



[www.egi.eu](http://www.egi.eu)

@EGI\_eInfra

## EGI Check-in pour les fournisseurs de services

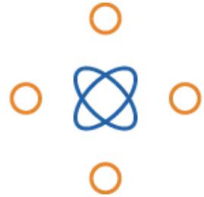
Baptiste Grenier (EGI Foundation) de la part de  
Nick Evangelou (GRNET)  
Nicolas Liampotis (GRNET)  
Valeria Ardizzone (EGI Foundation)



**The work of the EGI Foundation**  
*is partly funded by the European Commission  
under H2020 Framework Programme*

- À propos d'EGI
- EGI Check-in en un mot
- Gestion de l'identité utilisateur (cible: **utilisateur final**)
- Gestion des Organisations Virtuelles (VO) (cible: **communauté d'utilisateurs**)
- Intégration d'un service avec EGI Check-in (cible: **fournisseur de services**)
  - Pour les services SAML ou OIDC
  - Contrôle de l'accès des utilisateurs (authorisation)
  - Utilisation de certificats X.509
  - Collection de statistiques

# À propos d'EGI



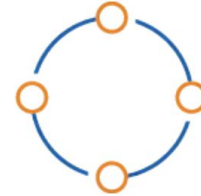
## La Fédération EGI

EGI est une fédération de fournisseurs de ressources de calcul et de stockage, unis par la mission de fournir des services avancés de calcul et d'analyse de données pour la recherche et l'innovation.



## La Fondation EGI

La Fondation EGI est une organisation à but non lucratif créée pour coordonner et développer l'infrastructure EGI et collaborer avec les différents utilisateurs des services EGI.



## La Communauté EGI

La communauté EGI est une communauté de chercheurs, de développeurs, de bailleurs de fonds, de technologues, de rêveurs et de faiseurs : toute personne intéressée par l'informatique avancée pour la recherche.





## Vision

Tous les chercheurs bénéficient d'un accès transparent aux services, aux ressources et à l'expertise pour collaborer et mener des recherches et des innovations de niveau mondial.

## Mission de la Fédération EGI

Fournir des solutions ouvertes pour le calcul avancé et l'analyse des données dans la recherche et l'innovation

## Mission de la Fondation EGI

Permettre à la Fédération EGI de servir ensemble la recherche et l'innovation internationales

[www.egi.eu](http://www.egi.eu)



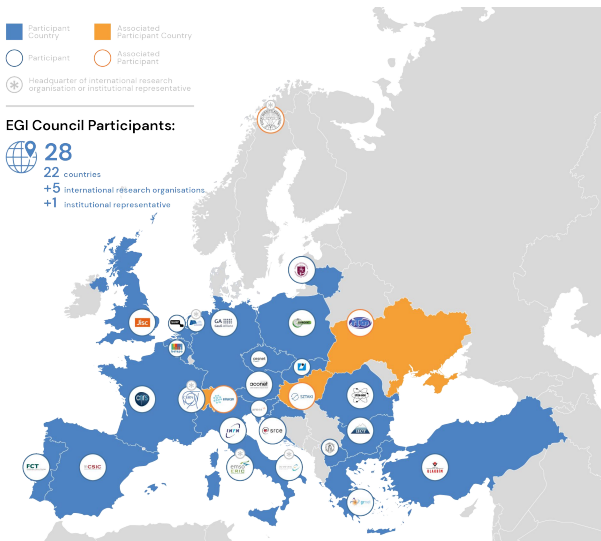
## Fédération EGI

Une infrastructure numérique phare européenne pour le calcul scientifique à forte intensité de données

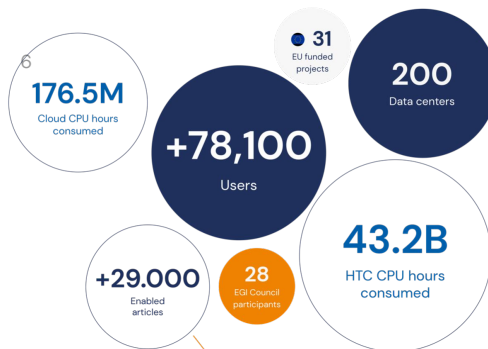


### EGI Council Participants:

 **28**  
 22 countries  
 +5 international research organisations  
 +1 institutional representative



## EGI en chiffres <sup>1</sup>



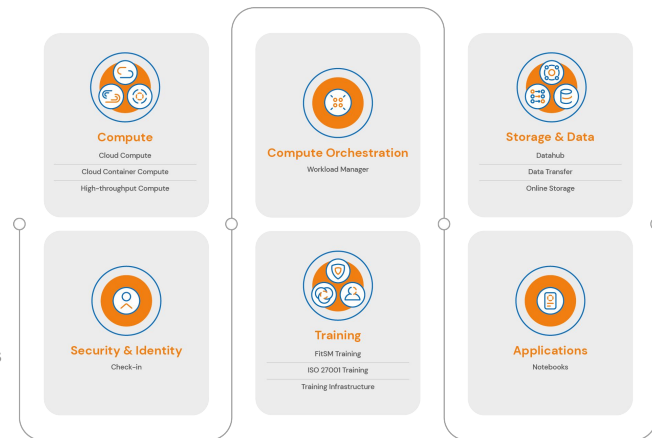
## Une fédération, pourquoi ?

- Soutenir la science à l'échelle internationale
- Construire une installation de recherche de très grande envergure
- Investir au niveau national, accéder au niveau mondial
- Mettre l'informatique au service des données

## Services EGI

EGI fournit des services informatiques avancés pour soutenir les scientifiques, les projets internationaux, les infrastructures de recherche et les entreprises.

## Services EGI pour la recherche



<sup>1</sup>the infographic shows the latest number of funded projects, members and data centers (updated in Sep 2022) and all-time data for the HTC and Cloud numbers according to the EGI accounting portal)

# EGI Check-in en un mot

Solution de gestion des identités et des accès pour sécuriser l'accès aux services et aux ressources.



## Composants

- Proxy IdP/SP (médiateur d'identité)
- Inscription des utilisateurs et gestion des groupes
- Federation Registry

## Documentation

- [Guide d'utilisation](#)
- [Guides d'integration](#)

# La motivation derrière Check-in

Connexion unique aux services par le biais de fournisseurs d'identité académiques (eduGAIN), de médias sociaux (par exemple, Google, Facebook) et d'autres fournisseurs d'identité gérés par la communauté.

Accès fédéré à de multiples fournisseurs de services hétérogènes (web et non-web) utilisant différentes technologies (OpenID Connect, OAuth 2.0, SAML et certificats X.509)

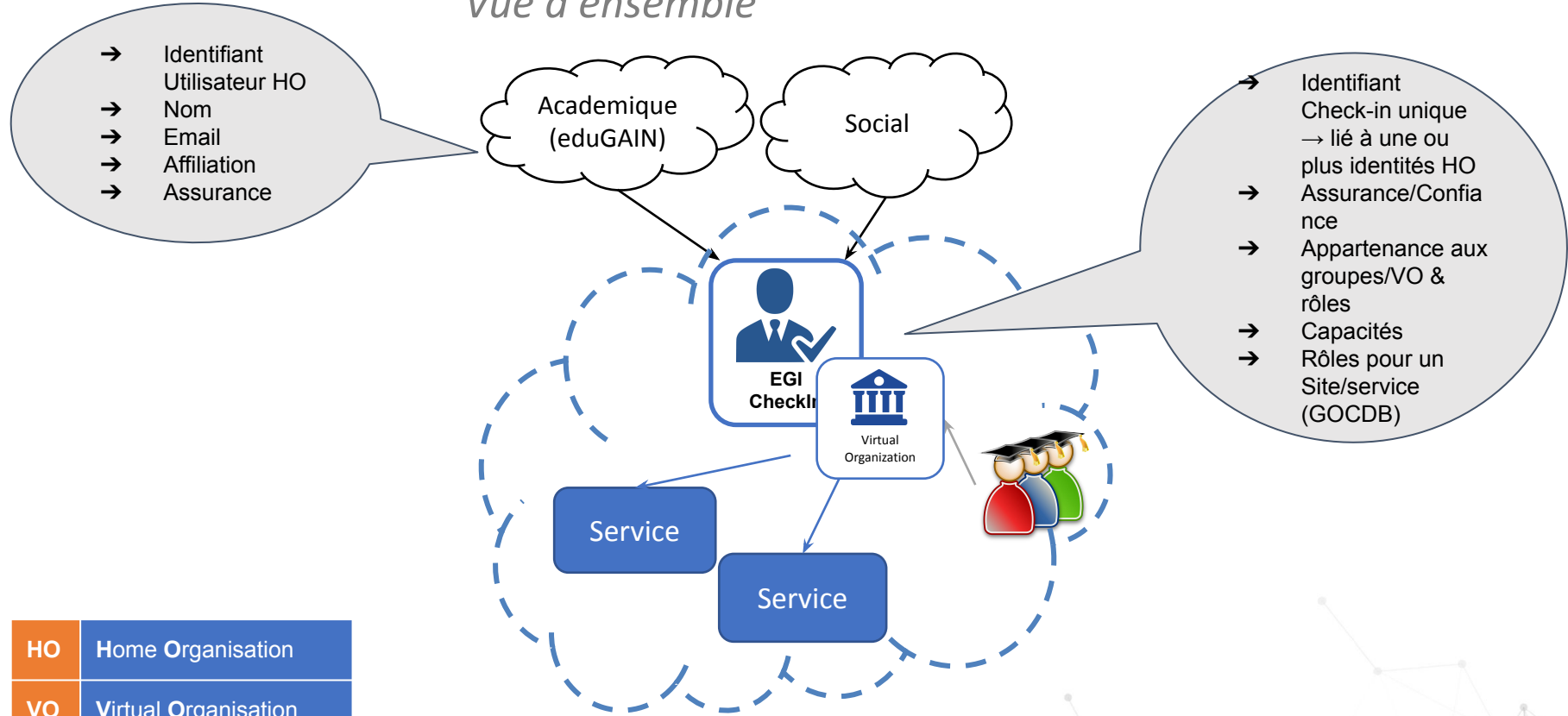
Accès aux ressources à l'aide de différents identifiants de connexion (académiques/sociaux) via la liaison d'identité.

Expression du niveau de confiance dans les assertions d'identité

Agrégation et harmonisation des informations relatives aux autorisations (organisations/groupes virtuels, rôles, confiance) provenant de sources multiples.

# Authentification & Autorisation

## Vue d'ensemble

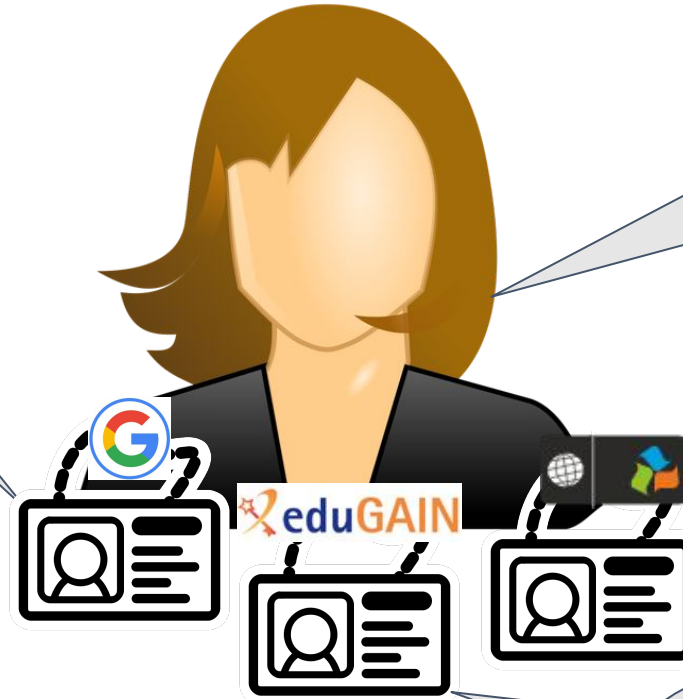


HO	Home Organisation
VO	Virtual Organisation

# Authentication & Autorisation

## Attributs d'identité

- Identifiant Utilisateur HO
- Nom
- Email
- Affiliation
- Assurance

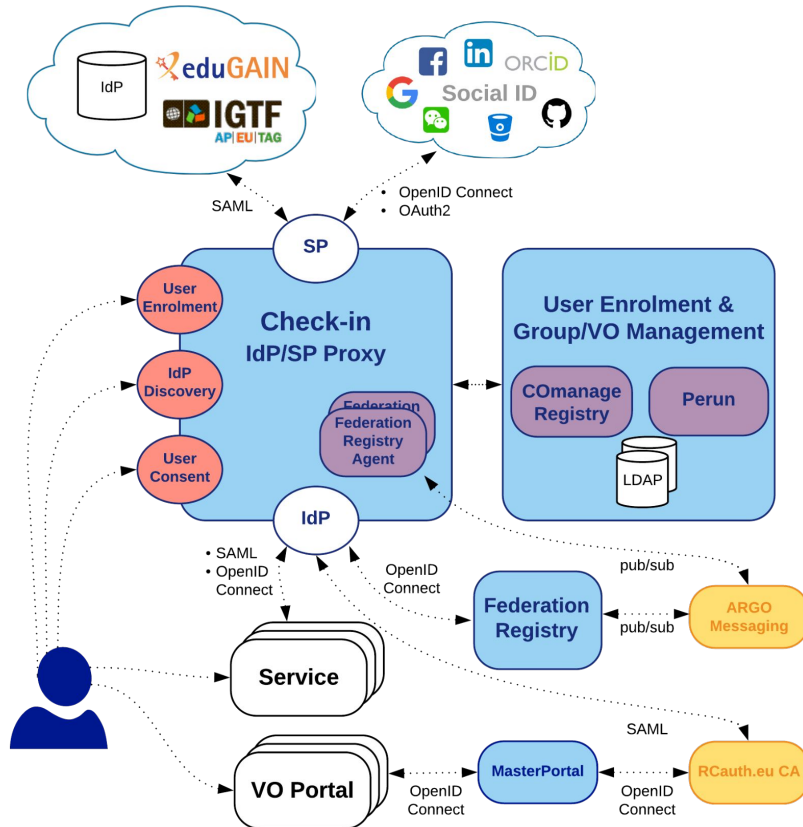


- Identifiant Check-in unique → lié à une ou plus identités HO
- Assurance/Confiance
- Appartenance aux groupes & rôles VO
- Capacités
- Rôles pour un Site/service (GOODB)

