EGI Check-in

Nicolas Liampotis

EGI AAI Technology Coordination Board Chair, GRNET

WLCG Grid Deployment Board, 8 Nov 2017, CERN

Outline

- Overview
- Use cases
- Status
- Next steps

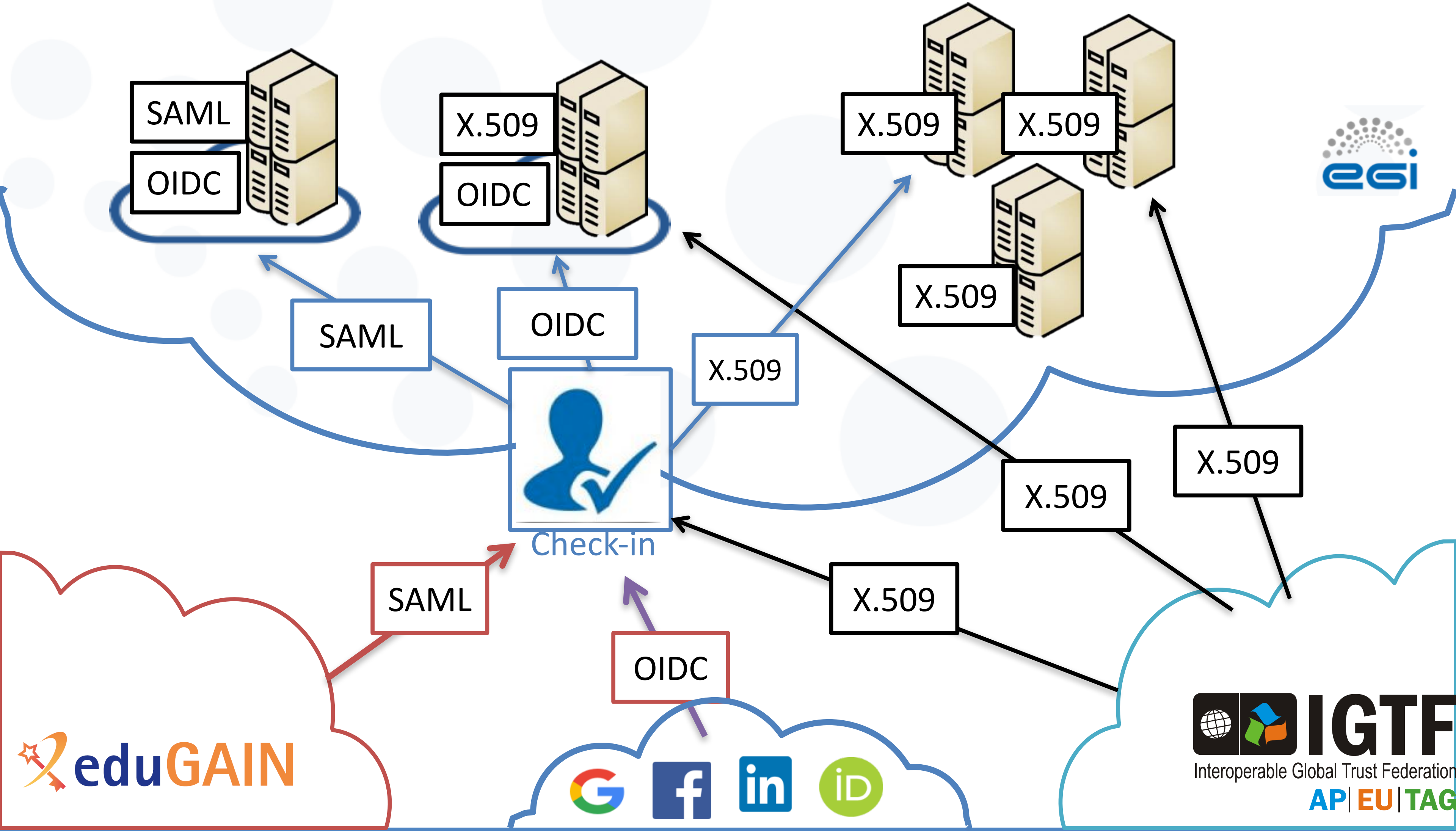
Check-in Overview

In a nutshell

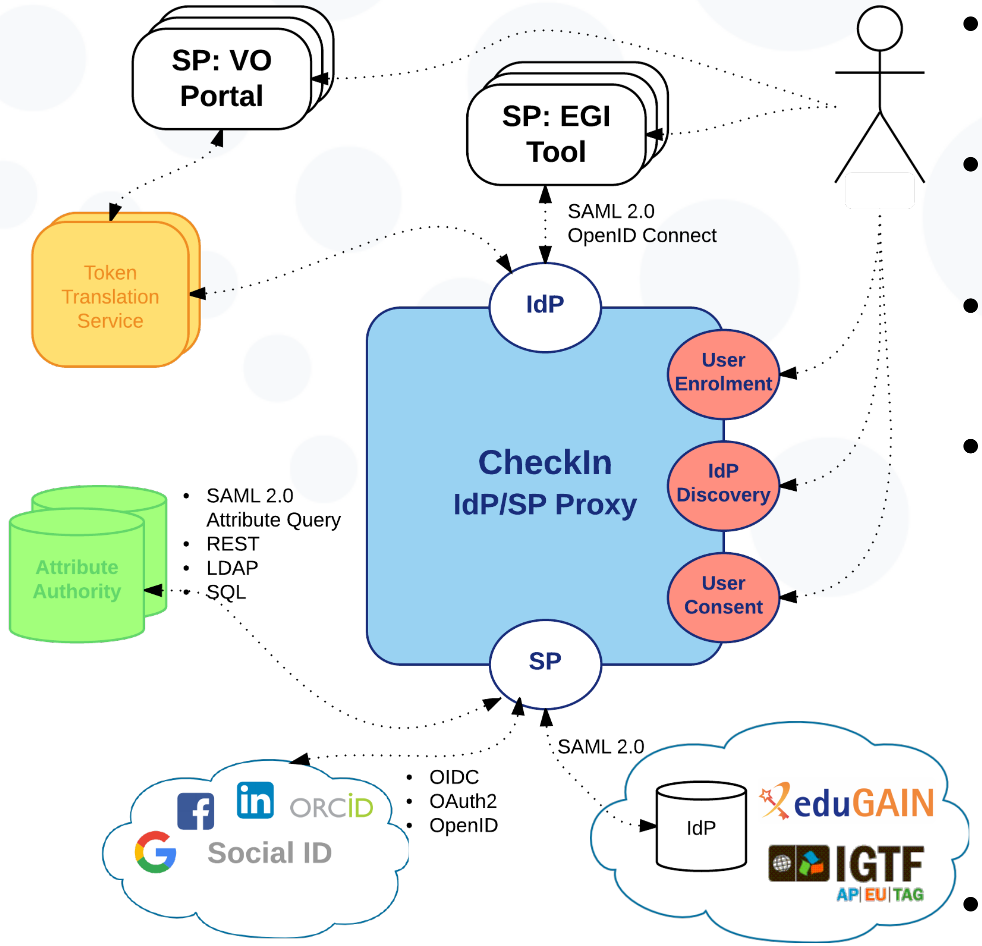
Check-in provides a reliable and interoperable AAI solution for the EGI service providers federation, and external service providers. It enables single sign-on to services through eduGAIN identity providers and other institutional or social media credentials

- Check-in has been developed in EGI-Engage, in close collaboration with the AARC project in order to implement the recommendations of the AARC Blueprint Architecture and Policy Framework
- Services connected to Check-in can be made available to +2,000 universities and research institutes with little or no administrative overhead

A bird's-eye view



Architecture



- Implementation of the AARC blueprint architecture
- All SPs can have one statically configured IdP
- No need to run an IdP Discovery Service on each SP
- Connected SPs get consistent/harmonised user identifiers and accompanying attribute sets from different IdPs/AAs that can be interpreted in a uniform way for authorisation purposes
- External IdPs only deal with a single EGI SP proxy

What is new or improved?

- ✓ Secure - operates under the strict security policies of the EGI federation
- ✓ Simple - hides the complexity of dealing with multiple authentication providers and sources of authorisation information
- ✓ Low overhead - lowers the bureaucratic burden of integrating multiple identity providers and attribute authorities
- ✓ Interoperable - implements the AARC blueprint architecture and is compliant with eduGAIN, REFEDS R&S and Sirtfi policies
- ✓ Polyglot - translates SAML 2.0, OpenID Connect, OAuth 2.0 and X.509 credentials

