

The EGI AAI “CheckIn” Service

Mario David - LIP Lisbon
On behalf of the EGI AAI Support Team

1st ASTERICS-OBELICS Workshop
12-14 December 2016, Rome, Italy.



www.egi.eu

Astronomy ESFRI & Research Infrastructure Cluster
ASTERICS - 653477

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142



- Intro to EGI and EGI challenges
- EGI AAI CheckIn Service
- Levels of Assurance
- EGI Unique Identifier
- Credential translation service (further details - Licia's presentation AARC)

- Demo

The EGI Services are provided by the EGI Federation

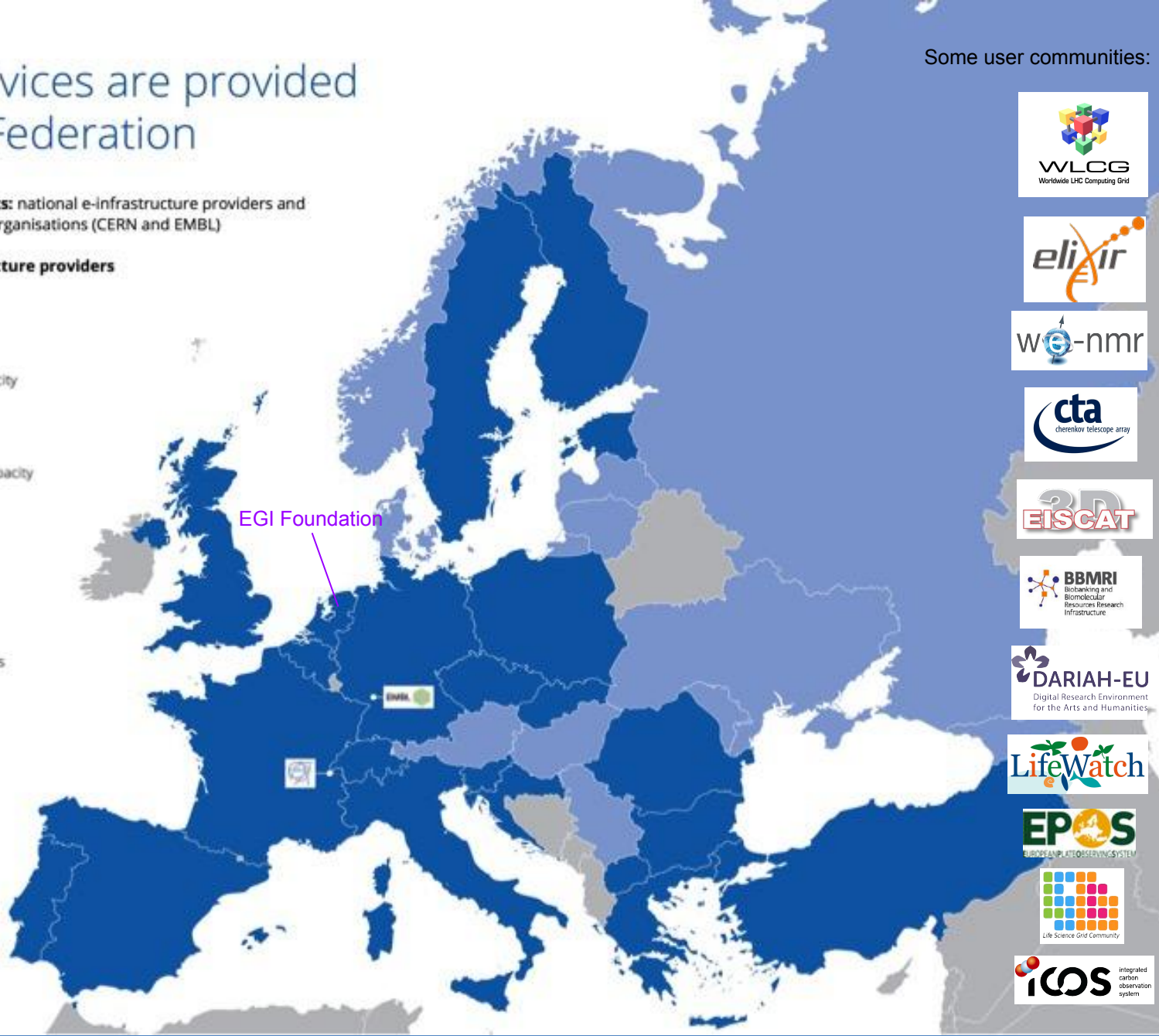
- **EGI Council participants:** national e-infrastructure providers and international research organisations (CERN and EMBL)
- **Integrated e-infrastructure providers**

 **826,000**
Cores of compute capacity

 **560,000**
Terabytes of storage capacity

 **48,000**
Users

 **15**
Research Infrastructures integrated with EGI



Some user communities:

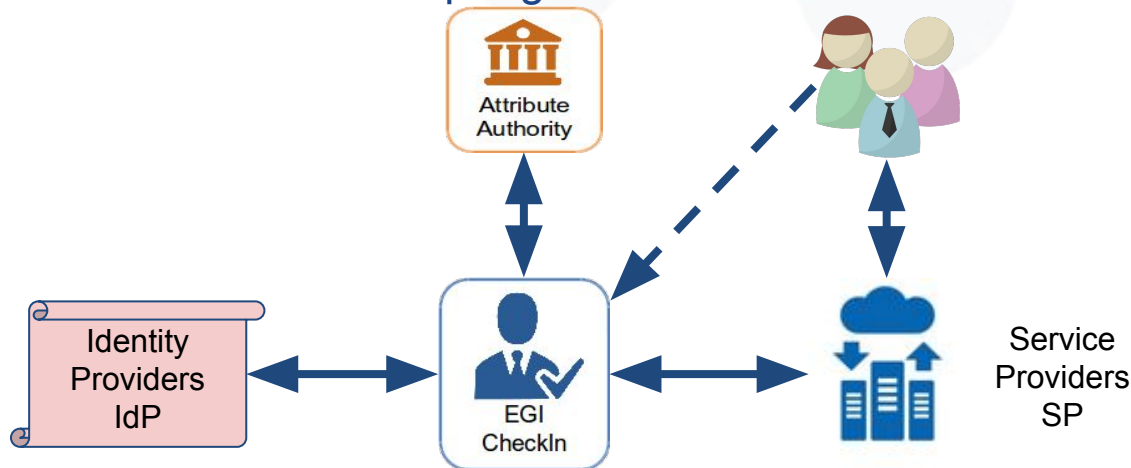


EGI challenges

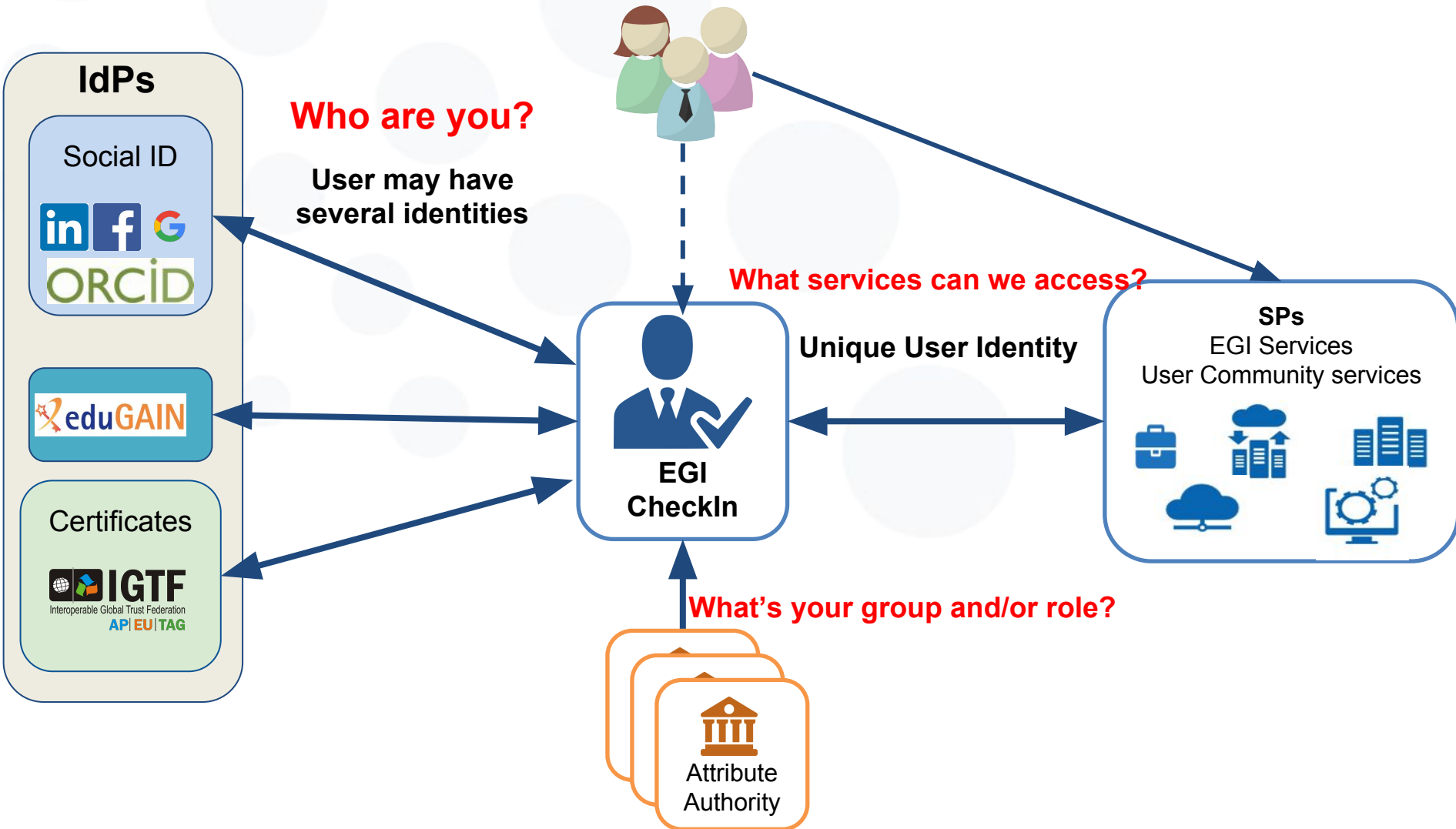
- Many users - Many Identity Providers (**IdPs**) ↔ Many Service Providers (**SPs**)
- Scalable authentication mechanisms
- **Trust** chain between Users (IdPs) and SPs - and vice-versa
- A way for communities to organize their users and how the those users access the services. A means to have “**groups**” and “**roles**”, that differentiate users capabilities to a given service.

