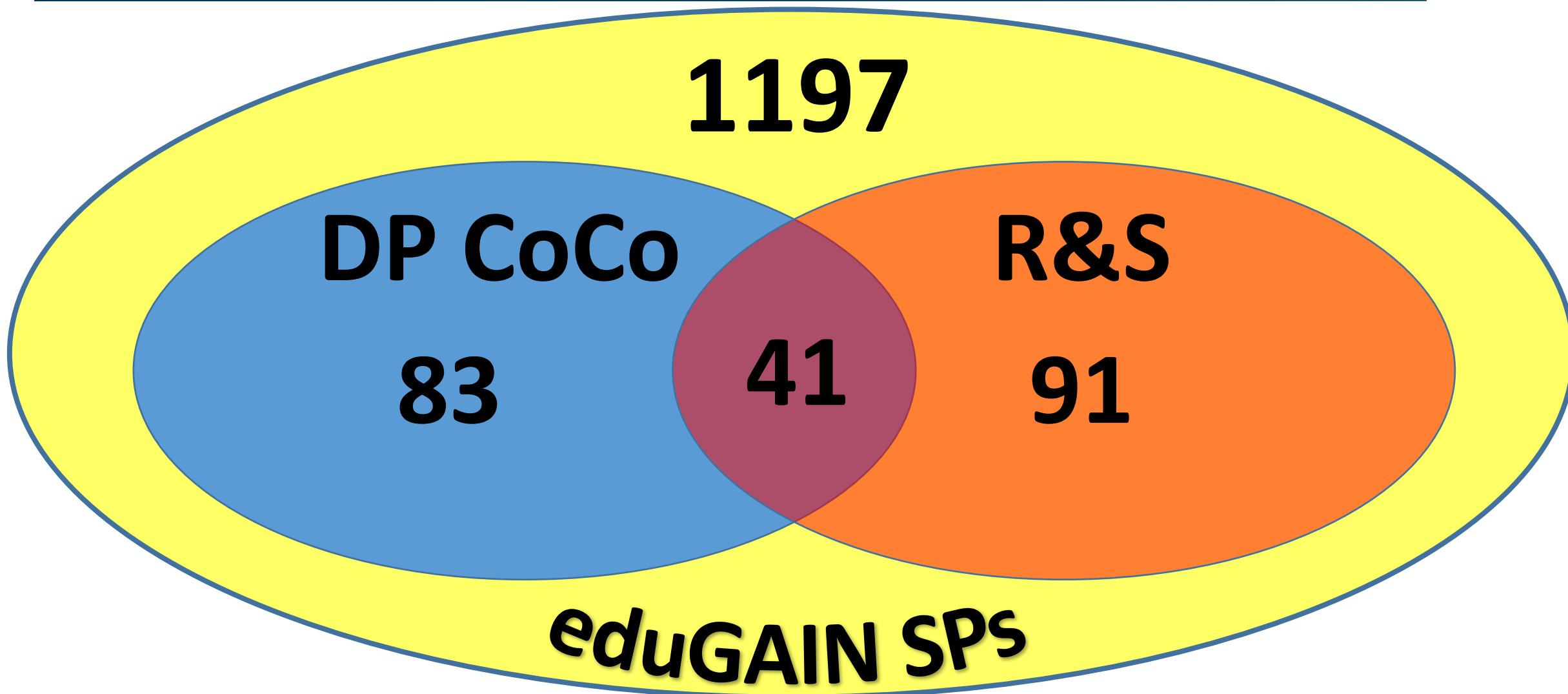
Identity Provider: GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP

General Membership Metadata Management Logs/Stats

Status	Enabled Managed locally
Last modification	2016-06-03 22:26:17
EntityID	https://idp.dir.garr.it/idp/shibboleth
Name of organization	it: GARR en: GARR
Displayname of organization	it: GARR en: GARR
URL to information about organization	it: http://www.garr.it en: http://www.garr.it/b/eng
Registration Authority	http://www.idem.garr.it/
Registration Date	2010-09-30 15:00:00
Registration Policy	en: https://www.idem.garr.it/idem-metadata-registration-practice-statement
Entity Categories	Research and Scholarship Entity Category for IdPs Code of Conduct v1 for IdPs
Valid From/Until	unlimited -- unlimited