- Identifiant Utilisateur HO
- Nom
- Email
- Affiliation
- Assurance

- Identifiant Utilisateur HO
- Nom
- Email
- Affiliation
- Assurance

HO	Home Organisation
VO	Virtual Organisation

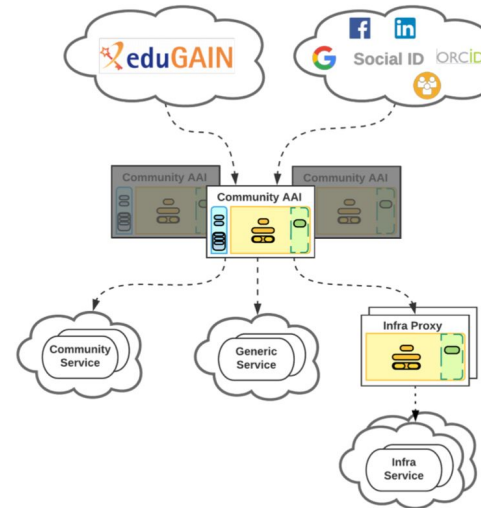
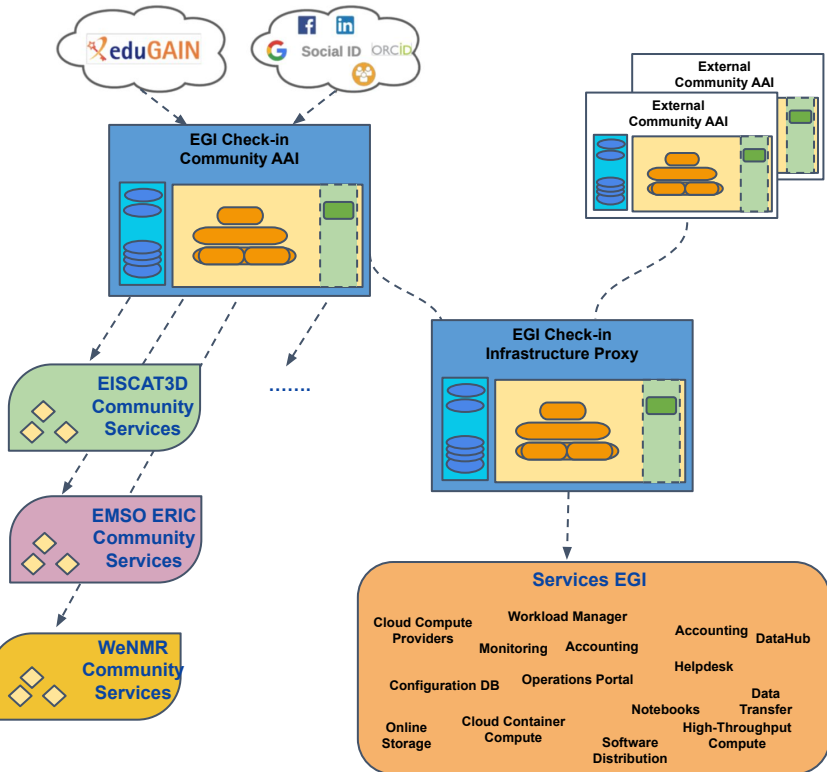


Implémentation de l'architecture du plan directeur de l'AARC

- Point d'intégration unique pour les fournisseurs d'identité (IdP) et les fournisseurs de services (SP).
- Enregistré dans eduGAIN en tant que SP conforme au cadre de sécurité REFEDS (R&S) et Sirtfi.
- Tous les services finaux connectés peuvent avoir un IdP configuré de manière statique.
- Inutile d'exécuter un service de découverte d'IdP pour chaque service.
- Tous les SP connectés obtiennent des identifiants d'utilisateur harmonisés et des ensembles d'attributs d'autorisation correspondants provenant de différents IdP.



### Écosystème EGI

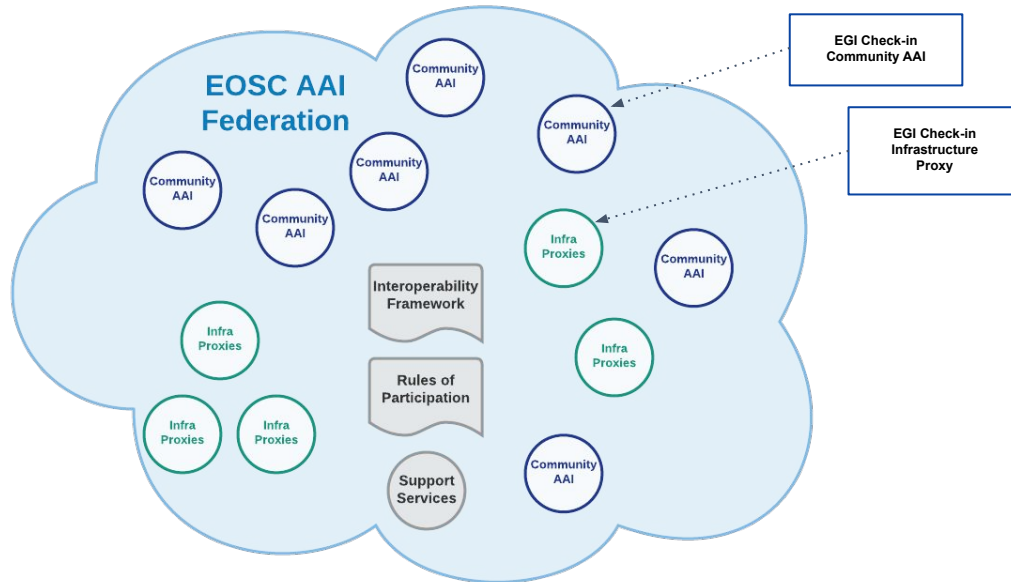


### "Community AAI"

L'objectif du "Community AAI" est de simplifier l'accès des chercheurs aux services, tant ceux fournis par leur propre infrastructure que ceux fournis par les infrastructures partagées avec d'autres communautés.

### "Infrastructure Proxy"

Le "Infrastructure Proxy" permet aux infrastructures disposant d'un grand nombre de ressources, de les fournir via un point d'intégration unique. L'infrastructure peut donc gérer de manière centralisée toutes les politiques et la logique métier pour mettre ces ressources à la disposition de plusieurs communautés.



- Les "Community AAI" et les "Infrastructure proxies" se connectent une fois à la Fédération EOSC AAI (enregistrement des métadonnées, des espaces de noms URN, des politiques, etc.)
- Conformité de l'interopérabilité technique testée et contrôlée par la Fédération EOSC AAI.
- Conformité au RGPD et à la politique de sécurité (avis de politique, politique d'utilisation acceptable, etc.) évaluée par la Fédération EOSC AAI.
- Les "Community AAI" et "Infrastructure Proxies" découvrent et établissent la confiance avec le reste des "Community AAI" et des "infrastructure proxies" par le biais de la fédération des IAA de l'EOSC.

Le [projet EOSC Future](#) se concentre sur les aspects de mise en œuvre de l'EOSC AAI sur la base du [Rapport sur EOSC AAI](#) publié par la Task Force AAI du WG Architecture du bureau exécutif EOSC. L'équipe EGI Check-in est impliquée dans les deux domaines de travail parallèles suivants :

- **Domaine 1** concerne l'**EOSC Core** et ses exigences à partir de l'EOSC AAI (niveau **micro**).
- **Domaine 2** concerne la **mise en œuvre de l'EOSC AAI** au niveau **macro** sur les aspects inter-infrastructures/domaines.

# Gestion de l'identité utilisateur

*Pour les utilisateurs finaux*

## Étape 1

Revoir les informations du profil utilisateur

- nom
- email
- affiliation

et agréer la Politique d'Utilisation Acceptable (AUP)

## Étape 2

Confirmation de l'email - *uniquement si une adresse électronique vérifiée n'est pas publiée par le fournisseur d'identité authentifiant l'utilisateur.*

## Accès

Accéder aux ressources

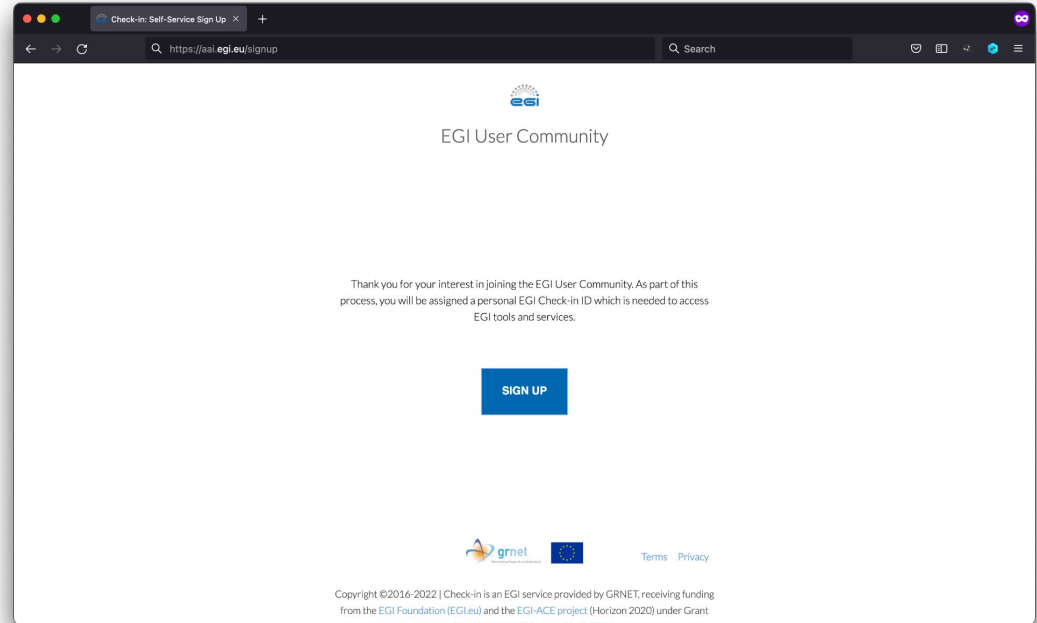
Fonctionnalités supplémentaires:

- Liaison d'identité
- Intégration avec l'AC en ligne RCAuth pour X.509

Pour accéder aux ressources protégées par EGI Check-in, il faut s'inscrire en utilisant son compte académique/social existant.

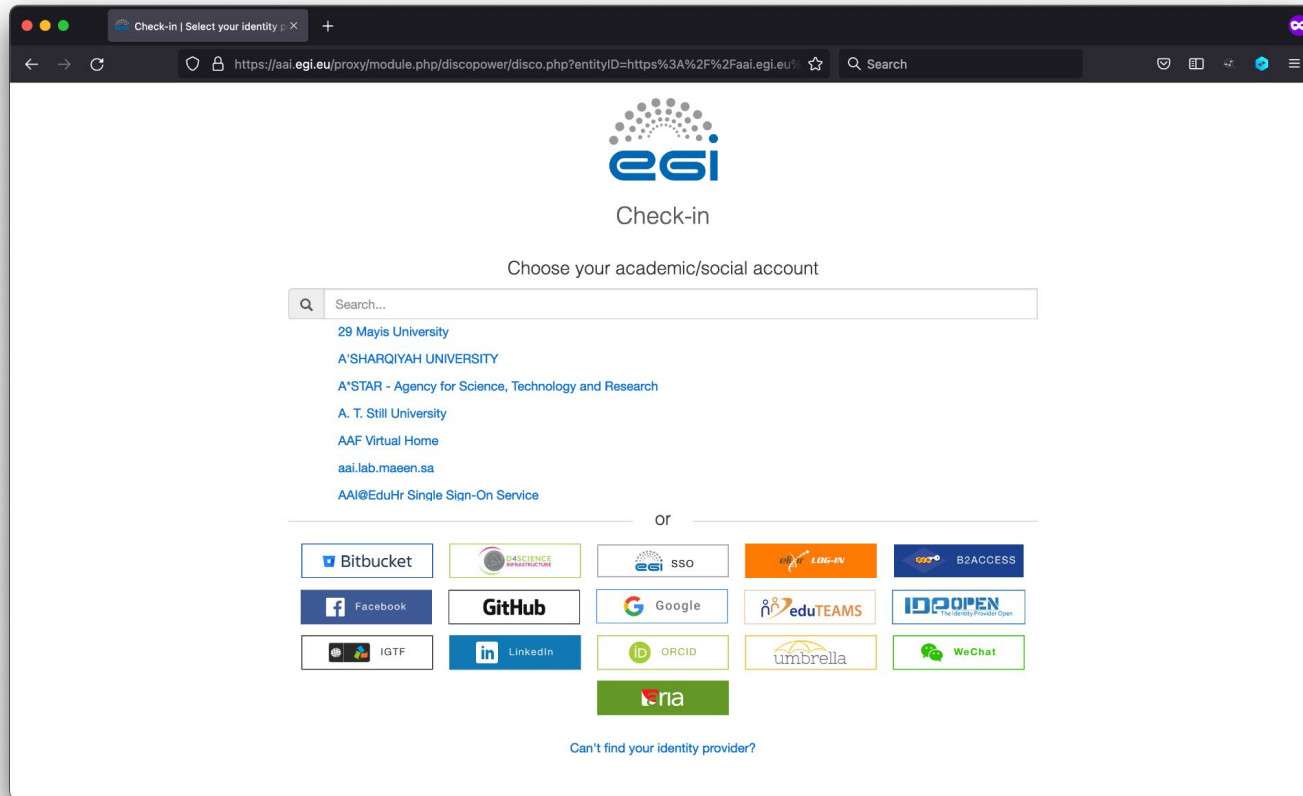
→ *Essayez-moi !*

<https://aai-demo.egi.eu/signup>



# Enregistrement | Connection

*Découverte du fournisseur d'identité*



The screenshot shows a web browser window with the URL `https://aai.egi.eu/proxy/module.php/discopower/disco.php?entityID=https%3A%2F%2Faai.egi.eu%`. The page features the EGI logo and the text "Check-in". Below this, it prompts the user to "Choose your academic/social account". A search bar is present with the text "Search...". A list of institutions is displayed, including "29 Mayis University", "A'SHARQIYAH UNIVERSITY", "A\*STAR - Agency for Science, Technology and Research", "A. T. Still University", "AAF Virtual Home", "aai.lab.maen.sa", and "AAI@EduHr Single Sign-On Service". Below the list, the word "or" is centered. A grid of identity provider logos is shown, including Bitbucket, B2ACCESS, Facebook, GitHub, Google, eduTEAMS, IDOPEN, IGTF, LinkedIn, ORCID, umbrella, WeChat, and ria. At the bottom, there is a link that says "Can't find your identity provider?".