EGI AAI CheckIn Service I

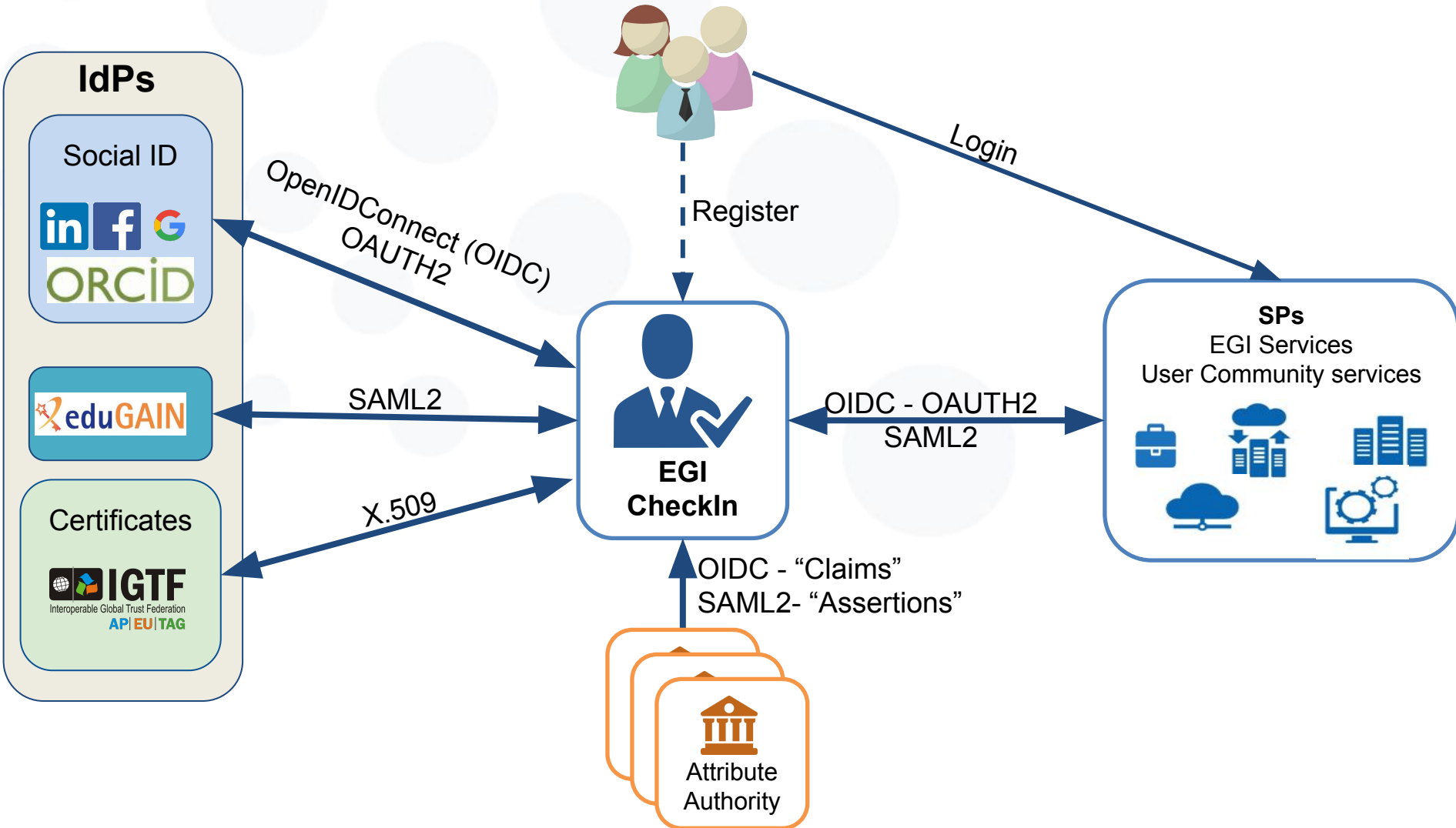
- Federated Identity Access Management (IAM) solution for research communities.
- Combines multi-protocol federated access and flexible group/Virtual Organization management capabilities in one single platform.
- Designed to enable users to transparently access distributed federated service providers.
- Minimize overhead for end users, communities and service providers.
- Implements the AARC bluepring