What benefits does Check-in bring?

- Only one account needed for federated access to multiple heterogeneous (web and non-web) service providers using different technologies (SAML, OpenID Connect, OAuth 2.0, X509)
- Identity linking enables access to resources using different login credentials (institutional/social)
- Assurance information associated to each authenticated identity
- Aggregation and harmonisation of authorisation information (VOs/groups, roles) from multiple sources

Deployment options

Check-in is offered in 2 deployment models:

- As a multi-tenant service:
  - All the standard Check-in authentication options
  - Independent community management using COmanage or Perun
  - Limited customisation of user-facing interfaces (e.g. community-specific themes for enrolment flows, group management)
  - Limited customisation of AAI proxy behaviour
- As a dedicated service (individual components or AAI platform as a whole:
  - Customisation of user-facing interfaces: WAYF, enrolment, group membership UI
  - Customisation of AAI proxy behaviour (e.g. attribute aggregation rules, service entitlements)
  - Easy integration with the main Check-in instance, or other dedicated instances if necessary

Reliable and secure AAI platform

EGI has always invested in improving and maintaining the reliability and security of the services

CERTIFIED BY TI TRUSTED INTRODUCER

TÜV SÜD ISO 20000

TÜV SÜD ISO 9001

- EGI has a mature and complete set of security policies and the processes to enforce them
  - Extended with Check-in specific policies:
    - ✓ Check-in acceptable usage policy
    - ✓ Check-in data protection policy
    - ✓ Agreement documents to integrate non-EGI and non-eduGAIN SPs and IdPs and maintain the compliance

Check-in use cases

Who can use Check-in? For what?