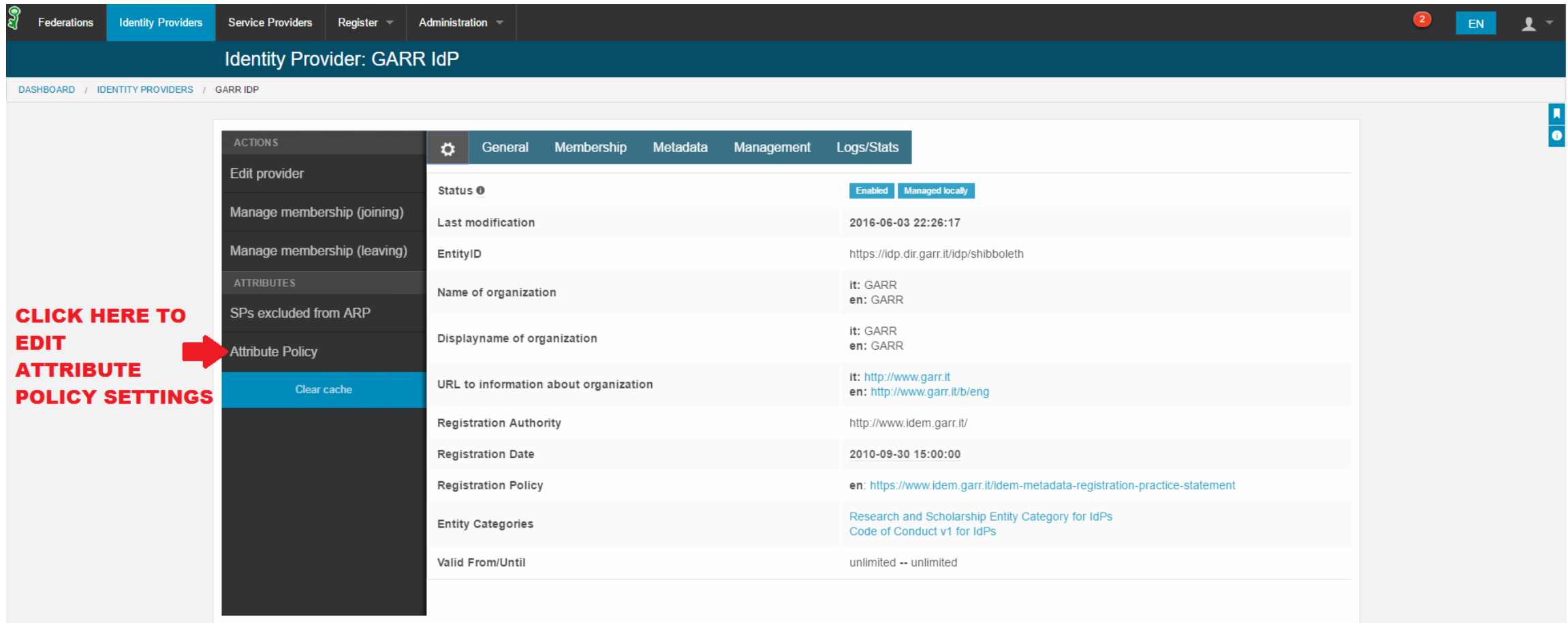
VERIFY THE APPLICATION OF THE EC SUPPORT



HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 3 – Declare which attributes are supported by the IdP

CLICK HERE TO EDIT ATTRIBUTE POLICY SETTINGS →



Identity Provider: GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP

ACTIONS

- Edit provider
- Manage membership (joining)
- Manage membership (leaving)

ATTRIBUTES

- SPs excluded from ARP
- Attribute Policy**
- Clear cache

General | Membership | Metadata | Management | Logs/Stats

Status ⓘ	Enabled Managed locally
Last modification	2016-06-03 22:26:17
EntityID	https://idp.dir.garr.it/idp/shibboleth
Name of organization	it: GARR en: GARR
Displayname of organization	it: GARR en: GARR
URL to information about organization	it: http://www.garr.it en: http://www.garr.it/b/eng
Registration Authority	http://www.idem.garr.it/
Registration Date	2010-09-30 15:00:00
Registration Policy	en: https://www.idem.garr.it/idem-metadata-registration-practice-statement
Entity Categories	Research and Scholarship Entity Category for IdPs Code of Conduct v1 for IdPs
Valid From/Until	unlimited -- unlimited

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 3 – Declare which attributes are supported by the IdP



Navigation bar: Federations, Identity Providers, Service Providers, Register, Administration