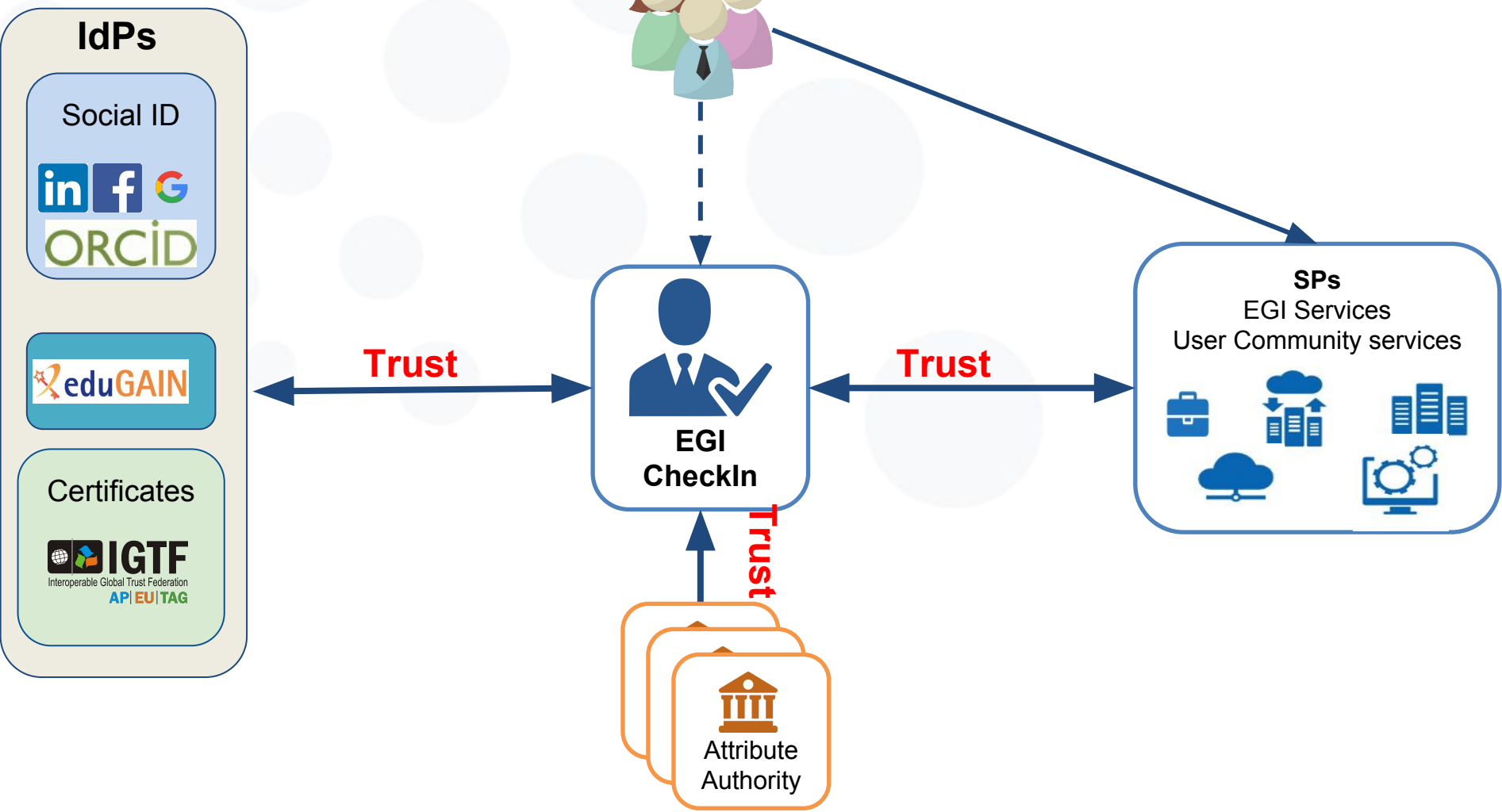
EGI CheckIn: AAI Federation II



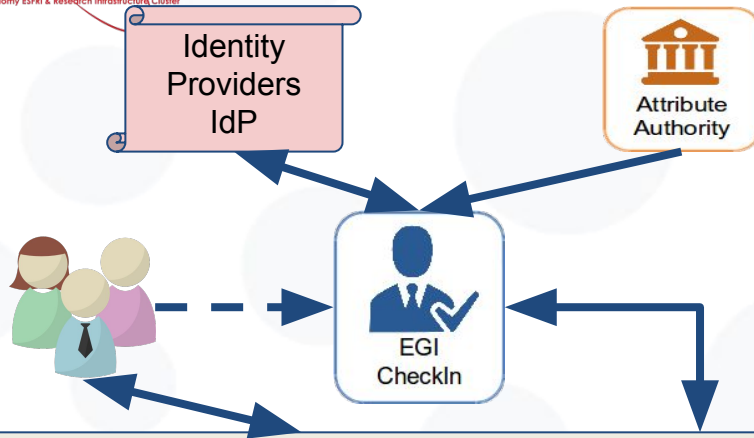
EGI CheckIn: AAI Federation III



EGI CheckIn: AAI Federation IV

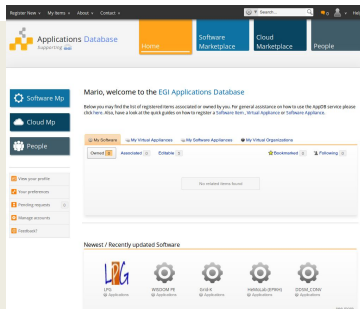
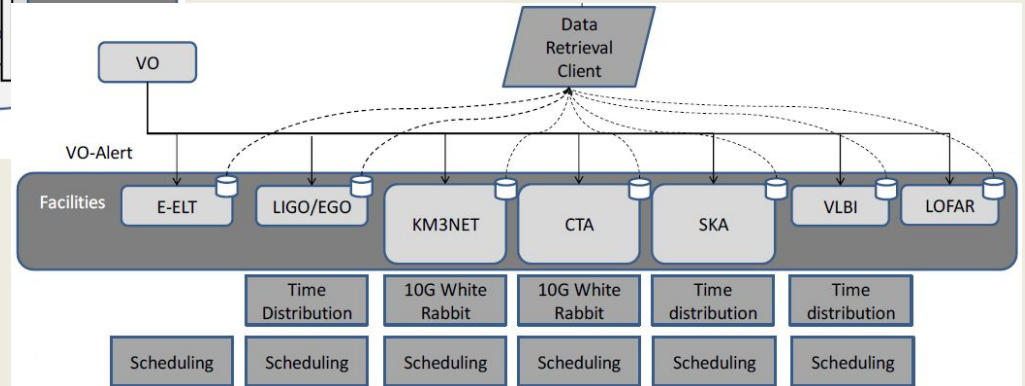
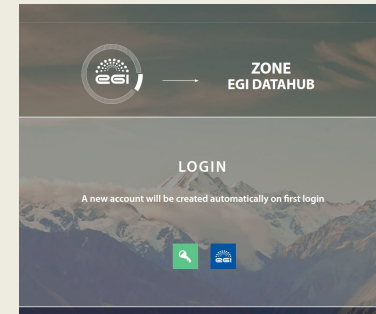
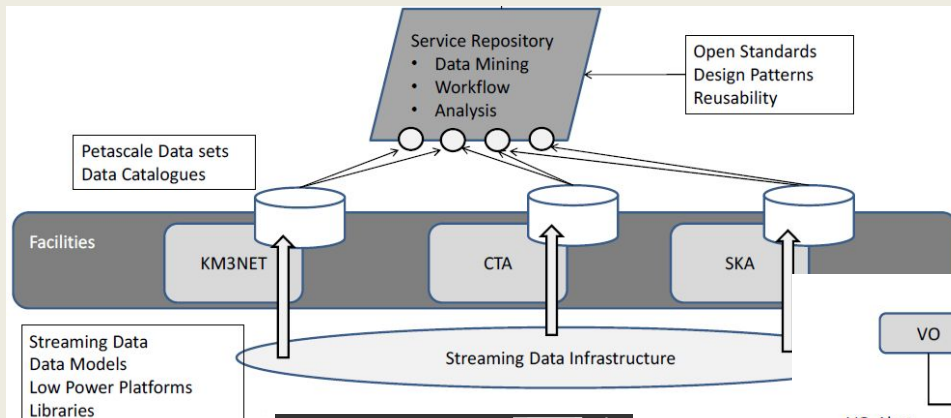


Where it fits in...



A possible model for OBELICS/Cleopatra

Service Providers - SPs



What is “Levels of Assurance” - LoA

- ***“How confident you are that the person who is authenticating really is the person who is authenticating”***
 - Not all the credentials are the same!
- **Examples:**
 - Very high level of assurance: eID - e-Government ID.
 - High level of assurance with ID verification:
 - X509 certificates, many institutional IdP
 - Social media credentials:
 - Everyone with an email account can have one.
- **Not always the highest LoA is required:**
 - For some low-risk activities low assurance credentials are usable!
- **The minimum LoA required is determined by the user community and the service provider requirements.**

Use cases for the LoA in EGI

- EGI services LoA are defined by EGI.
- Community services LoA defined by the community.
- Allow an IdP to advertise those LoAs for which it is able to meet the associated requirements.
- Allow an IdP to indicate the actual LoA in its responses.
- Allow a SP to express its expectations for the LoA at which a user should be authenticated.

Levels of Assurance

- LoA: null
 - Social-identity credentials with no vetting, no uniqueness of the ID
 - Allowed in EGI:
 - Access open data.
 - Perform read-only operation on non-sensitive data.
- LoA: A
 - EduGain Accounts
 - Allowed in EGI:
 - Low risk services, which do not hold data
 - Demos and training - limited time duration

Levels of Assurance

- LoA: B

- Subset of EduGain - IdPs that comply with R&S and Sirtfi (includes X509 certificates):
 - REFEDS: A Security Incident Response Trust Framework for Federated Identity ([Sirtfi](#))
 - REFEDS: Research & Scholarship Entity Category ([R&S](#))
- Allowed in EGI:
 - Submit pre-defined applications through science gateways.
 - Use PaaS on the cloud.

- LoA: C

- IdPs with LoA: B **plus** meet the requirement of IGTF [BIRCH](#) - identity vetting
- Allowed in EGI:
 - Submit and manage virtual machines.
 - Access sensitive protected data.