EGI User Community

EGI ID Identifier  
fc96d5eccf1513b8fd9e08f3a93a8998a4a3c572991b6b29aef1c

Name\* Your full name  
Given Name\* Ioannis  
Family Name\* Igoumenos

Email Your current email address  
Email\* igioume@gmail.com

- ✓ Revue de l'information du profil
- ✓ Agréer les conditions d'utilisation (AUP)

EGI User Community

EGI ID Identifier  
fc96d5eccf1513b8fd9e08f3a93a8998a4a3c572991b6b29aef1c

Name\* Your full name  
Given Name\* Ioannis  
Family Name\* Igoumenos

Email Your current email address  
Email\* igioume@gmail.com

Affiliation Faculty

Organisation Organisation\*

Agree to Acceptable Use Policy and Conditions of Use (AUP)  
You must review and agree to the following AUP before continuing.

EGI AUP Terms of Use  
 Review Acceptable Use Policy  Agree

After you click Submit, we'll send you an email and you simply click on a link to confirm your email address.

\*denotes required field

Submit



Ensuite, vous devrez confirmer votre adresse électronique. Vérifiez votre boîte de réception et ouvrez le lien sur votre navigateur.

Cette étape est **PASSÉE** dans le cas d'un courriel connu pour être **vérifié** par le fournisseur d'identité.

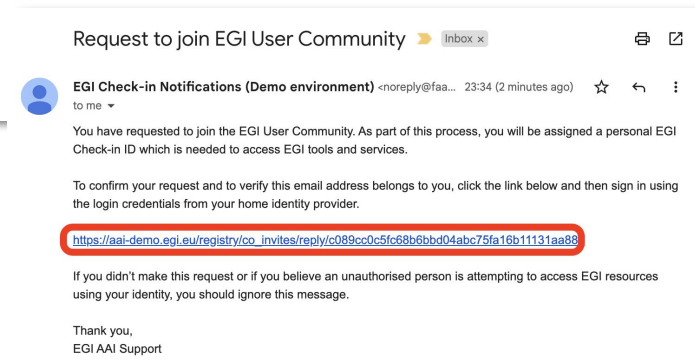


## We Sent You An Email

Just **click the link in that email** to complete your signup.

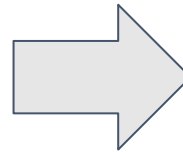
If you do not find the email in your Inbox, please check your **Spam** or **Junk** folder for an email from **EGI Check-in Notifications** > noreply@faai.grnet.gr. If you do find the email in these folders, mark the email as "safe" or "not spam" to ensure that you receive any future notifications about your EGI Check-in ID.

YOU WILL HAVE 72 HOURS TO VERIFY YOUR ACCOUNT

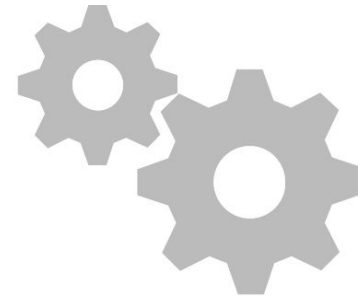




Your enrollment is being processed,  
please do not refresh or close and click  
back button on this window.



**Welcome!**



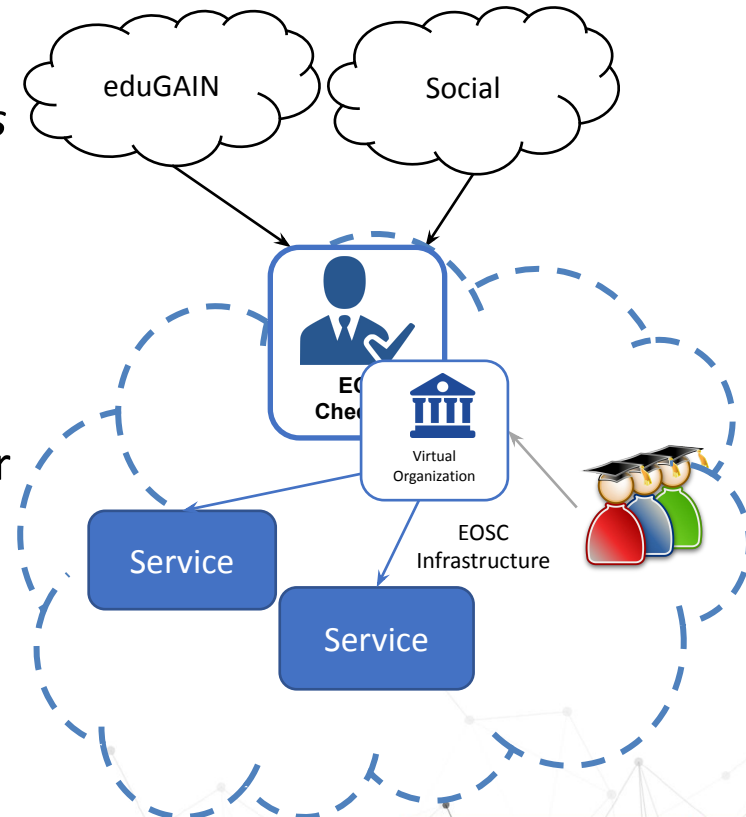
# Gestion de VO avec COmanage Registry

*Pour les communautés  
d'utilisateurs*

# Cas d'utilisation: communauté voulant une solution de gestion de groupes prête à l'emploi

*Les communautés qui n'opèrent pas leur propre service de gestion de groupe, peuvent tirer parti des capacités de la plateforme Check-in pour :*

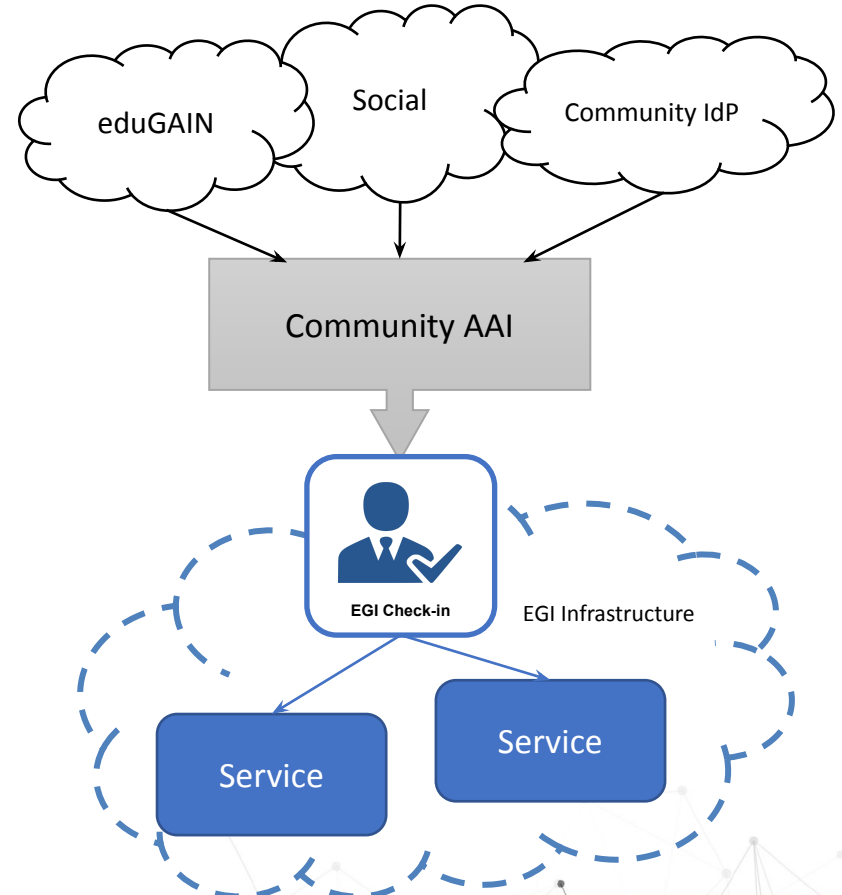
- Éviter les coûts liés au déploiement d'un service dédié
- Permettre aux administrateurs de groupe de gérer les informations relatives à leurs utilisateurs de manière indépendante.
- Permettre un accès facile et sécurisé aux ressources offertes par EGI et d'autres infrastructures (e.g. EOSC).



# Cas d'utilisation: communautés gérant son propre AAI

*L'AAI de la communauté est connecté à Check-in en tant que Proxy IdP pour permettre à ses utilisateurs d'accéder aux services et ressources d'EGI.*

- La Communauté peut accéder aux services EGI sans modifier le flux d'authentification de ses utilisateurs.

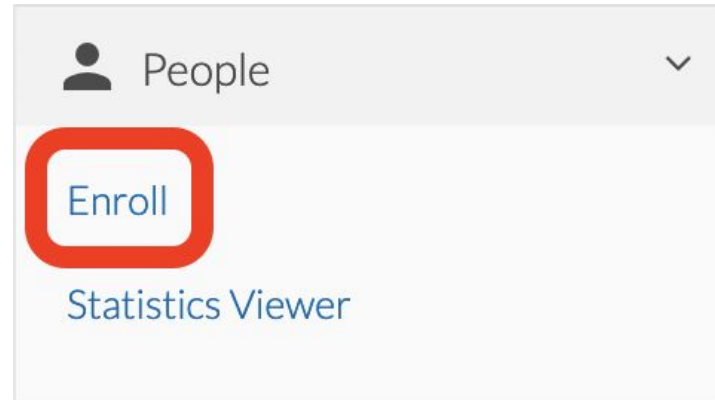


- Les groupes peuvent uniquement être créés par les administrateurs de Check-in
- Contactez [checkin-support@mailman.egi.eu](mailto:checkin-support@mailman.egi.eu) en indiquant les informations suivantes pour chaque (sous-) groupe :
  - Nom de la VO
  - Nom du groupe
  - Description du groupe
  - Optionnel: manager(s) du groupe
  - Optionnel: Nom du groupe parent (dans le cas d'un groupe hiérarchique, e.g. <VO> → <GROUPE\_PARENT> → <GROUPE>)
- *Limitation connue : Les noms de groupe doivent être uniques, il peut donc être nécessaire d'ajuster les noms pour garantir leur unicité.*

<https://docs.egi.eu/users/aai/check-in/vos/#managing-vo-groups>

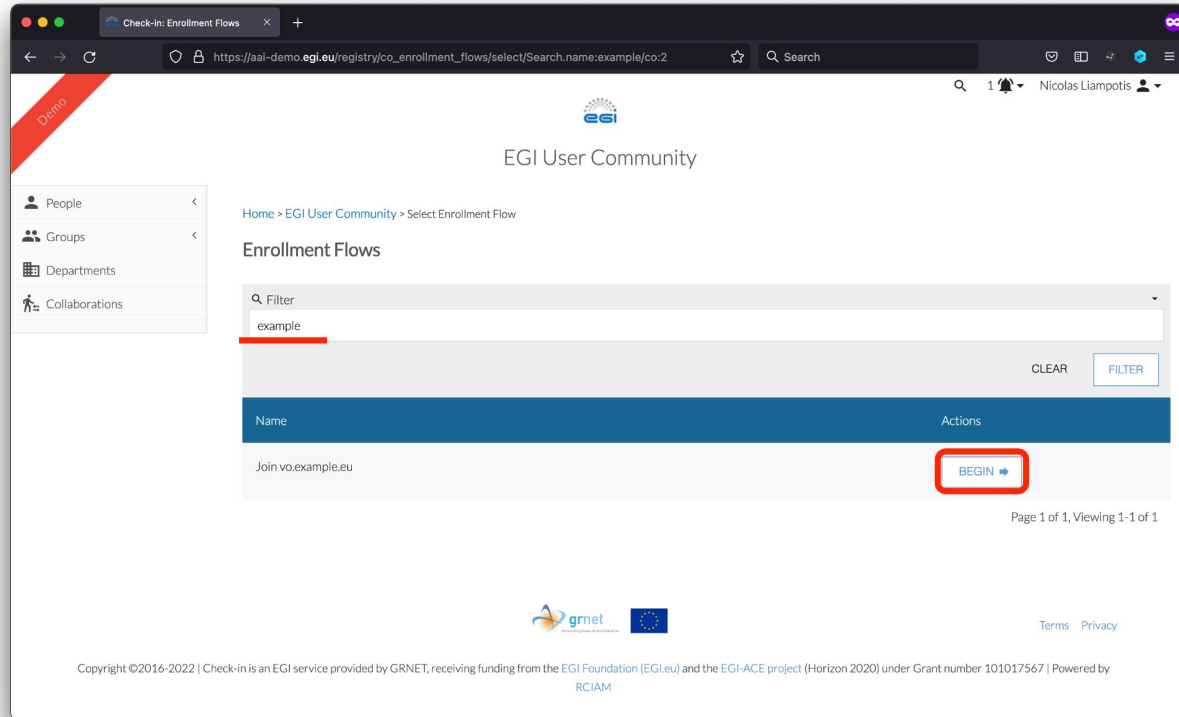
- L'utilisateur peut demander à être membre d'une VO par le biais d'**une page d'inscription**
- Chaque page d'inscription possède une **URL** unique où l'utilisateur peut se rendre pour s'inscrire à la VO souhaitée.
  - Les responsables de VO peuvent partager cette URL avec les utilisateurs, ou bien
  - Les utilisateurs peuvent cliquer sur **Enroll** dans le menu **People** et sélectionner la page appropriée.

[https://aai.egi.eu/registry/co\\_petitions/start/coef:<##>](https://aai.egi.eu/registry/co_petitions/start/coef:<##>)



# Demande d'adhésion à une VO

→ *Essayer moi !*



The screenshot shows a web browser window with the URL `https://aai-demo.egi.eu/registry/co_enrollment_flows/select/Search.name:example/co:2`. The page title is "EGI User Community". A navigation menu on the left includes "People", "Groups", "Departments", and "Collaborations". The main content area is titled "Enrollment Flows" and contains a search filter with the text "example". Below the filter is a table with one row: "Join vo.example.eu". The "Actions" column for this row contains a "BEGIN" button with a right-pointing arrow, which is highlighted by a red rectangular box. The page footer includes logos for GRNET and the European Union, along with copyright information: "Copyright ©2016-2022 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EGI-ACE project (Horizon 2020) under Grant number 101017567 | Powered by RCIAM".

[https://aai-demo.egi.eu/registry/co\\_petitions/start/coef:45](https://aai-demo.egi.eu/registry/co_petitions/start/coef:45)

# Gérer les adhésions à la VO

## Examen des demandes d'adhésion à la VO

View Petition for [redacted]

### Petition

Status Pending Approval

APPROVE

DENY

Optional

*If provided and the message template suitably configured, this comment will be made available to the enrollee. Use the "Add Comment" option instead for privileged comments that should not be visible to the enrollee.*

Enrollment Flow Join vo.example.org VO

Enrollment Flow Next Step waitForApproval

Le gestionnaire de VO peut justifier l'approbation ou le refus de la demande.

La page de révision de la demande fournit des informations sur le niveau de confiance sur les informations de l'utilisateur.