Check-in can provide secure and user-friendly federated authentication and authorisation for:

- User communities with different needs:
  - operating their own full-fledged AAI solution
  - operating their own group management service
  - in need of a ready-to-use group management solution
- Service Providers
  - looking to leverage “AAI as a Service”

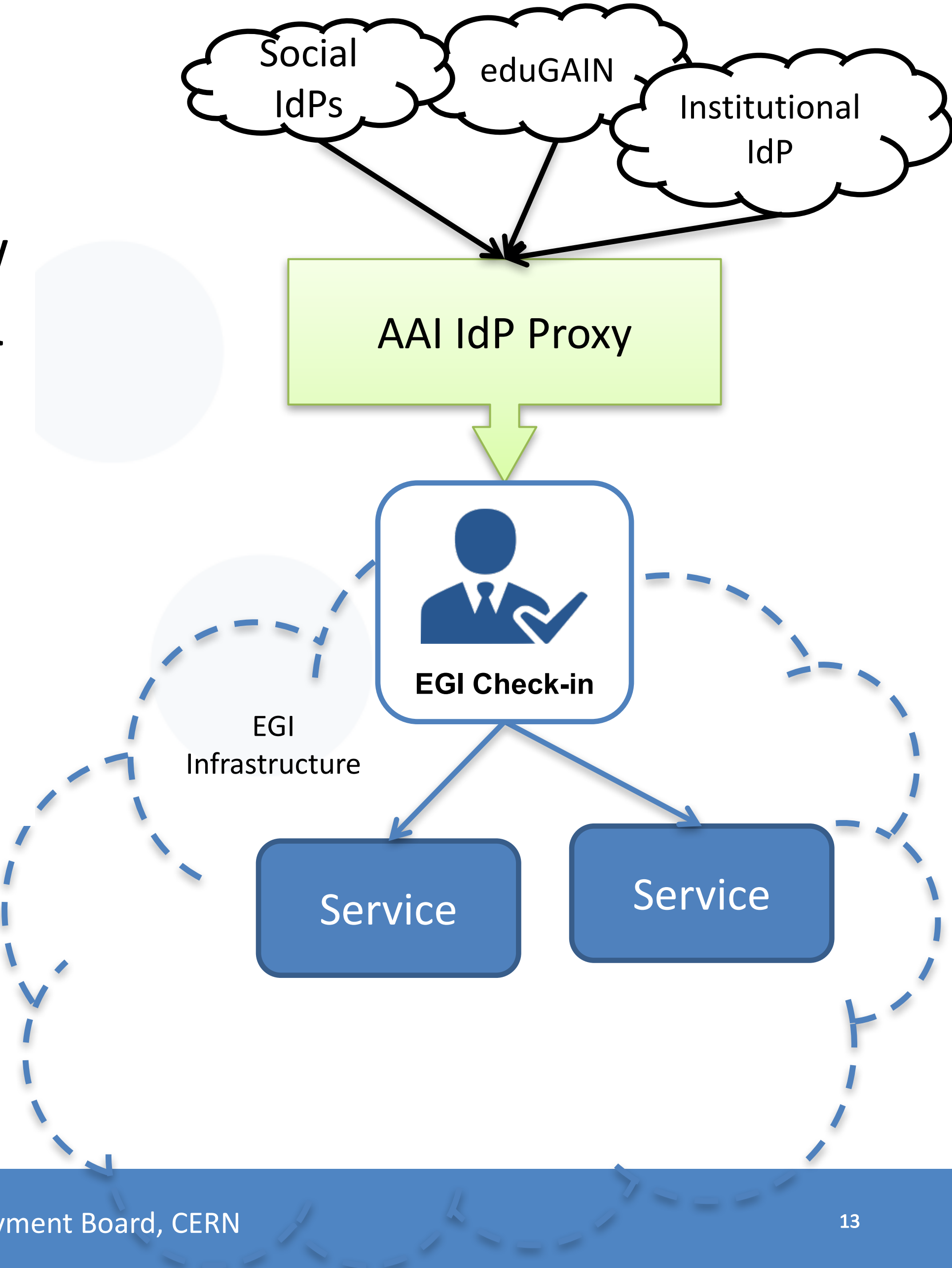
www.egi.eu

For communities operating their own AAI

Community's AAI connected to Check-in as an IdP Proxy to allow its users to access EGI services & resources