Breadcrumbs: DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY

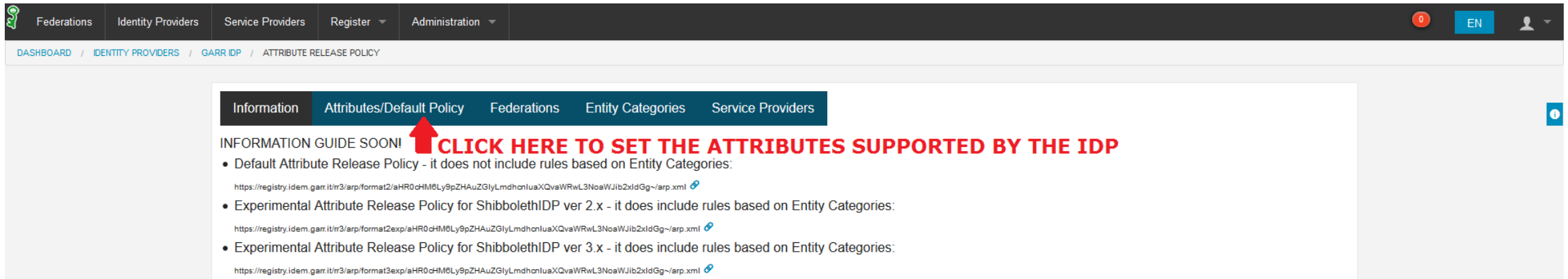
Sub-navigation: Information, Attributes/Default Policy, Federations, Entity Categories, Service Providers

INFORMATION GUIDE SOON!

- Default Attribute Release Policy - it does not include rules based on Entity Categories:
<https://registry.idem.garr.it/ir3/arp/format2/aHR0dHM6Ly9pZHAuZGlyLmdhbnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 2.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/ir3/arp/format2exp/aHR0dHM6Ly9pZHAuZGlyLmdhbnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 3.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/ir3/arp/format3exp/aHR0dHM6Ly9pZHAuZGlyLmdhbnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 3 – Declare which attributes are supported by the IdP



Federations Identity Providers Service Providers Register Administration

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY

Information Attributes/Default Policy Federations Entity Categories Service Providers

INFORMATION GUIDE SOON! **CLICK HERE TO SET THE ATTRIBUTES SUPPORTED BY THE IDP**

- Default Attribute Release Policy - it does not include rules based on Entity Categories:
<https://registry.idem.garr.it/ir3/arp/format2/aHR0dHM6Ly9pZHAuZGlyLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 2.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/ir3/arp/format2exp/aHR0dHM6Ly9pZHAuZGlyLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 3.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/ir3/arp/format3exp/aHR0dHM6Ly9pZHAuZGlyLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 3 – Declare which attributes are supported by the IdP



FederationsIdentity ProvidersService ProvidersRegisterAdministration

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY

InformationAttributes/Default PolicyFederationsEntity CategoriesService Providers

CLICK HERE TO ADD A NEW SUPPORTED ATTRIBUTE

Add attribute

Attribute name	Attribute support/default policy	Action
----------------	----------------------------------	--------

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 3 – Declare which attributes are supported by the IdP

Federations Identity Providers Service Providers Register Administration

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY

Information

Attribute name

CHOOSE THE SUPPORTED ATTRIBUTE

Attribute: email

Policy: deny

LEAVE "deny" AS VALUE OF "policy"

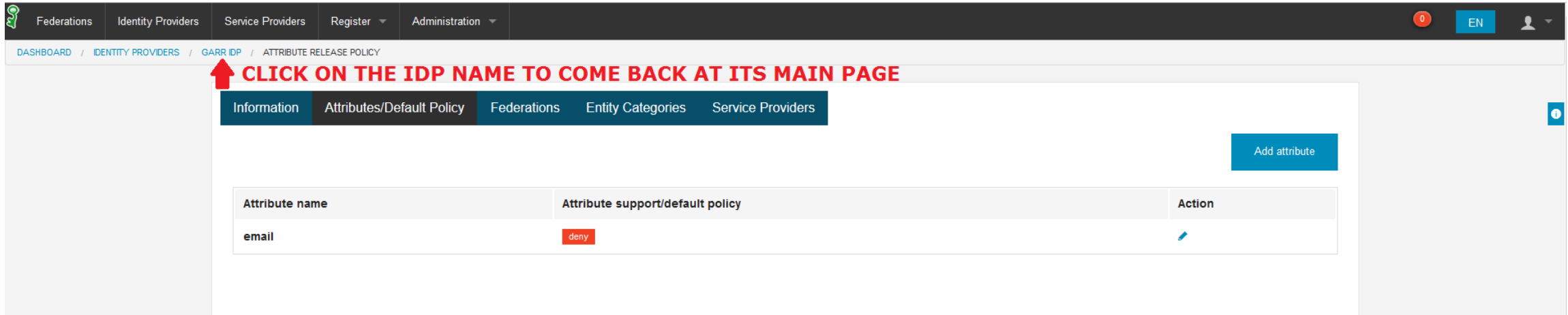
Cancel Add

APPLY THE CHOICE


Add attribute

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 4 – Set the Attribute Release Policy for SPs