EGI User Identifier

- EGI User ID is created by the Checkin service at the moment of the user's first connection - User registers in the EGI Checkin.
- EGI Checkin service “generates” the EGI User ID from the attribute “eduPersonUniqueId” released by the user IdP.
- EGI User ID is:
 - **personal, persistent, non-reassignable, non-targeted, globally unique, opaque**

Attributes released by the IdP (SAML assertions)

Mail	Display name	Given name	Surname	Distiguated name
------	--------------	------------	---------	------------------

EGI Checkin service



Unique, non-reassignable, persistent pseudonymous EGI ID

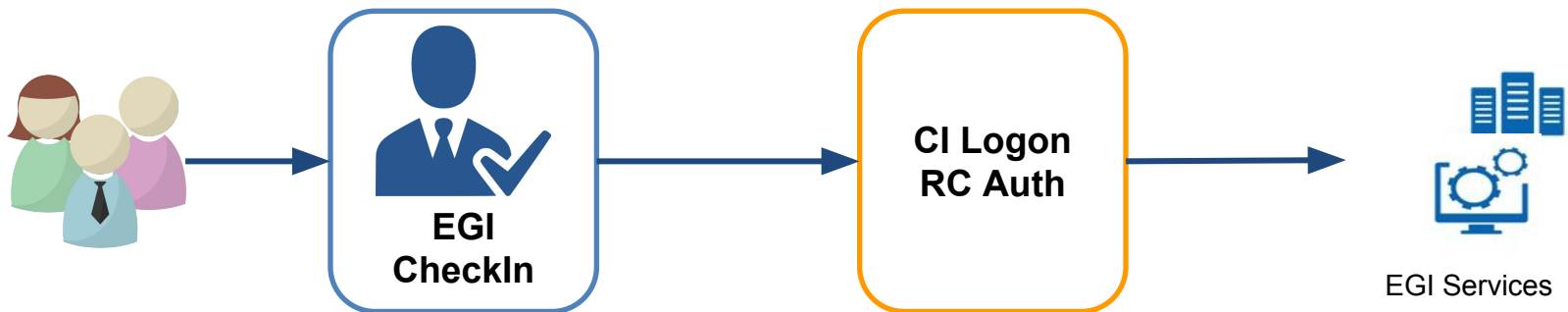
556d330ce42165b90550088edd8271447103fa119d52ad6d3c7629052cb56126@egi.eu

Identity assurance profile

https://aai.egi.eu/LoA#Low

Credential translation service

- CheckIn service is integrated with the RC Auth Online CA to provide X.509 credentials:
 - The CI Logon delegation service makes possible to implement secure provisioning of X.509 credentials to science gateways, portals and other applications.
 - Workflow designed in the AARC project.
- RC Auth is an accredited certification authority in the IGTF federation.
 - It will be accepted in all EGI services, and in all the other federations accepting IGTF certificates.
- All the users holding credentials with a sufficient level of assurance are able to access RC Auth certificates through the CheckIn Service.



The EGI AAI “CheckIn” Service Demo

Mario David - LIP Lisbon
On behalf of EGI-Engage JRA1.1

1st ASTERICS-OBELICS Workshop
12-14 December 2016, Rome, Italy.