### Attached Identities

CO Person

CO Person Role

43928

Organizational Identity

Organizational Identity Source  
Records

### Assurance

Organizational Identity  
(<https://janus.cnrs.fr/idp>)

[https://aai.egi.eu/LoA#Substantial \(profile\)](https://aai.egi.eu/LoA#Substantial)



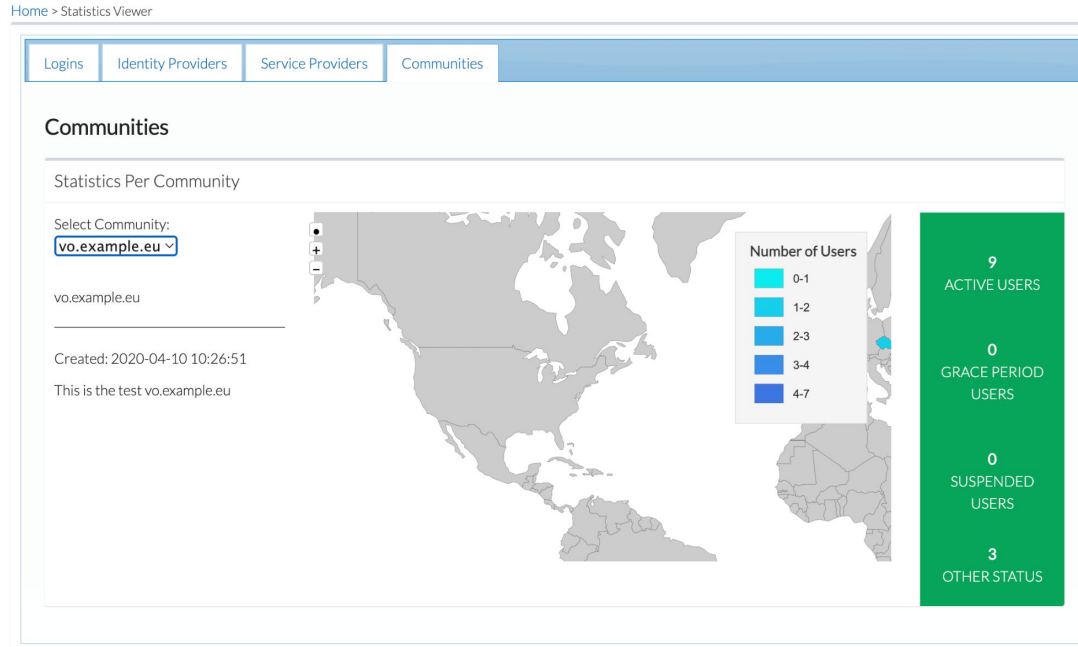
COMANAGE fournit une API REST qui permet de :

- Gérer les informations sur les membres uniquement pour les VO pour lesquels ils ont autorité.
- Récupérer des informations sur les groupes de VO uniquement pour les VO pour lesquels ils ont autorité. Un accès LDAP en lecture seule est aussi disponible.

Caractéristiques :

- Les membres du VO sont identifiés via leur identifiant d'utilisateur EGI Check-in (CUID).
- L'adhésion peut être limitée à une période donnée
- Toutes les affiliations REFEDS sont prises en charge
- Les rôles sont pris en charge
- Différentes valeurs de statut d'adhésion sont prises en charge, à savoir Actif, Expiré, Supprimé, Suspendu.
- L'enregistrement modifie automatiquement le statut de l'affiliation d'Actif à Expiré au-delà de la période de validité.

## Accessible depuis **People** → **Statistics Viewer**



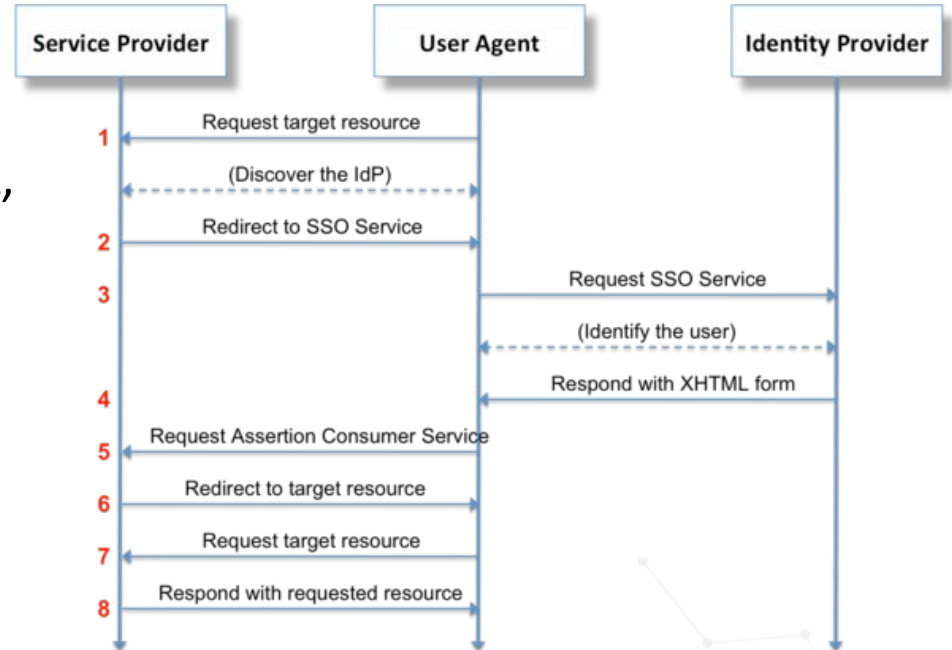
# Intégration d'un service avec Check-in

*Pour les fournisseurs de services*

EGI Check-in peut sécuriser l'accès aux services en utilisant différents protocoles :

- OAuth 2.0 / OpenID Connect (OIDC)
- SAML (Security Assertion Markup Language)
- Certificats X.509

Le langage SAML (Security Assertion Markup Language) est un format de données standard ouvert, basé sur XML, permettant d'échanger des données d'authentification et d'autorisation entre parties, en particulier entre un fournisseur d'identité et un fournisseur de services.





## Comment contrôler l'accès des utilisateurs à un service connecté à Check-in ?

## 1. Autorisation basée sur des attributs

- Informations sur les membres et les rôles des VO/Groupes
- Rôles GOCDDB
- Information sur la confiance
- Affiliation à l'organisation d'origine

## 2. Autorisation basée sur les capacités

- Ressources auxquelles un utilisateur est autorisé à accéder
- Liste facultative d'actions spécifiques que l'utilisateur est autorisé à effectuer



# Autorisation basée sur les attributs

*Informations sur les groupes et les rôles*

- Permet aux services de contrôler l'accès aux ressources sur la base d'informations sur les VO/groupes dont un utilisateur est membre.
- Une ou plusieurs valeurs encapsulées dans l'attribut :
  - `eduPersonEntitlement` (SAML attribute)
  - `eduperson_entitlement` (OIDC claim)
- Chaque valeur est formatée comme un URN → [AARC-G002](#)

```
<NAMESPACE>:group:<VO>[:<GROUP>*][:role=<ROLE>]#<GROUP-AUTHORITY>
```

# Autorisation basée sur les attributs

*Informations sur les groupes et les rôles*

- Example:



- Les capacités peuvent être utilisées pour transmettre des informations d'autorisation aux services sous une *forme compacte*.
- Une ou plusieurs valeurs encapsulées dans l'attribut :
  - eduPersonEntitlement attribute (SAML)
  - eduperson\_entitlement claim (OIDC)
- URN syntax → [AARC-G027](#)

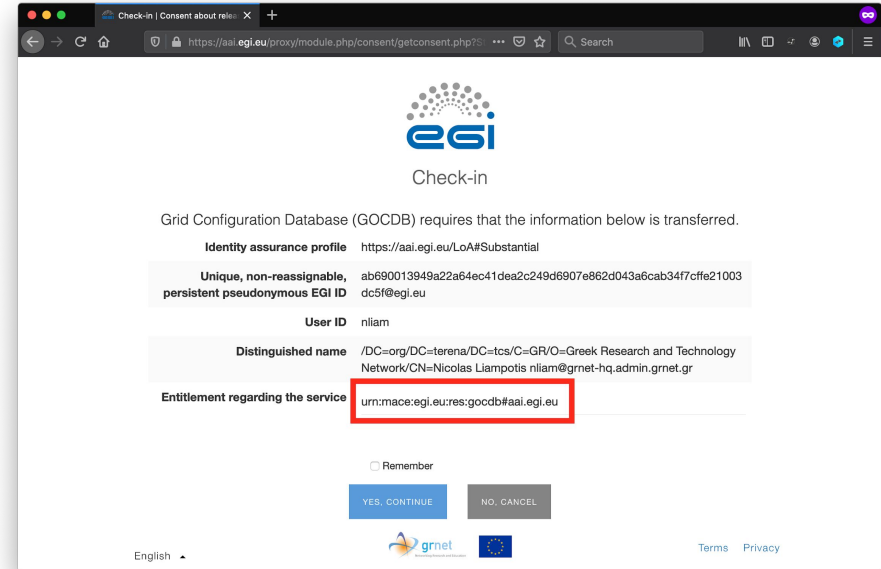
```
<NAMESPACE>:res:<RESOURCE>[:<CHILD-RESOURCE>]...
[:act:<ACTION>[,<ACTION>]...]#<AUTHORITY>
```

- Example:

`urn:mace:egi.eu:res:gocdb#aai.egi.eu`

NAMESPACE

RESOURCE AUTHORITY



Check-in | Consent about relin... X +

https://aai.egi.eu/proxy/module.php/consent/getconsent.php?...



**egi**  
Check-in

Grid Configuration Database (GOCDB) requires that the information below is transferred.

<b>Identity assurance profile</b>	https://aai.egi.eu/LoA#Substantial
<b>Unique, non-reassignable, persistent pseudonymous EGI ID</b>	ab690013949a22a64ec41dea2c249d6907e862d043a6cab347cfe21003dc5f@egi.eu
<b>User ID</b>	nliam
<b>Distinguished name</b>	/DC=org/DC=terena/DC=tcs/C=GR/O=Greek Research and Technology Network/CN=Nicolas Liampotis nliam@gnet-hq.admin.gnet.gr
<b>Entitlement regarding the service</b>	urn:mace:egi.eu:res:gocdb#aai.egi.eu

Remember

YES, CONTINUE NO, CANCEL

English   Terms Privacy

En fonction de la méthode d'authentification sélectionnée par l'utilisateur, EGI Check-in Proxy attribue un niveau d'assurance/confiance (LoA).

EGI Check-in distingue actuellement trois niveaux de LoA, de manière similaire à l'eID Assurance Framework (eIDAF). Chaque niveau est représenté par un URI comme suit :

- **Low:** Authentification par le biais d'un fournisseur d'identité sociale ou d'un autre fournisseur à faible assurance d'identité :  
<https://aai.egi.eu/LoA#Low>
- **Substantial:** Mot de passe /X.509 à l'IDP de l'organisation de l'utilisateur:  
<https://aai.egi.eu/LoA#Substantial>
- **High:** Substantial + authentification multi-facteurs (pas encore supporté):  
<https://aai.egi.eu/LoA#High>

# Assurance/confiance: Qu'est ce que c'est ?

## REFEDS Assurance Composants & Profils

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

**AARC Assam**  
**IGTF Dogwood**  
**RAF Cappuccino**  
**IGTF Birch**  
**RAF Espresso**

**Nouveaux profils!**

# Connecter votre Service à EGI Check-in

Pour intégrer votre service, suivez le [Guide d'intégration pour les fournisseurs de services](#). Vous devez soumettre une demande par le biais du [Federation Registry](#).

L'intégration suit un processus en deux étapes :

**Étape 1.** Enregistrez votre service et testez l'intégration technique avec l'instance de **démonstration**, et préparez la validation non technique (politique de protection des données,...). Vous pouvez tester les nouvelles fonctionnalités qui ne sont pas encore en production, en testant l'intégration avec l'instance de **développement**.

**Étape 2.** Enregistrez votre fournisseur de services auprès de l'instance de **Production** de EGI Check-in pour permettre aux membres de la communauté d'utilisateurs EGI d'accéder à votre service.

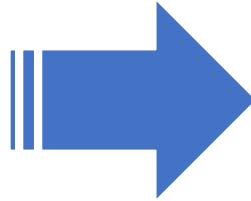


# Connecter votre Service à EGI Check-in

## Environnements d'intégration

### DEMO

- Pour les services prêts pour la production
- Prend en charge toutes les options de connexion académiques et sociales
- L'enregistrement / la reconfiguration des services nécessite l'approbation des opérateurs :
  - Examen des paramètres techniques



### PRODUCTION

- Utilisé pour les services en production
- Prend en charge toutes les options de connexion académiques et sociales
- Enregistrement et reconfiguration du service nécessite une approbation :
  - Examen des paramètres techniques
  - Examen des aspects "politiques"

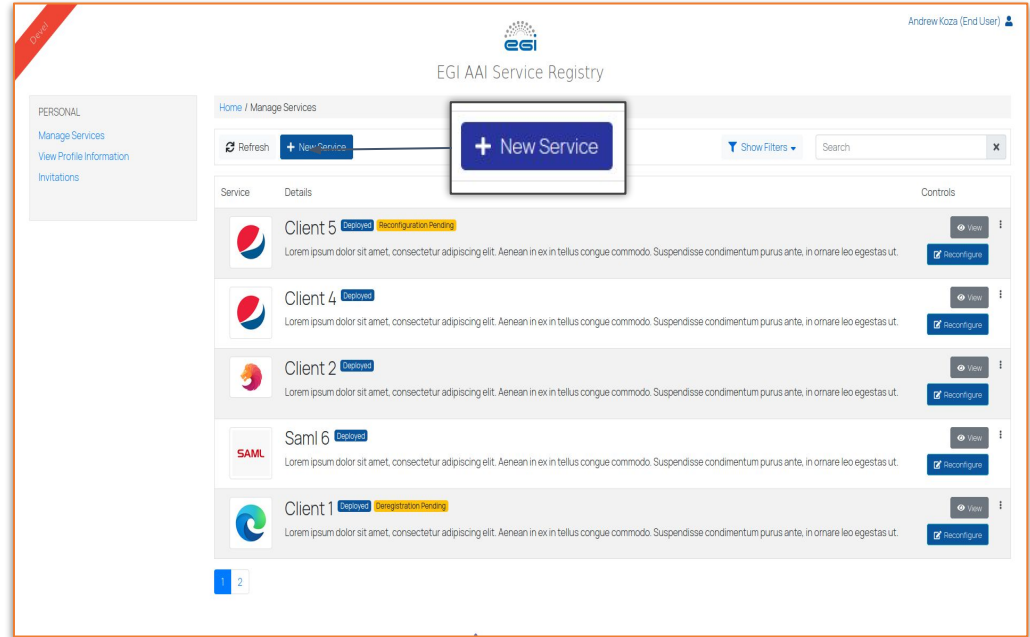
### DEVELOPMENT

- Utilisé pour tester des fonctionnalités expérimentales
- Options de connexion limitées
- Enregistrement et reconfiguration des services auto-approuvés par les propriétaires des services.