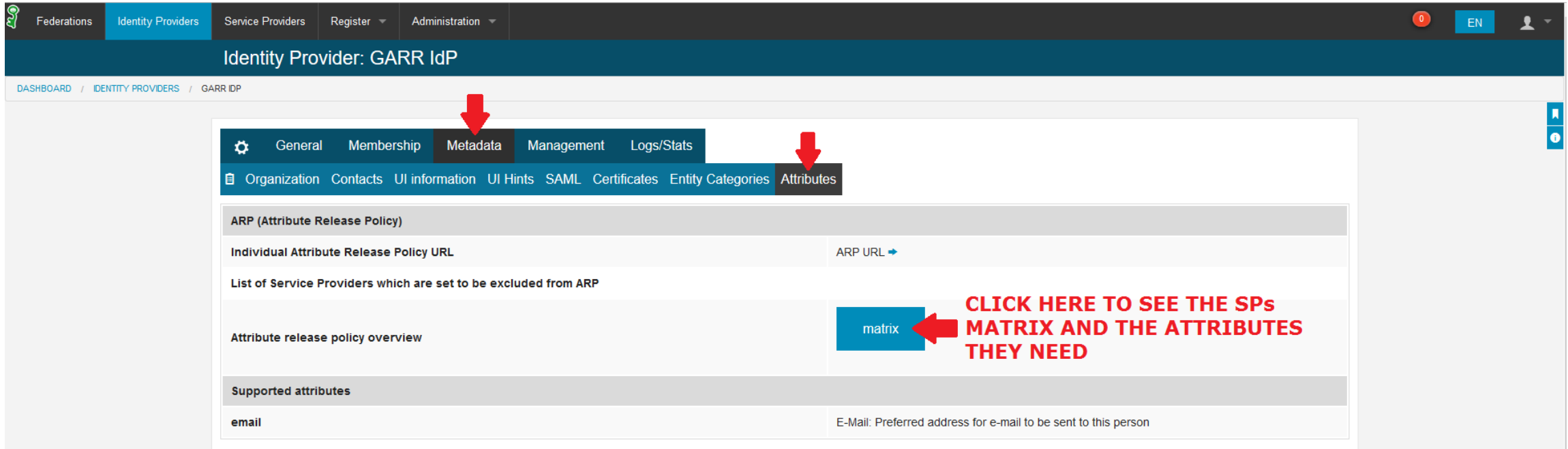


The screenshot shows the IDEM Entity Registry interface. The top navigation bar includes links for Federations, Identity Providers, Service Providers, Register, and Administration. The breadcrumb trail indicates the current path: DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY. A red arrow points to the 'GARR IDP' link in the breadcrumb, with a red text overlay stating: **CLICK ON THE IDP NAME TO COME BACK AT ITS MAIN PAGE**. Below the breadcrumb, there are tabs for Information, Attributes/Default Policy (which is active), Federations, Entity Categories, and Service Providers. An 'Add attribute' button is located on the right. A table displays the attribute release policy for the 'email' attribute, showing its support/default policy as 'deny' and an edit icon in the Action column.

Attribute name	Attribute support/default policy	Action
email	deny	

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 4 – Set the Attribute Release Policy for SPs