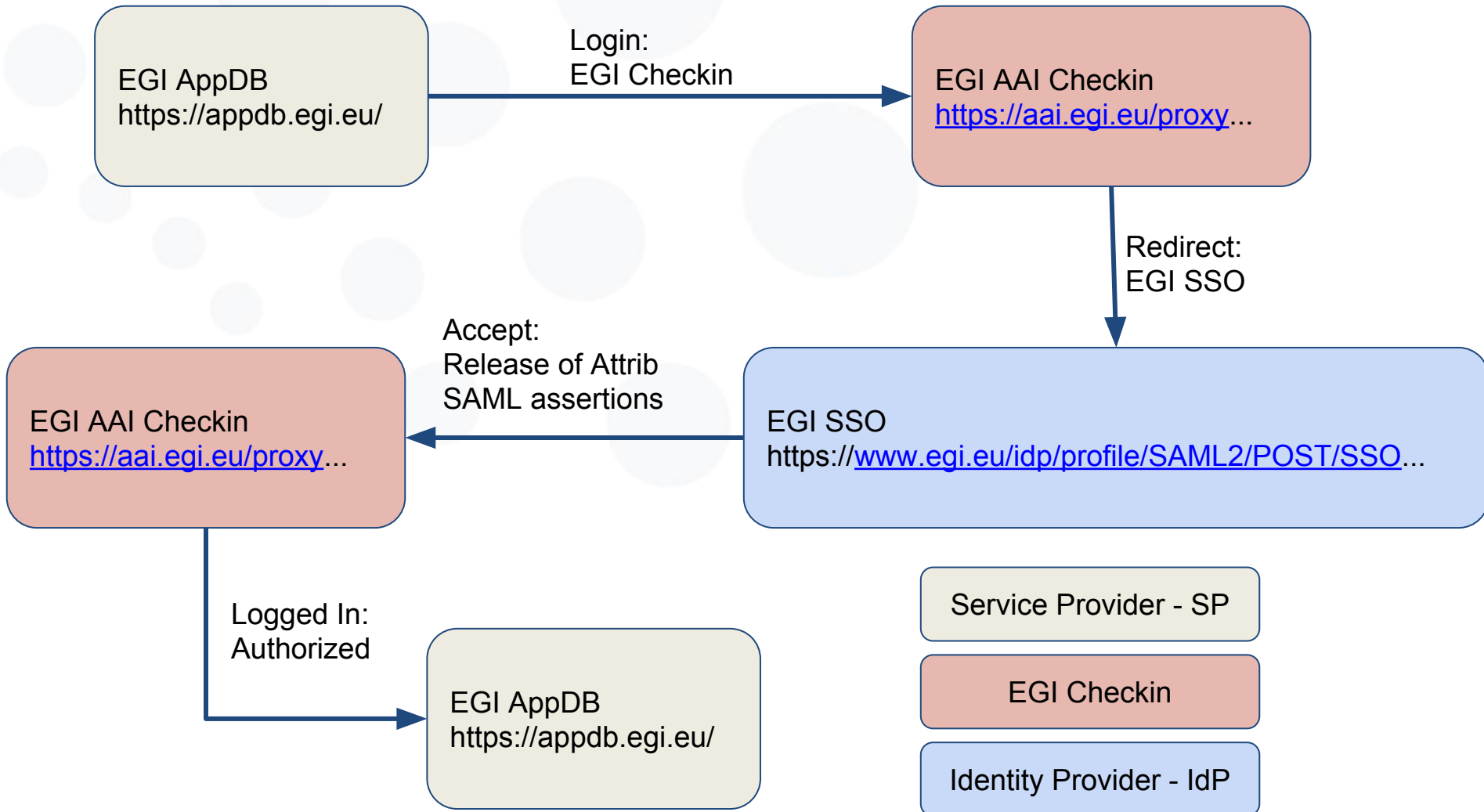
www.egi.eu

Astronomy ESFRI & Research Infrastructure Cluster
ASTERICS - 653477

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142



Demo workflow



AppDB login - <https://appdb.egi.eu/>



Navigation menu: About, Contact, Search, Sign In, Help.

Main navigation: Applications Database (Supporting EGI), Home, Software Marketplace, Cloud Marketplace.

Dropdown menu (Sign In): EGI AAI Check-in, Create an EGI SSO account, x509 Digital Certificates.

Software Mp

Cloud Mp

People

Welcome to the EGI Applications Database

The EGI Applications Database (AppDB) is a central service that stores and provides to the public information about:

- **software solutions** in the form of native software products, virtual appliances and/or software appliances,
- the **programmers** and the **scientists** who are involved, and
- **publications** derived from the registered solutions

Reusing software products, registered in the AppDB, means that scientists and developers may find a solution that can be directly utilized on the European Grid Infrastructure. without reinventing the wheel....read more






Need access

Register your solution

Join as a contact

Send us your feedback

Newest / Recently updated Software

				
LPG Applications	WISDOM PE Applications	Grid-K Applications	HeMoLab (EPIKH) Applications	DDSM_CONV Applications

...see more

English | Bokmål | Nynorsk | Sámegeella | Dansk | Deutsch | Svenska | Suomi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

You have previously chosen to authenticate at **EGI SSO**

Login at EGI SSO

All

EGI

ELIXIR

Search for your institution...



 EGI SSO

ELIXIR research infrastructure AAI



Login to EGI AAI Service Provider
Proxy

Username

mdavid

Password

.....

Don't Remember Login

Clear prior granting of permission for
release of your information to this
service.

Login



You are about to access the service:
EGI AAI Service Provider Proxy of EGI.eu

Description as provided by this service:
Service provider proxy for all federated EGI services

[Additional information about the service](#)

Information to be Provided to Service

cn	Mario David
displayName	Mario David
eduPersonEntitlement	urn:egi.eu:group:egi-engage-wp6.1 urn:egi.eu:group:cc-epos urn:egi.eu:group:otag urn:egi.eu:group:egi-engage-cb urn:egi.eu:group:egi-engage-training-coordination urn:egi.eu:group:egi-aal-support urn:egi.eu:group:fedcloud-tf urn:egi.eu:group:egi-engage-members urn:egi.eu:group:fedcloud-users urn:egi.eu:group:egi-engage-JRA1-aal urn:egi.eu:group:fc-usersupport urn:egi.eu:group:wiki-editors urn:egi.eu:group:cc-lifewatch urn:egi.eu:group:aal-cloud-pilot urn:egi.eu:group:egi-emso urn:egi.eu:group:noc-managers urn:egi.eu:group:egi-engage-wp6.2
eduPersonPrincipalName	mdavid@egi.eu
egiPartnerOrg	LIP
givenName	Mario
mail	david@lip.pt
o	LIP
sn	David
uid	mdavid
userCertificateSubject	/O=GRID-FR/C=FR/O=CNRS/OU=IPGP/CN=Mario David /C=PT/O=LIPCA/O=LIP/OU=Lisboa/CN=Mario David

displayName	Mario David
eduPersonEntitlement	urn:egi.eu:group:egi-engage-wp6.1 urn:egi.eu:group:cc-epos urn:egi.eu:group:otag urn:egi.eu:group:egi-engage-cb urn:egi.eu:group:egi-engage-training-coordination urn:egi.eu:group:egi-aal-support urn:egi.eu:group:fedcloud-tf urn:egi.eu:group:egi-engage-members urn:egi.eu:group:fedcloud-users urn:egi.eu:group:egi-engage-JRA1-aal urn:egi.eu:group:fc-usersupport urn:egi.eu:group:wiki-editors urn:egi.eu:group:cc-lifewatch urn:egi.eu:group:aal-cloud-pilot urn:egi.eu:group:egi-emso urn:egi.eu:group:noc-managers urn:egi.eu:group:egi-engage-wp6.2
eduPersonPrincipalName	mdavid@egi.eu
egiPartnerOrg	LIP
givenName	Mario
mail	david@lip.pt
o	LIP
sn	David
uid	mdavid
userCertificateSubject	/O=GRID-FR/C=FR/O=CNRS/OU=IPGP/CN=Mario David /C=PT/O=LIPCA/O=LIP/OU=Lisboa/CN=Mario David

[Data privacy information of the service](#)

The information above would be shared with the service if you proceed. Do you agree to release this information to the service every time you access it?