# Connecter votre Service à EGI Check-in

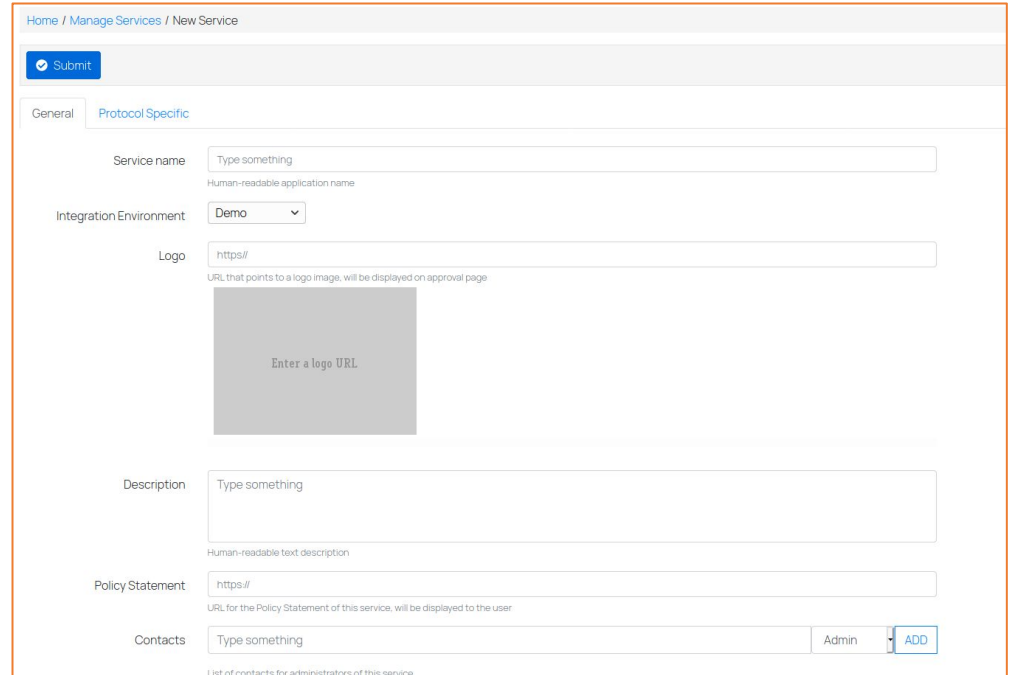
## Directives générales

1. Connectez vous sur <https://aai.egi.eu/federation>
2. Dans le tableau de bord "Manage services", cliquez sur "New Service".



The screenshot shows the EGI AAI Service Registry interface. At the top right, the user is identified as Andrew Kozsa (End User). The main heading is "EGI AAI Service Registry". Below this, there is a navigation menu on the left with options: PERSONAL, Manage Services, View Profile Information, and Invitations. The main content area is titled "Home / Manage Services" and features a "Refresh" button, a "+ New Services" button, and a prominent "+ New Service" button highlighted with a red box. Below the navigation, there is a table of services with columns for Service, Details, and Controls. The table lists several services: Client 5 (Deployed, Configuration Pending), Client 4 (Deployed), Client 2 (Deployed), SAML 6 (Deployed), and Client 1 (Deployed, Registration Pending). Each service entry includes a status indicator, a description, and control buttons for "View" and "Reconfigure".

3. Dans l'onglet "**General**", remplissez les informations requises sur votre service. Sélectionnez également "**Demo**" comme "**Integration Environment**".
4. Dans l'onglet "Protocol Specific", configurez les options du service (informations à suivre).
5. Soumettez la demande
6. Attendez la revue




Home / Manage Services / New Service

General **Protocol Specific**

Service name   
Human-readable application name

Integration Environment

Logo   
URL that points to a logo image, will be displayed on approval page

  
Enter a logo URL

Description   
Human-readable text description

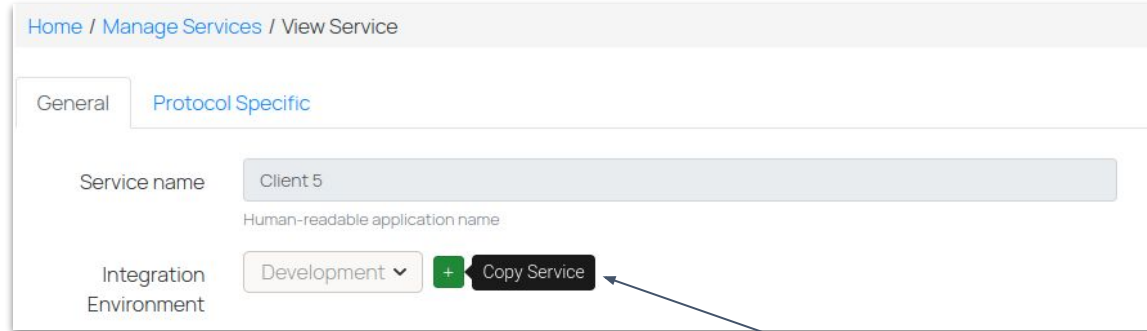
Policy Statement   
URL for the Policy Statement of this service, will be displayed to the user

Contacts     
List of contacts for administrators of this service

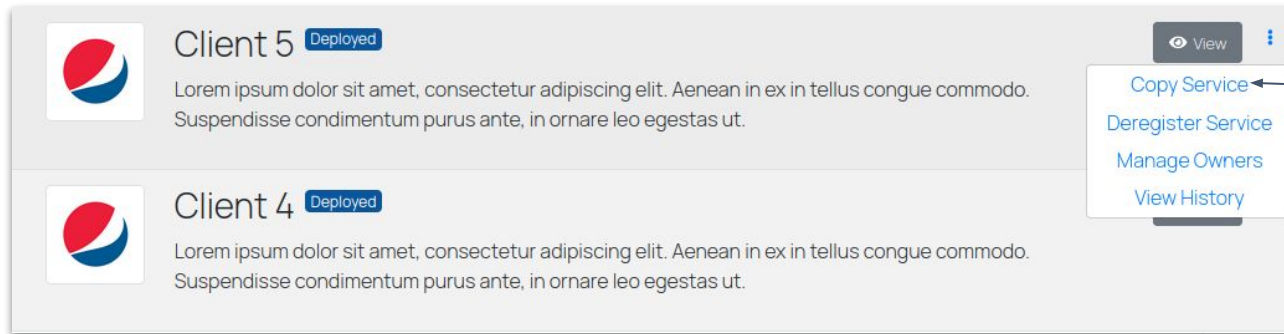
# Connecter votre Service à EGI Check-in

## Directives générales

Complétez les tests dans l'environnement **Demo** ⇒ Passer la configuration du client en **production**



Lors de l'affichage du service



Plus d'options sont disponibles dans le menu

# Certificats X.509

# Qu'est ce que X.509

X.509 est un format standard pour les certificats de clé publique, des documents numériques qui associent de manière sécurisée des paires de clés cryptographiques à des identités telles que des sites web, des personnes ou des organisations.

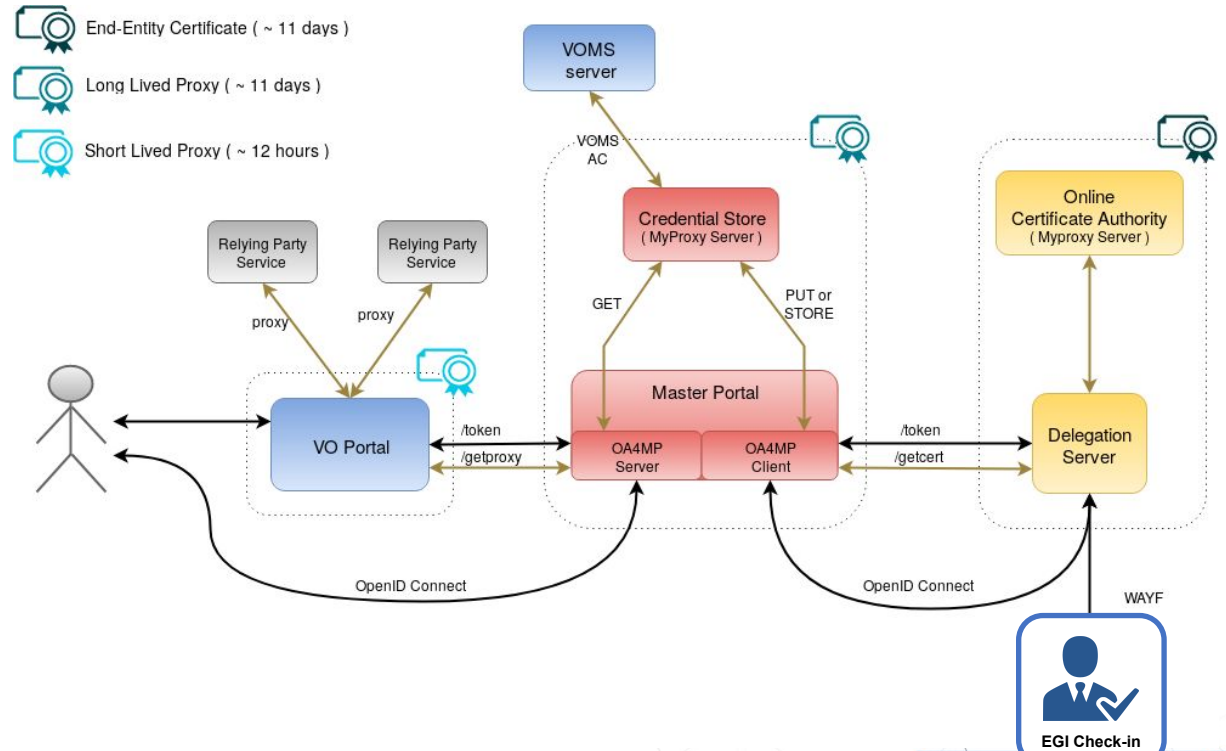
<b>Subject Name</b>	_____
	org
	terena
	tcs
<b>Country</b>	GR
<b>Organization</b>	Greek Research and Technology Network
<b>Common Name</b>	Nikolaos Evangelou nikosev@grnet-hq.admin.grnet.gr
<b>Issuer Name</b>	_____
<b>Country</b>	NL
<b>State/Province</b>	Noord-Holland
<b>Locality</b>	Amsterdam
<b>Organization</b>	TERENA
<b>Common Name</b>	TERENA eScience Personal CA 3

# X.509 pour le non web et l'accès délégué

*Certificats fournis par RAuth.eu Online CA*

Check-in a été intégré à l'AC en ligne RAuth.eu pour permettre aux utilisateurs de récupérer des certificats proxy X.509 en utilisant leurs informations d'identification fédérées.

- Master Portal récupère le certificat d'entité finale de RAuth.eu
- Certificat proxy à longue durée de vie stocké dans un serveur MyProxy
- Proxies à courte durée de vie fournis via :
  - Science Gateways via OIDC ( VO-portals)
  - utilisateurs via SSH key

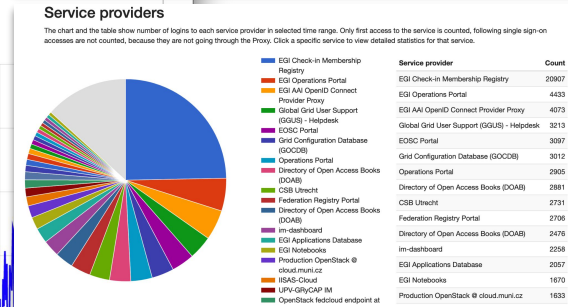
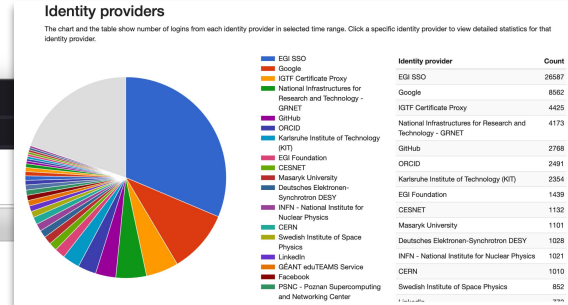
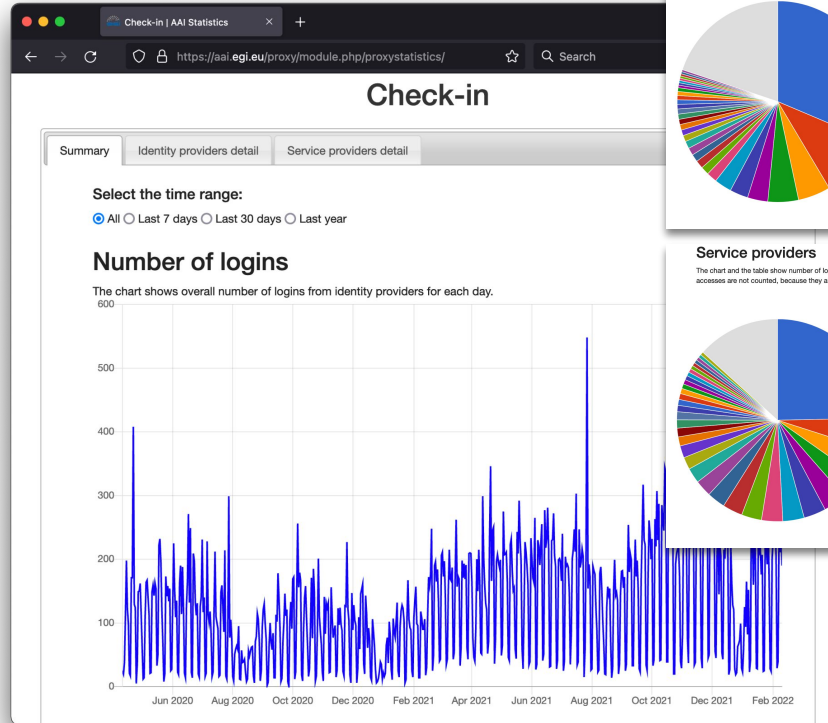