The screenshot shows the 'Identity Provider: GARR IdP' interface. The top navigation bar includes 'Federations', 'Identity Providers', 'Service Providers', 'Register', and 'Administration'. The 'Identity Providers' section is active. Below the navigation bar, the breadcrumb trail reads 'DASHBOARD / IDENTITY PROVIDERS / GARR IDP'. The main content area has a sub-navigation bar with tabs: 'General', 'Membership', 'Metadata', 'Management', and 'Logs/Stats'. The 'Metadata' tab is selected. Below this, there is a sub-navigation bar with tabs: 'Organization', 'Contacts', 'UI information', 'UI Hints', 'SAML', 'Certificates', 'Entity Categories', and 'Attributes'. The 'Attributes' tab is selected. The main content area displays the 'ARP (Attribute Release Policy)' section. It includes a form for 'Individual Attribute Release Policy URL' with a placeholder 'ARP URL'. Below this is a section for 'List of Service Providers which are set to be excluded from ARP'. There is a button labeled 'matrix' with a red arrow pointing to it and a red text overlay that says 'CLICK HERE TO SEE THE SPs MATRIX AND THE ATTRIBUTES THEY NEED'. Below the 'matrix' button is a section for 'Supported attributes' with a table showing 'email' and its description 'E-Mail: Preferred address for e-mail to be sent to this person'.

Identity Provider: GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP

General Membership Metadata Management Logs/Stats

Organization Contacts UI information UI Hints SAML Certificates Entity Categories Attributes

ARP (Attribute Release Policy)

Individual Attribute Release Policy URL ARP URL

List of Service Providers which are set to be excluded from ARP

Attribute release policy overview matrix

Supported attributes

email E-Mail: Preferred address for e-mail to be sent to this person

CLICK HERE TO SEE THE SPs MATRIX AND THE ATTRIBUTES THEY NEED

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 4 – Set the Attribute Release Policy for SPs



Federations

Identity Providers

Service Providers

Register

Administration

EN

Identity Provider: GARR IdP

https://idp.dir.garr.it/idp/shibboleth

Attribute release policy overview

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY OVERVIEW

denied

permitted

not supported

R required

D desired

	cn	displayName	eduPersonAffiliation	eduPersonEntitlement	eduPersonOrgDN	eduPersonOrgUnitDN	eduPersonPrincipalName	eduPersonScopeAffiliation	email	facsimile Telephone Number	givenName	l	mobile	organizationName	persistentId	preferredLanguage	schacHomeOrganization	schacMotherTongue	schacPersonalUniqueID	sn	telephoneNumber	title	transientId	uid
WIFI provided by GARR							R																	
IDEM Website - special contents	R							R							D									
Wiki IDEM Website - https://wiki.idem.garr.it							D	R																
le@rningGARR							R				R				R					R				
GINS - https://gins.garr.it	D						R				D			D						D			R	
IDEM Entity Registry							R				R									R				
VCONF							R	R			R									R				R
FileSender GARR	R						D																	
GARR - Science Gateway																								
GARRBOX Service							R							R						R				R
Firstlogin service for GARRbox							R				R			R						R				R
Filesender for ELCIRA	D			D			D	D	D		R									R				D
GARR WebMeetings Service provided by GARR							R		D		R				R					R				
GARR SP2-test																								R
IDEM Grouper SP	D	D					R				D									D				R
Test SP shib 2.4	D			D	D	D	D	D	D		D		D		D	D	D		D	D	D			
IDEM GARR AAI Wiki	D						R				D									D				

CLICK ON THE CELL TO MODIFY THE RELEASE RULE

ATTRIBUTE SUPPORTED BY THE IDP BUT DENIED TO ALL SPs

D = attribute Desired by the SP

R = attribute Required by the SP for the access

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 4 – Set the Attribute Release Policy for SPs



FederationsIdentity ProvidersService ProvidersRegisterAdministration

Identity Provider: GARR IdP
https://idp.dir.garr.it/idp/shibboleth

DASHBOARDIDENTITY PROVIDERSGARR IDPATtribute Release Policy Overview

denied

permitted

not supported

R required

D desired

	cn	displayname	email	sn	telephoneNumber	transientId	uid
WiFi provided by GARR							
IDEM Website - special contents	R						
Wiki IDEM Website - https://wiki.idem.garr.it							
le@rningGARR							
GIN S - https://gins.garr.it	D						
IDEM Entity Registry							
VCONF							
FileSender GARR	R						
GARR - Science Gateway							
GARRBOX Service							
Firstlogin service for GARRbox							
Filesender for ELCIRA	D						
GARR WebMeetings Service provided by GARR							
GARR SP2-test							
IDEM Grouper SP	D	D					
Test SP shib 2.4	D		D	D	D		
IDEM GARR AAI Wiki	D			R			

Update policy

Requester: https://sgw.garr.it/shibboleth

Attribute name: email

Current attribute flow

supported

default

deny

federation

no policy => inherit from parent

Requester

no policy => inherit from parent

Policy

Please Select

Please Select

never

permit only if required

permit if required or desired

remove policy based on requester

CHOOSE THE RULE TO FOLLOW AND "UPDATE"