Select an information release consent duration:

- Ask me again at next login
 - I agree to send my information this time.
- Ask me again if information to be provided to this service changes
 - I agree that the same information will be sent automatically to this service in the future.
- Do not ask me again
 - I agree that **all** of my information will be released to **any** service.

This setting can be revoked at any time with the checkbox on the login page.

Reject

Accept



English | Bokmål | Nynorsk | Sámeigiella | Dansk | Deutsch | Svenska | Suomi | Español | Français | Italiano | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

EGI Applications Database requires that the information below is transferred.

Remember

Yes, continue

No, cancel

Information that will be sent to EGI Applications Database

Entitlement regarding the service

- urn:mace:egi.eu:www.egi.eu:egi-engage-wp6.1:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:cc-epos:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:otag:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-cb:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-training-coordination:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-aai-support:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:fedcloud-tf:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-members:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:fedcloud-users:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-JRA1-aai:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:fc-usersupport:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:wiki-editors:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:cc-lifewatch:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:aai-cloud-pilot:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-emso:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:noc-managers:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-wp6.2:member@egi.eu
- urn:mace:egi.eu:goc.egi.eu:46162G0:INSU01-PARIS:Site+Operations+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:46162G0:INSU01-PARIS:Site+Administrator@egi.eu
- urn:mace:egi.eu:goc.egi.eu:265G0:NGC-INGRID-PT:Site+Operations+Deputy+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:296G0:LIP-Coimbra:Site+Operations+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:21:NGI_IBERGRID:NGI+Operations+Deputy+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:121G0:LIP-Lisbon:Site+Operations+Manager@egi.eu

Mail

david@lip.pt

- urn:mace:egi.eu:www.egi.eu:cc-epos:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:otag:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-cb:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-training-coordination:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-aai-support:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:fedcloud-tf:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-members:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:fedcloud-users:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-JRA1-aai:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:fc-usersupport:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:wiki-editors:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:cc-lifewatch:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:aai-cloud-pilot:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-emso:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:noc-managers:member@egi.eu
- urn:mace:egi.eu:www.egi.eu:egi-engage-wp6.2:member@egi.eu
- urn:mace:egi.eu:goc.egi.eu:46162G0:INSU01-PARIS:Site+Operations+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:46162G0:INSU01-PARIS:Site+Administrator@egi.eu
- urn:mace:egi.eu:goc.egi.eu:265G0:NGC-INGRID-PT:Site+Operations+Deputy+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:296G0:LIP-Coimbra:Site+Operations+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:21:NGI_IBERGRID:NGI+Operations+Deputy+Manager@egi.eu
- urn:mace:egi.eu:goc.egi.eu:121G0:LIP-Lisbon:Site+Operations+Manager@egi.eu

Mail

david@lip.pt

Display name

Mario David

Given name

Mario

Surname

David

Distinguished name

- /O=GRID-FR/C=FR/O=CNRS/OU=IPGP/CN=Mario David
- /C=PT/O=LIPCA/O=LIP/OU=Lisboa/CN=Mario David

Unique, non-reassignable, persistent pseudonymous EGI ID

556d330ce42165b9055008edd8271447103fa119d52ad6d3c7629052cb56126@egi.eu

Identity assurance profile

https://aai.egi.eu/LoA#Low



Register New ▾ My Items ▾ About ▾ Contact ▾

Search... 0 Help

Applications Database
Supporting egi

Home Software Marketplace Cloud Marketplace People

Software Mp

Cloud Mp

People

View your profile

Your preferences

Pending requests 0

Manage accounts

Feedback?

Mario, welcome to the EGI Applications Database

Below you may find the list of registered items associated or owned by you. For general assistance on how to use the AppDB service please click here. Also, have a look at the quick guides on how to register a Software Item , Virtual Appliance or Software Appliance.

My Software My Virtual Appliances My Software Appliances My Virtual Organizations

Owned 0 Associated 0 Editable 5 Bookmarked 0 Following 0

No related items found

Newest / Recently updated Software



LPG Applications

WISDOM PE Applications

Grid-K Applications

HeMoLab (EPIKH) Applications

DDSM_CONV Applications

...see more



Since: 2014-10-24

Mario David

[\[permalink\]](#)

Gender: Male (id:906)
Scientific Orientation: Systems Administration
Country: Portugal  [View country's related items](#)
Access Groups:  National Representatives, Power Users
edit groups

Organizations: *No related organizations*
Projects: *No related projects*

Virtual Organization Membership

Contact Information

✉ e-mail : david@lip.pt

EGI Datahub - <https://datahub.egi.eu/>



ZONE
EGI DATAHUB

LOGIN

A new account will be created automatically on first login



Data and storage
management framework

OneData

Projects:
Indigo-Datacloud
EGI-Engage

Thank you for your attention.

Questions?

Acknowledgement

- H2020-Astronomy ESFRI and Research Infrastructure Cluster (Grant Agreement number: 653477).
- EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142



www.egi.eu