# Collection de statistiques d'utilisation



## Statistiques publiques

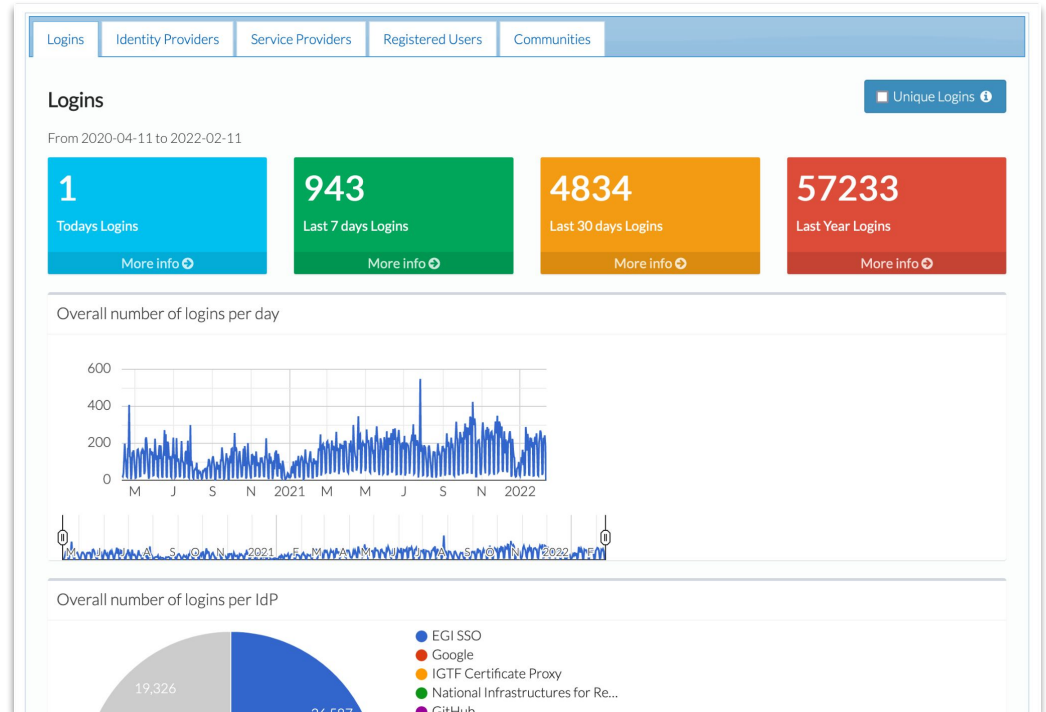
- Logins
  - total
  - par Identity Provider
  - par Service Provider



<https://aai.egi.eu/proxy/statistics>

## Plugin pour des statistiques avancées

- Logins / Unique logins
  - total
  - par Identity Provider
  - par Service Provider
  - par Pays
- Utilisateurs enregistrés
- Communautés/Virtual Organisations



<https://aai.egi.eu/registry>



What's  
Next?

- Nouvelle technologie
  - Keycloak
- Expérience utilisateur améliorée
  - Liaison d'identité implicite
  - IdP discovery (hinting)
- Authentification plus forte
  - Authentification Deux Facteurs (OTP)
  - Authentification sans mot de passe (Webauthn)
- Nouveaux fournisseurs d'authentification
  - eIDAS

- [Guide d'utilisation](#)
- [Guide d'intégration pour les fournisseurs de services](#)
- [Guide d'intégration pour les fournisseurs d'identités](#)
- Nous contacter: [check-in@egi.eu](mailto:check-in@egi.eu) , [operations@egi.eu](mailto:operations@egi.eu), [support@egi.eu](mailto:support@egi.eu)
- Me contacter: [baptiste.grenier@egi.eu](mailto:baptiste.grenier@egi.eu)

# EGI: Advanced Computing for Research



[www.egi.eu](http://www.egi.eu)



@EGI\_eInfra

Thank you  
for your attention.

*Questions?*



**This work by the EGI Foundation**  
is licensed under a Creative Commons  
Attribution 4.0 International License.

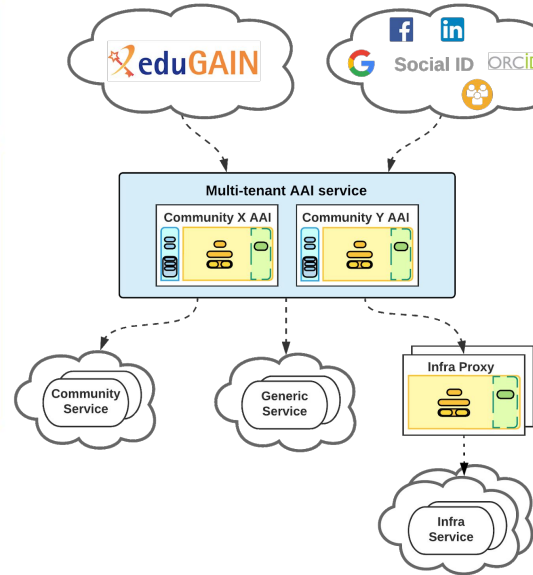
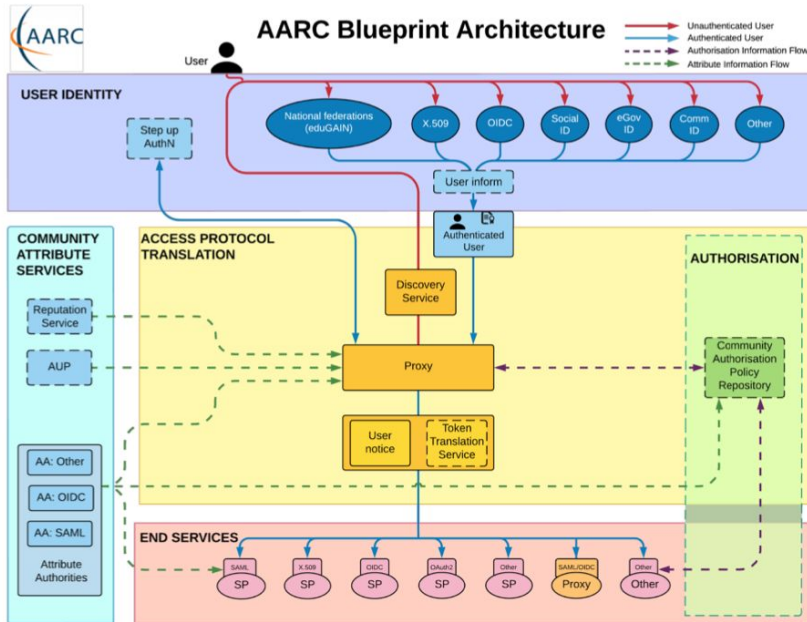


**The work of the EGI Foundation**  
is partly funded by the European Commission  
under H2020 Framework Programme

**Backup slides, if you don't have enough**

# AARC Blueprint Architecture

Basic components: Community AAI and Infrastructure Proxy



## Community AAI

The purpose of the Community AAI is to streamline researchers' access to services, both those provided by their own infrastructure as well as the services provided by infrastructures that are shared with other communities.

## Infrastructure Proxy

The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant policies and business logic for making available these resources to multiple communities

# Federation Registry

- A service is owned by a group of users called **owners group**
- Users in an owners group can take one of two roles:
  - **Member**
  - **Manager**
- Both **Members & Managers** can view and create reconfiguration requests for that service.
- **Managers** have control over group members, and can invite or remove users

### Group Members

Username	Email	Group Manager
akoza	<a href="mailto:koza-sparrow@hotmail.com">koza-sparrow@hotmail.com</a>	✔

### Group Invites


Username	User Email	Manager	Sent to	Invitation Date	Action
Not linked to account		<a href="mailto:andreaskoza@admin.grnet.gr">andreaskoza@admin.grnet.gr</a>		2021-04-23	✖ ↺

Invitation was sent successfully to: [andreaskoza@admin.grnet.gr](mailto:andreaskoza@admin.grnet.gr)

### Send Invites

Member

Dev
Federation Registry Portal Deployed
View



This is for the federation registry

- [Copy Service](#)
- [Deregister Service](#)
- [Manage Owners](#)
- [View History](#)

[Manage Owners](#)



# My Service supports SAML, what should I do?

**Use case:** Federated access to a web-based application (e.g. portal, wiki)

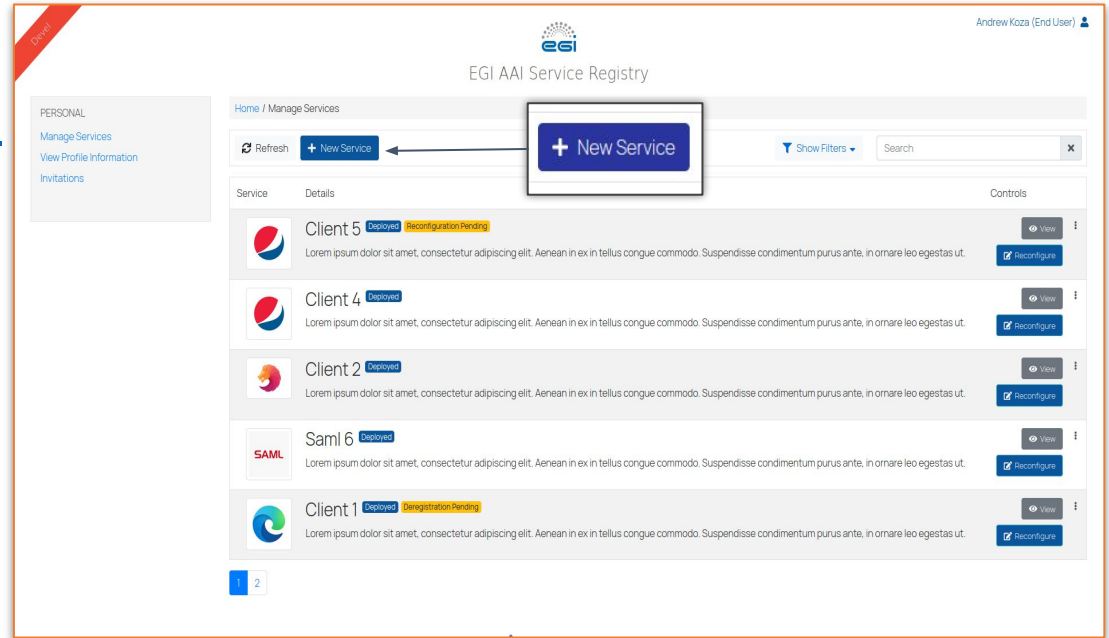
- Connect to EGI Check-in IdP as a SAML Service Provider (SP)
- Once the user is authenticated, the EGI Check-in Proxy will return a SAML assertion to the application containing information about the authenticated user

- SAML authentication relies on the use of metadata
- Both parties (you as a SP and the EGI Check-in IdP) need to exchange metadata in order to know and trust each other
- Metadata include information such as the location of the service endpoints, certificates for signing/encrypting SAML messages
- It is important that you serve your metadata over HTTPS using a browser-friendly SSL certificate, i.e. issued by a trusted certificate authority

Your SAML SP needs to add the EGI Check-in SAML IdP metadata:

- Demo: <https://aai-demo.egi.eu/proxy/saml2/idp/metadata.php>
- Production: <https://aai.egi.eu/proxy/saml2/idp/metadata.php>

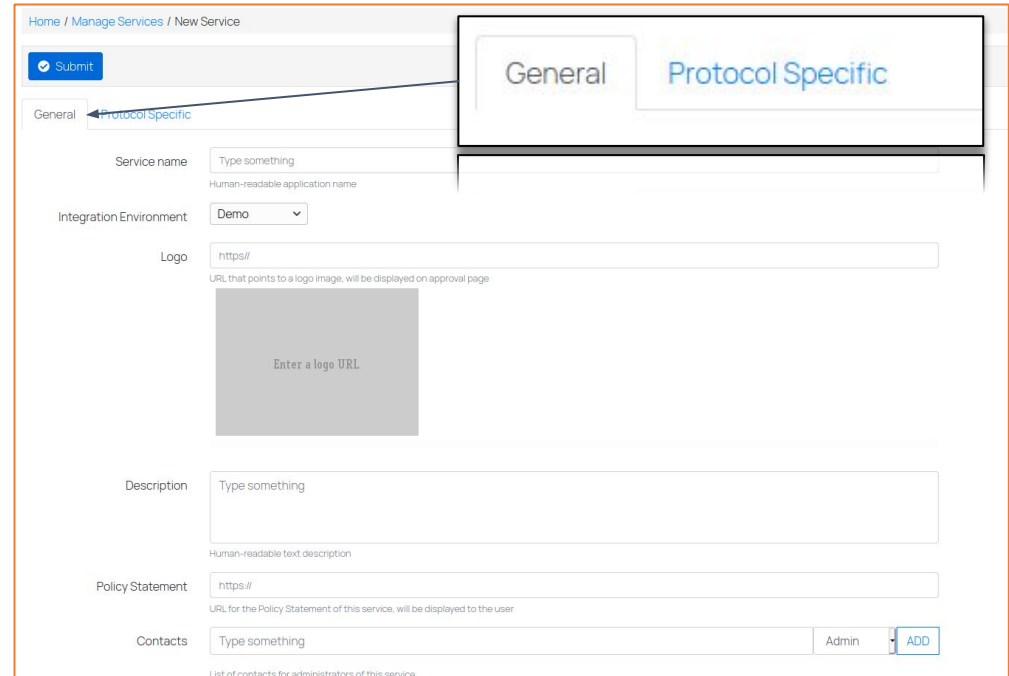
1. Log into <https://aai.egi.eu/federation>
2. In the “Manage Services” dashboard click on “New Service”



# Connect SAML Service

## General information

3. In the “General” tab fill the required information about your Service. Also, select “Demo” as “Integration Environment”.