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 4 – Set the Attribute Release Policy for SPs



FederationsIdentity ProvidersService ProvidersRegisterAdministration

Identity Provider: GARR IdP
https://idp.dir.garr.it/idp/shibboleth

Attribute release policy overview

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY OVERVIEW

denied
permitted
not supported
R required
D desired

cn	displayName	eduPersonAffiliation	eduPersonEntitlement	eduPersonOrgDN	eduPersonOrgUnitDN	eduPersonPrincipalName	eduPersonScopeAffiliation	email	facsimileTelephoneNumber	givenName	l	mobile	organizationName	persistentId	preferredLanguage	schacHomeOrganization	schacMotherTongue	schacPersonalUniqueID	sn	telephoneNumber	title	transientId	uid
WIFI provided by GARR						R	R																
IDEM Website - special contents					R		R			R				D									
Wiki IDEM Website - https://wiki.idem.garr.it					D		R																
le@rningGARR					R		R			R				R					R				
GINS - https://gins.garr.it	D						R			D			D	D					D				R
IDEM Entity Registry					R		R			R									R				
VCONF						R	R			R									R				R
FileSender GARR	R						D																
GARR - Science Gateway							R																
GARRBOX Service						R				R			R						R				R
Firstlogin service for GARRbox						R				R			R						R				R
Filesender for ELCIRA	D			D		D	D			R									R				D
GARR WebMeetings Service provided by GARR						R		D		R				R					R				
GARR SP2-test																							R
IDEM Grouper SP	D	D				R				D									D				R
Test SP shib 2.4	D			D	D	D	D			D		D		D	D	D			D	D	D		
IDEM GARR AAI Wiki	D					R				D									D				

CLICK ON THE IDP NAME TO COME BACK AT ITS MAIN PAGE

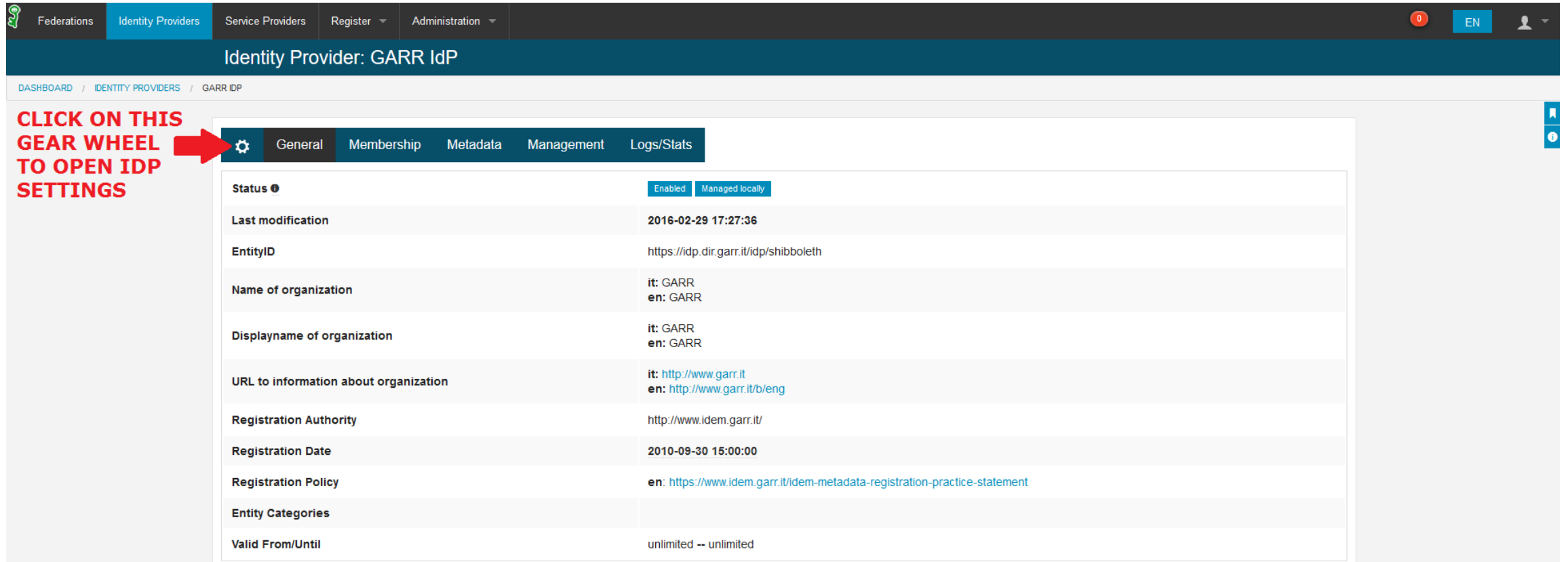
garr

THE NEW RULE HAS BEEN APPLIED!

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 5 – Retrieve the new attribute policy release by URL

CLICK ON THIS GEAR WHEEL TO OPEN IDP SETTINGS →

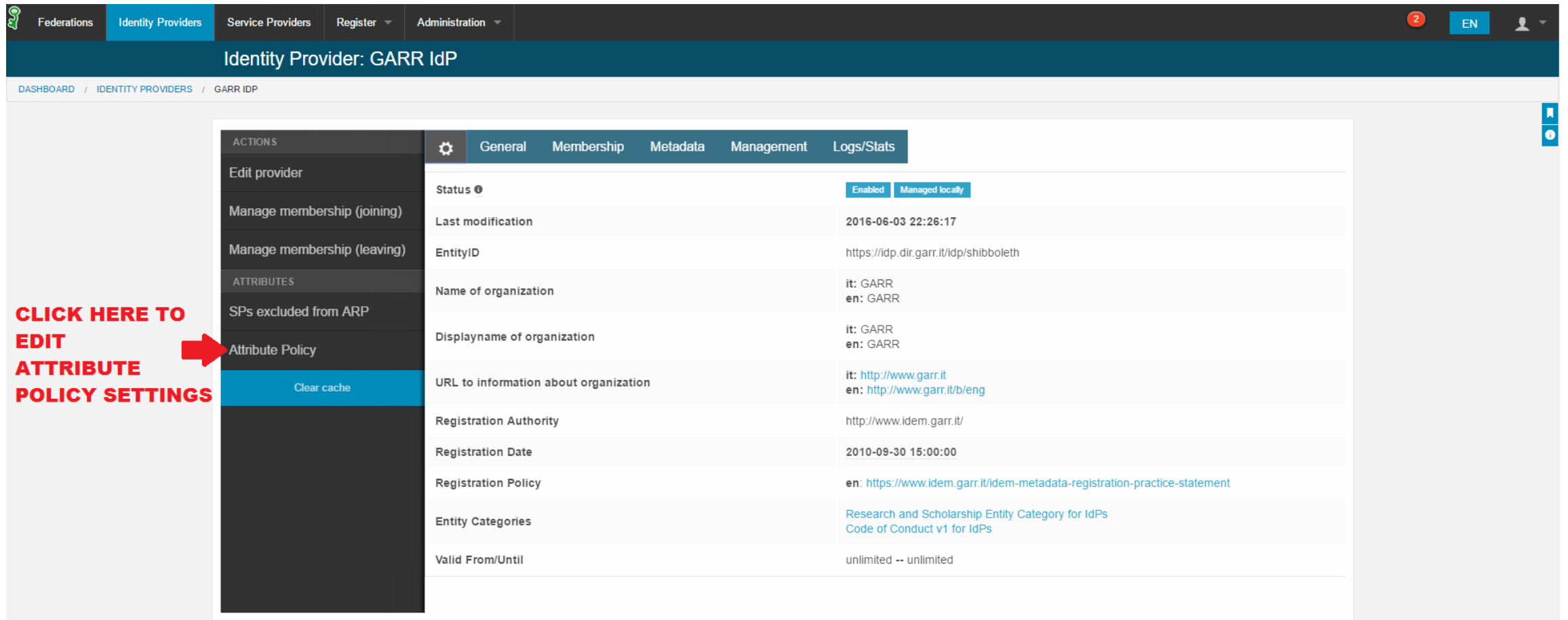


Identity Provider: GARR IdP	
DASHBOARD / IDENTITY PROVIDERS / GARR IDP	
CLICK ON THIS GEAR WHEEL TO OPEN IDP SETTINGS →	
General Membership Metadata Management Logs/Stats	
Status	Enabled Managed locally
Last modification	2016-02-29 17:27:36
EntityID	https://idp.dir.garr.it/idp/shibboleth
Name of organization	it: GARR en: GARR
Displayname of organization	it: GARR en: GARR
URL to information about organization	it: http://www.garr.it en: http://www.garr.it/b/eng
Registration Authority	http://www.idem.garr.it/
Registration Date	2010-09-30 15:00:00
Registration Policy	en: https://www.idem.garr.it/idem-metadata-registration-practice-statement
Entity Categories	
Valid From/Until	unlimited -- unlimited