Home / Manage Services / New Service

Submit

General Protocol Specific

Service name   
Human-readable application name

Integration Environment

Logo   
URL that points to a logo image, will be displayed on approval page

Enter a logo URL

Description   
Human-readable text description

Policy Statement   
URL for the Policy Statement of this service, will be displayed to the user

Contacts  Admin

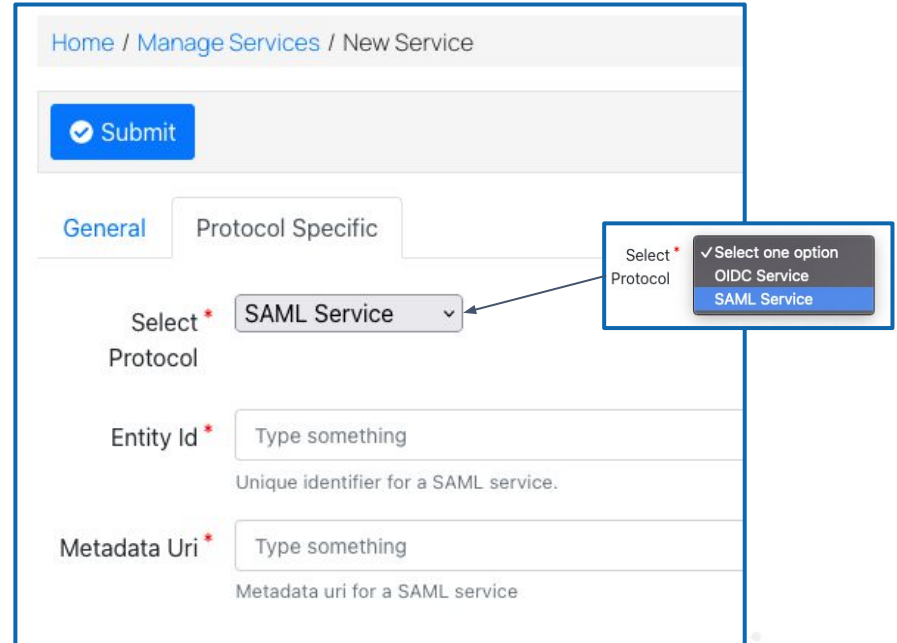
List of contacts for administrators of this service

# Connect SAML Service

*Protocol-specific information*

4. In the “Protocol Specific” tab, select “SAML” as “Protocol” and fill the “EntityID” and “Metadata URL”

5. Click “Submit”



Home / Manage Services / New Service

Submit

General Protocol Specific

Select \* Protocol SAML Service

Entity Id \* Type something  
Unique identifier for a SAML service.

Metadata Uri \* Type something  
Metadata uri for a SAML service

Select \*  
Select one option  
OIDC Service  
SAML Service

# My Service supports OpenID Connect, what should I do?

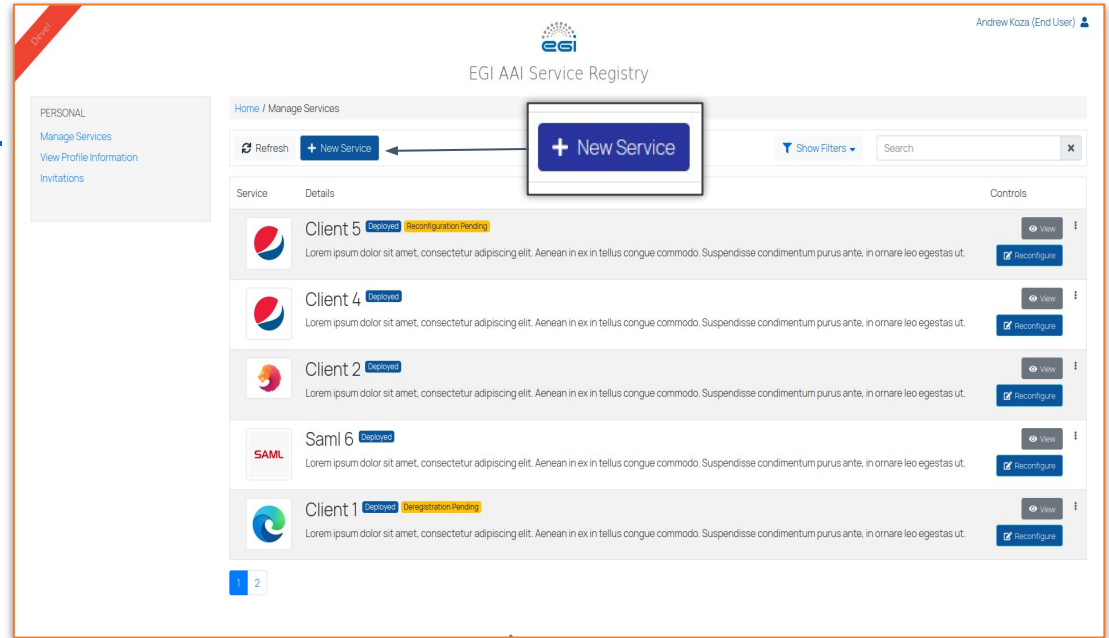
## Use case: Protecting access to

- Web-based application (e.g. portal, wiki)
- Non-web-based resources (e.g. API, CLI)
  - also when the user is not present (offline access)

You need OAuth 2.0 credentials (e.g. client ID and client secret) to authenticate users through the EGI Check-in OIDC Provider.



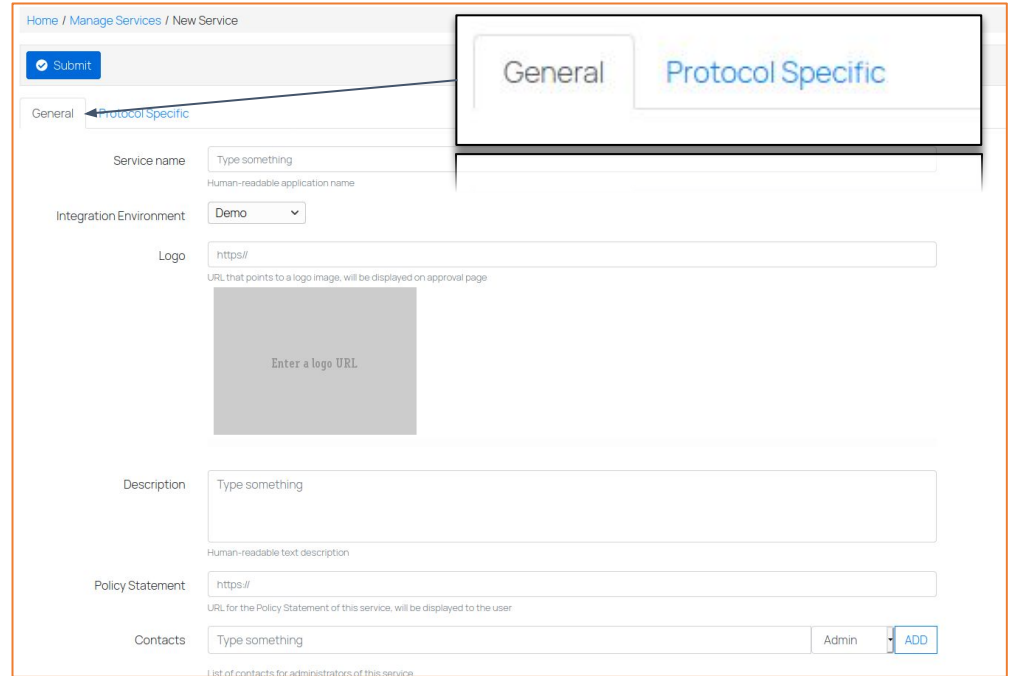
1. Log into <https://aai.egi.eu/federation>
2. In the “Manage Services” dashboard click on “New Service”



# Connect OIDC Service

## General information

3. In the “General” tab fill the required information about your Service. Also, select “Demo” as “Integration Environment”.



Home / Manage Services / New Service

Submit

General Protocol Specific

Service name   
Human-readable application name

Integration Environment

Logo   
URL that points to a logo image, will be displayed on approval page

Description   
Human-readable text description

Policy Statement   
URL for the Policy Statement of this service, will be displayed to the user

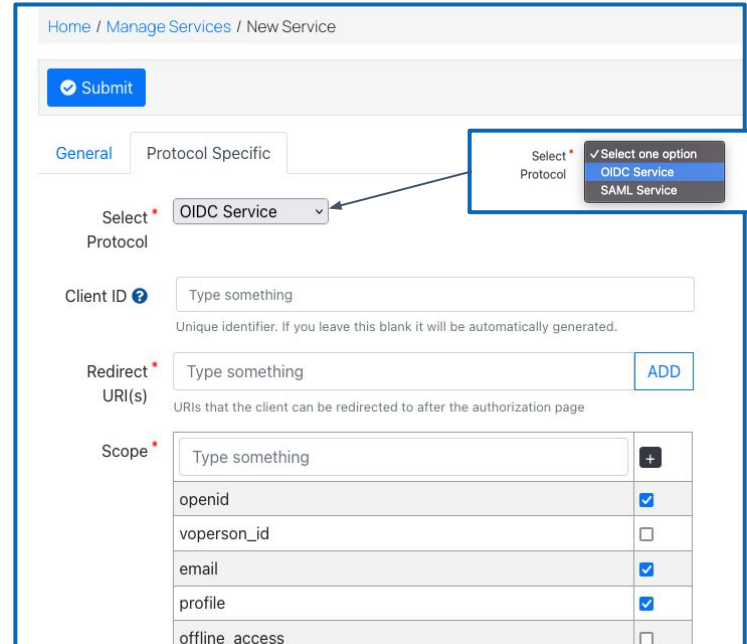
Contacts  Admin

List of contacts for administrators of this service

# Connect OIDC Service

## General information

4. In the “Protocol Specific” tab, select “OIDC” as “Protocol” and modify the Service configuration:
  - Redirect URIs
  - Scopes
  - Client authentication method
  - Grant
5. Click “Submit”



Home / Manage Services / New Service

General Protocol Specific

Select \* Protocol  √ Select one option  
OIDC Service  
SAML Service

Client ID   
Unique identifier. If you leave this blank it will be automatically generated.

Redirect \* URI(s)    
URIs that the client can be redirected to after the authorization page

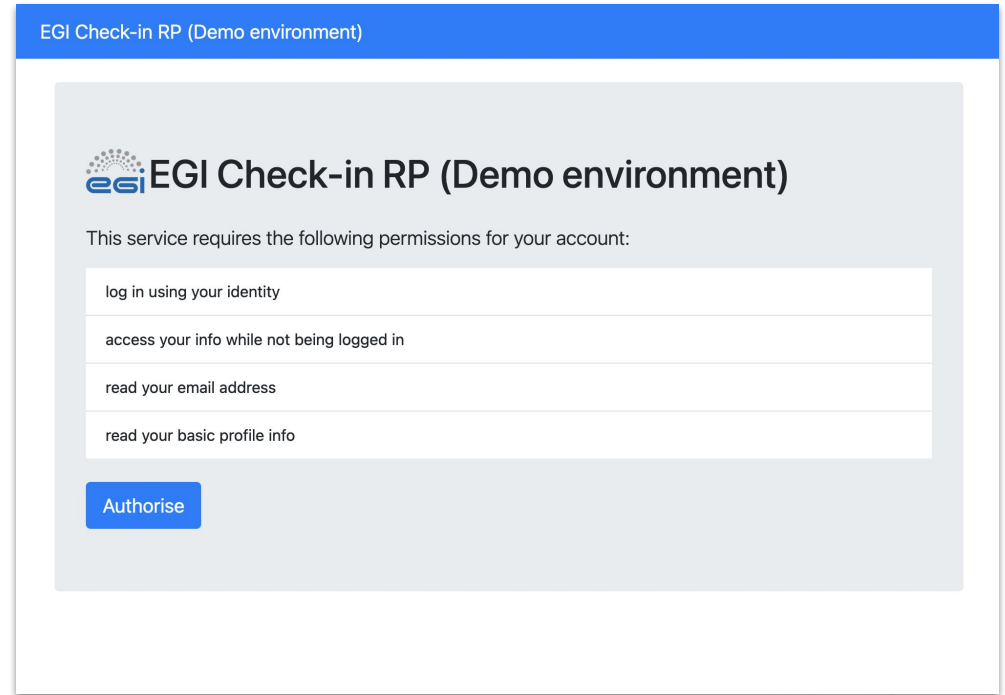
Scope  

openid	<input checked="" type="checkbox"/>
voperson_id	<input type="checkbox"/>
email	<input checked="" type="checkbox"/>
profile	<input checked="" type="checkbox"/>
offline_access	<input type="checkbox"/>

# AuthN/AuthZ Flows

1. User clicks Login within web application
2. User is redirected to the Check-in (OIDC /authorize endpoint).
3. Check-in redirects the user to the Identity Provider Discovery page
4. User authenticates using academic/social login options and may see a consent page listing the permissions Check-in will give to the web application
5. Check-in redirects the user back to the application with an authorization code (can be used only once)
6. Web application sends this code to Check-in (OIDC /token endpoint) along with the application's Client credentials (ID and Secret)
7. Check-in verifies the code and Client credentials
8. Check-in responds with an **ID Token** and **Access Token** (and optionally, a **Refresh Token**)

User logs into OIDC web application


A screenshot of a web application interface for an authorization code flow. The page has a blue header bar with the text 'EGI Check-in RP (Demo environment)'. Below the header, the main content area has a light gray background. At the top of this area is the ESI logo followed by the text 'EGI Check-in RP (Demo environment)'. Below this, it says 'This service requires the following permissions for your account:'. There is a white box containing four lines of text: 'log in using your identity', 'access your info while not being logged in', 'read your email address', and 'read your basic profile info'. At the bottom left of this white box is a blue button with the text 'Authorise'.

# Authorization Code Flow


Users chooses academic/social identity

The screenshot displays the EGI Check-in Demo Service interface. At the top, the EGI logo and 'Check-in' text are visible. Below this, a search bar prompts the user to 'Choose your academic/social account'. A list of search results includes 'A'SHARQIYAH UNIVERSITY', 'A\*STAR - Agency for Science, Technology and Research', 'A. T. Still University', 'AAF Virtual Home', 'aal.lab.maeen.sa', and 'AAI@EduHr Single Sign-On Service'. Below the search results, there is an 'OR' separator and a grid of social and academic identity provider logos, including na, Bitbucket, EGI SSO, LOG-IN, Facebook, GitHub, IDOPEN, IGTF, and ORCID. An orange banner at the top of the right-hand panel reads 'GRNET-HQ Identity Provider'. Below this banner, the text 'Login to EGI Check-in Demo Service' is displayed. The login form contains fields for 'Username' (with the value 'nikosev') and 'Password' (masked with dots). There are two checkboxes: 'Don't Remember Login' and 'Clear prior granting of permission for release of your information to this service.'. A blue 'Login' button is positioned below the form. At the bottom of the panel, the EGI logo and 'EGI Check-in Demo Service' text are repeated.

User consents to the release of information from the IdP to Check-in



grnet  
Networking Research and Education



ESI

You are about to access the service:  
**EGI Check-in Demo Service** of EGI Foundation

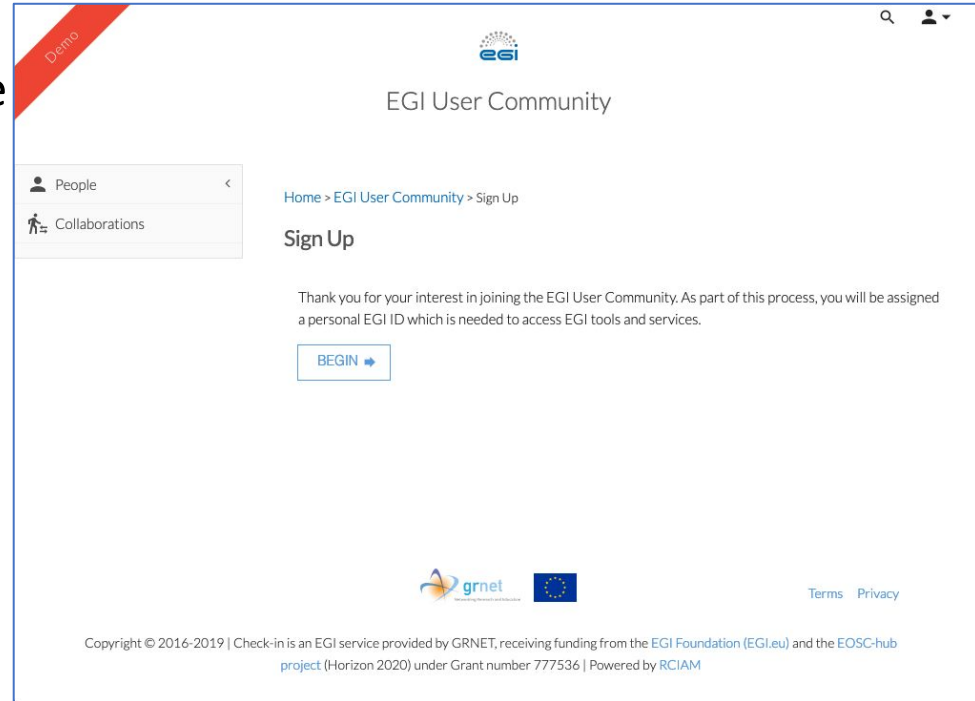
Description as provided by this service:  
*EGI Check-in Demo Service*

[Additional information about the service](#)

Information to be Provided to Service	
displayName	<b>Nikolaos Evangelou</b>
eduPersonPrincipalName	<b>nikosev@grnet-hq.admin.grnet.gr</b>
eduPersonScopedAffiliation	<b>staff@grnet-hq.admin.grnet.gr</b>
email	<b>nikosev@admin.grnet.gr</b>
givenName	<b>Nikolaos</b>
surname	<b>Evangelou</b>



If the user accesses EGI Check-in for the first time, they will need to register an account (see User Registration slides)




The screenshot shows the EGI User Community Sign Up page. A red diagonal banner in the top-left corner reads "Demo". The page header includes the EGI logo and the text "EGI User Community". A navigation menu on the left contains "People" and "Collaborations". The main content area features a breadcrumb trail "Home > EGI User Community > Sign Up", the heading "Sign Up", and a paragraph: "Thank you for your interest in joining the EGI User Community. As part of this process, you will be assigned a personal EGI ID which is needed to access EGI tools and services." Below this text is a blue "BEGIN" button with a right-pointing arrow. The footer contains logos for GRNET and the European Union, along with "Terms" and "Privacy" links. At the bottom, a copyright notice states: "Copyright © 2016-2019 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EOSC-hub project (Horizon 2020) under Grant number 777536 | Powered by RCIAM".

## User consents to the release of their information from Check-in to the OIDC Client

Demo
Check-in

Approval Required for Service "EGi Check-in OpenID Connect Relying Party (PHP Client Demo)". Please read the [Privacy Policy](#)



This service would like to:

- read your user identifier
- read your basic profile info
- read your email address
- access your info while not being logged in

Select the approval duration:

- prompt me again next time
- remember this decision for one hour
- remember this decision until I revoke it

This setting can be revoked in [Manage Approved Services](#) page.

A PHP-based OpenID Connect Relying Party used for EGI Check-in demonstration purposes

➤ [more information](#)

You will be redirected to the following page if you click Authorise:

<https://snf-666522.vm.okeanos.gnet.gr/egi-demo-rp/auth.php>

Do you authorise "EGi Check-in OpenID Connect Relying Party (PHP Client Demo)"?

AUTHORISE

DENY

OIDC Client obtains

- **ID Token**
- **Access Token**
- **Refresh Token**  
(optional if offline access is granted)

Access Token:

```
eyJraWQiOiJvaWRjliwiYWxnjoiUIMyNTYifQ.eyJzdWIiOiJiZjAwOWM4N2NiMDRmMGE2OWZ
```

Copy

To get the user info use the following curl command:

```
curl -H 'Authorization: Bearer eyJraWQiOiJvaWRjliwiYWxnjoiUIMyNTYifQ.eyJzdWIiOiJiZjAw
```

Copy

To introspect the token use the following curl command:

```
curl -u 'f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4':AMRnknUWxJ3nN9C2XzZ2NuLt-pBJf
```

Copy

NOTE: New access tokens expire in 1 hour.

Refresh Token:

```
eyJhbGciOiJub25lbn0.eyJleHAiOiE1ODk1Nzc1MzgsImp0aSI6IjUwN2ZkYjJLWM3NjltNDRINS
```

Copy

NOTE: New refresh tokens expire in 13 months.

To generate access tokens from this refresh token use the following curl command:

```
curl -X POST -u 'f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4':AMRnknUWxJ3nN9C2XzZ2N
```

Copy

NOTE: New access tokens expire in 1 hour.

You can manage your refresh tokens in the following link:

<https://aai-demo.egi.eu/oidc/manage/user/services>

# Using Access Token to obtain information from UserInfo

```
grnet@GRNETs-MacBook-Pro-2 ~ % curl -H 'Authorization: Bearer eyJraWQiOiJvaWRjIiwiaWxzIjoiUlMyNTYiLCJ0eXkiOiJ1IiwiaWF0IjoiYjZjAw0wM4N2IiwidmVudCI6ImNjOTg3Njc5NDdlnWI3NDAA4YmVkyVWVmdDlnZB1ZjMzZWY3NzczMThlNjEwQGVnaS5ldSI6ImY2OGY1ZGY0LWQxYjEtdNDRlMS1hOTNkLTRhYWI4ZjgwZTVjNCIsImZscyI6Imh0dHBzOlwvXC9hYmktZGVtb51Z2kuZlZkL29pZGNlcysImV4cCI6MTU4OTU1MjZ0cWlaWF0iJ0xNTg5NTQ4NzM4LjQdGkiOiI3ZjRmYTVkS1h0TRhLTQyMDQtYmNhZS01YmFhNmVhODA1ZHU1fQ.UK4QWwtT1rayAz21vosFJax4qkacw101FbKIaf_LKFK-V_cjLiLlM6zLhmokSZL34pdxmDjbyI0nxjt2G-Ud4YPwd6TUeqkXkJRAUpaepSF7XlD3Gqy_7uRKdZiMvFBHyV7vQ8WG3BE8xVkurdqfK3o6-Z6kg0vqL_jv8EJSRBQB_bB0N-k54E5M5nYPseDkNZ_jUkdVoFM4CB1a2sQ01v-jA2qTfSonbELAgzFVb0Lk3yQDbdEFYF2m_i-RLcLmS15Cq4swb0boCUFb1iZM1JoSH08IH0h3ysxQAd7yXlB5TYBK563C0sxcFEe_kmPVHBmPjgFE8quyIzY7nVJwQ' -H 'Content-type: application/json' https://aai-demo.egi.eu/oidc/userinfo | python -m json.tool;
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 1133 100 1133 0 0 6511 0 --:--:-- --:--:-- --:--:-- 6549
{
  "acr": "https://aai.egi.eu/LoA#Substantial",
  "eduperson_assurance": [
    "https://aai.egi.eu/LoA#Substantial"
  ],
  "eduperson_entitlement": [
    "urn:mace:egi.eu:group:registry:test-group:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:services.aai.egi.eu:members:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:demo.fedcloud.egi.eu:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:demo.fedcloud.egi.eu:members:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:service-integration.aai.egi.eu:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:training.egi.eu:role=vm_operator#aai.egi.eu",
    "urn:mace:egi.eu:group:registry:test-group:role=owner#aai.egi.eu",
    "urn:mace:egi.eu:group:services.aai.egi.eu:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:training.egi.eu:role=member#aai.egi.eu",
    "urn:mace:egi.eu:group:service-integration.aai.egi.eu:role=vm_operator#aai.egi.eu"
  ],
  "eduperson_scoped_affiliation": [
    "member@grnet-hq.admin.grnet.gr"
  ],
  "email": "nikosev@admin.grnet.gr",
  "family_name": "Evangelou",
  "given_name": "Nikolaos",
  "name": "Nikolaos Evangelou",
  "preferred_username": "nevangelou",
  "sub": "bf009c87cb04f0a69fb2cc98767147e5b7408bedae07b70ef33ef777318e610@egi.eu"
}
```





```
grnet@GRNETs-MacBook-Pro-2 ➜ curl -X POST -u 'f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4': 'AMRnkxnUWxJ3nN9C2XzZ2NuLt-pBJRr3eJRB|
F9jfkOrUH2Zmb7Nzqwh4k58YR0meRx5Y847IwEOUNTfWxwQUSUGg' -d 'client_id=f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4&client_secret=AMRnkxn
UWxJ3nN9C2XzZ2NuLt-pBJRr3eJRBf9jfkOrUH2Zmb7Nzqwh4k58YR0meRx5Y847IwEOUNTfWxwQUSUGg&grant_type=refresh_token&refresh_token=eyJhbG
ciOiJub25lIn0.eyJleHAiOiJlODk1ODAxMzIsImp0aSI6IjA2NGQ2ODk1LWQ5ZDMtNDNiZS05OTQ2LWw3NWYwNTMzNjdkYyJ9.&scope=openid%20email%20pro
file' 'https://aai-demo.egi.eu/oidc/token' | python -m json.tool;
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 2081    0 1757 100 324 6100 1125 --:--:-- --:--:-- --:--:-- 7225
{
  "access_token": "eyJraWQiOiJvaWRjIiwiaWxniIjoilUMyNTYifQ.eyJzdWIiOiJiZjA2NGQ2ODk1LWQ5ZDMtNDNiZS05OTQ2LWw3NWYwNTMzNjdkYyJ9",
  "expires_in": 3599,
  "id_token": "eyJraWQiOiJvaWRjIiwiaWxniIjoilUMyNTYifQ.eyJzdWIiOiJiZjA2NGQ2ODk1LWQ5ZDMtNDNiZS05OTQ2LWw3NWYwNTMzNjdkYyJ9",
  "refresh_token": "eyJhbGciOiJub25lIn0.eyJleHAiOiJlODk1ODAxMzIsImp0aSI6IjA2NGQ2ODk1LWQ5ZDMtNDNiZS05OTQ2LWw3NWYwNTMzNjdkYyJ9",
  "scope": "openid profile email",
  "token_type": "Bearer"
}
```

# Device AuthZ Grant

**Use Case:** Obtaining tokens in browserless or input-constrained devices



The “device” creates a HTTP request to the /devicecode endpoint:

```
curl -H 'Content-Type: application/x-www-form-urlencoded' -X POST  
'https://aai-demo.egi.eu/oidc/devicecode' -d  
'client_id=f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4&scope=openid%20email%20profile' | python -m  
json.tool;
```

The user opens the “verification\_uri” in their browser and enters the “user\_code”

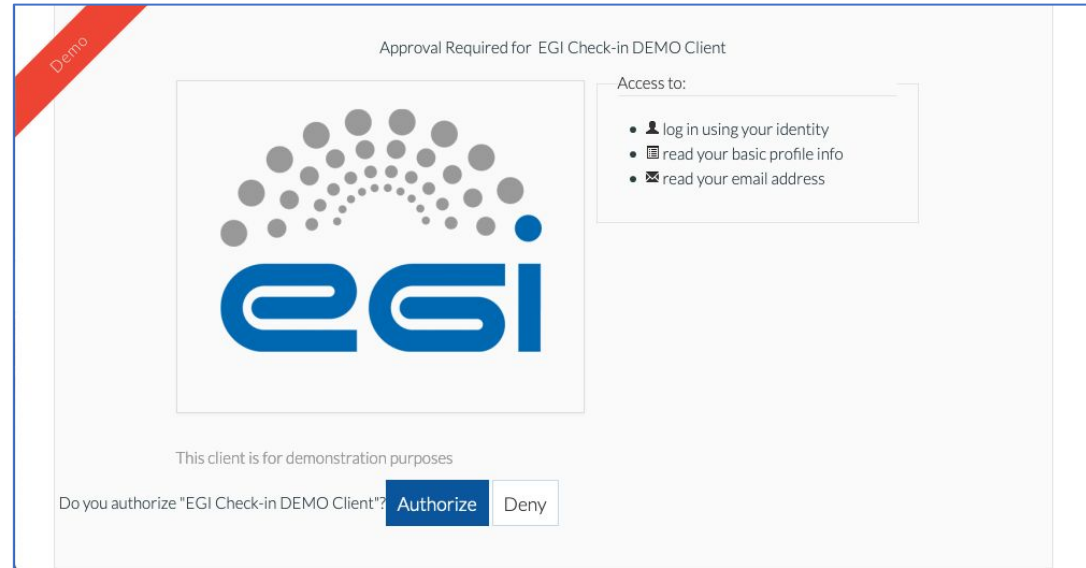
```

grnet@GRNETs-MacBook-Pro-2 ➜ curl -H 'Content-Type: application/x-www-form-urlencoded' -X POST 'https://aai-demo.egi.eu/oidc/devicecode' -d 'client_id=f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4&scope=openid%20email%20profile' | python -m json.tool;
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left     Speed
100  227  100  150  100    77    485    249  --:--:--  --:--:--  --:--:--   734
{
  "device_code": "46ff7852-6c39-444a-8fc7-86e46e85d34c",
  "expires_in": 1800,
  "user_code": "qjfm0T",
  "verification_uri": "https://aai-demo.egi.eu/oidc/device"
}

```

*Response*

Then the user approves the request.



Back to the terminal, create a variable for the “device\_code”.

```
{
  "device_code": "46ff7852-6c39-444a-8fc7-86e46e85d34c",
  "expires_in": 1800,
  "user_code": "qjfm0T",
  "verification_uri": "https://aai-demo.egi.eu/oidc/device"
}
grnet@GRNETs-MacBook-Pro-2 ➤ export device_code=46ff7852-6c39-444a-8fc7-86e46e85d34c
```

The “device” creates a HTTP request to the /token endpoint:

```
curl -H 'Content-Type: application/x-www-form-urlencoded' -X POST
'https://aai-demo.egi.eu/oidc/token' -d
'grant_type=urn:ietf:params:oauth:grant-type:device_code' -d "device_code=${device_code}" -d
'client_id=f68f5df4-d1b1-44b1-a93d-4aab8f80e5c4' -d
'client_secret=AMRnkxnUwxJ3nN9C2XzZ2NuLt-pBJRr3eJRBF9jfkOrUH2Zmb7Nzqwh4k58YROmeRx5Y847IwEOUNtFW
xwQSUGg' -d 'scope=openid email profile' | python -m json.tool;
```