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 5 – Retrieve the new attribute policy release by URL

CLICK HERE TO EDIT ATTRIBUTE POLICY SETTINGS →



Identity Provider: GARR IdP

DASHBOARD / IDENTITY PROVIDERS / GARR IDP

ACTIONS

- Edit provider
- Manage membership (joining)
- Manage membership (leaving)

ATTRIBUTES

- SPs excluded from ARP
- Attribute Policy**
- Clear cache

General | Membership | Metadata | Management | Logs/Stats

Status ⓘ	Enabled Managed locally
Last modification	2016-06-03 22:26:17
EntityID	https://idp.dir.garr.it/idp/shibboleth
Name of organization	it: GARR en: GARR
Displayname of organization	it: GARR en: GARR
URL to information about organization	it: http://www.garr.it en: http://www.garr.it/b/eng
Registration Authority	http://www.idem.garr.it/
Registration Date	2010-09-30 15:00:00
Registration Policy	en: https://www.idem.garr.it/idem-metadata-registration-practice-statement
Entity Categories	Research and Scholarship Entity Category for IdPs Code of Conduct v1 for IdPs
Valid From/Until	unlimited -- unlimited

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 5 – Retrieve and Use the new custom attribute release policy



Federations Identity Providers Service Providers Register Administration

DASHBOARD / IDENTITY PROVIDERS / GARR IDP / ATTRIBUTE RELEASE POLICY

Information Attributes/Default Policy Federations Entity Categories Service Providers

INFORMATION GUIDE SOON!

- Default Attribute Release Policy - it does not include rules based on Entity Categories:
<https://registry.idem.garr.it/rr3/arp/format2/aHR0cHM6Ly9pZHAuZGlyLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml> **CLICK HERE FOR CUSTOM SHIB IDP v2.x ARP**
- Experimental Attribute Release Policy for ShibbolethIDP ver 2.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/rr3/arp/format2exp/aHR0cHM6Ly9pZHAuZGlyLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 3.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/rr3/arp/format3exp/aHR0cHM6Ly9pZHAuZGlyLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml> **CLICK HERE FOR CUSTOM SHIB IDP v3.x ARP**

HOW TO Use the IDEM Entity Registry for creating custom ARP

STEP 5 – Retrieve and Use the new custom attribute release policy



1. Add the following bean to the «services.xml» :

- `vim /opt/shibboleth-idp/conf/services.xml`

```
<bean id="FileBackedIdemJaggerAttributeFilter"
class="net.shibboleth.ext.spring.resource.FileBackedHTTPResource"
  c:client-ref="shibboleth.FileCachingHttpClient"
  c:url="### IDEM JAGGER ARP URL ###"
  c:backingFile="%{idp.home}/conf/attribute-filter-custom.xml"
  minRefreshDelay="PT5M" maxRefreshDelay="PT1H"
  refreshDelayFactor="0.75"/>
...
<util:list id="shibboleth.AttributeFilterResources">
  ...
  <ref bean="FileBackedIdemJaggerAttributeFilter"/>
</util:list>
```

2. Restart the Attribute Filter Service of the Shibboleth IdP:

- `cd /opt/shibboleth-idp/bin`
- `./reload-service.sh -id shibboleth.AttributeFilterService`

1. By using attribute release policy with rules based on the Entity Categories defined before, it is possible to answer correctly and quickly to the attribute requests coming from the federated resources without change the configurations on your own IdP.
2. By using a tool like Jagger to create an attribute release policy custom, it is possible to answer correctly and quickly to the attribute requests coming from the federated resources not yet R&S or CoCo compliant without changing the configurations on your own IdP, but only acting on the GUI provided by Jagger. (90%)
3. By using a tool like Jagger to create an attribute release policy custom, the IDP Manager, and hence the institution, maintains the authoritative role on the release of the attributes to those resources that are not yet R&S or CoCo compliant.
4. By using a tool like Jagger becomes more difficult met syntax mistakes when you create a custom ARP and its GUI makes all easier.
5. By using a tool like Jagger becomes easy the research and the discovery of the new resources available.

Credits



- Chris Phillips
- Brook Schofield
- Ann Harding

Thank you

Any Questions?

marialaura.mantovani@garr.it
simona.venuti@garr.it
marco.malavolti@garr.it



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).