✓ Access EGI services without changing your authentication workflow

Examples: *ELIXIR Research Infrastructure - Check-in allows ELIXIR users to use their ELIXIR IDs to interact with relevant EGI services (Cloud, Configurations database, Applications on Demand*



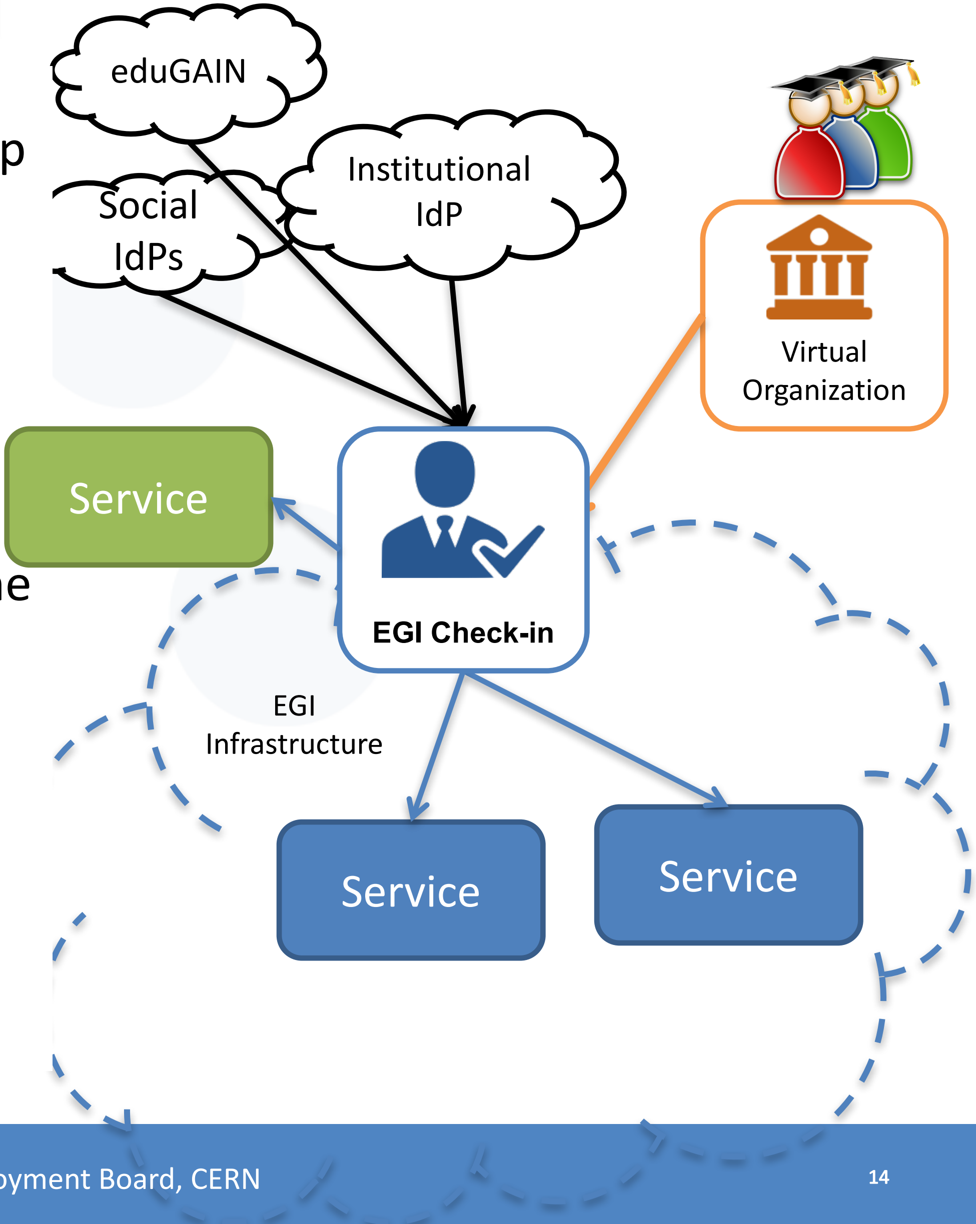
www.egi.eu

For communities operating their own group management service

Community managing authorisation information about the users (VO/group memberships and roles) via their own group management service, which is connected to Check-in as an external attribute authority

- ✓ Check-in will handle the configuration of the IdPs and the aggregation of the attributes for the SPs
- ✓ No need to migrate the group management functionality to an EGI-specific attribute authority

***Examples:** VOMS-managed VOs such as FedCloud*

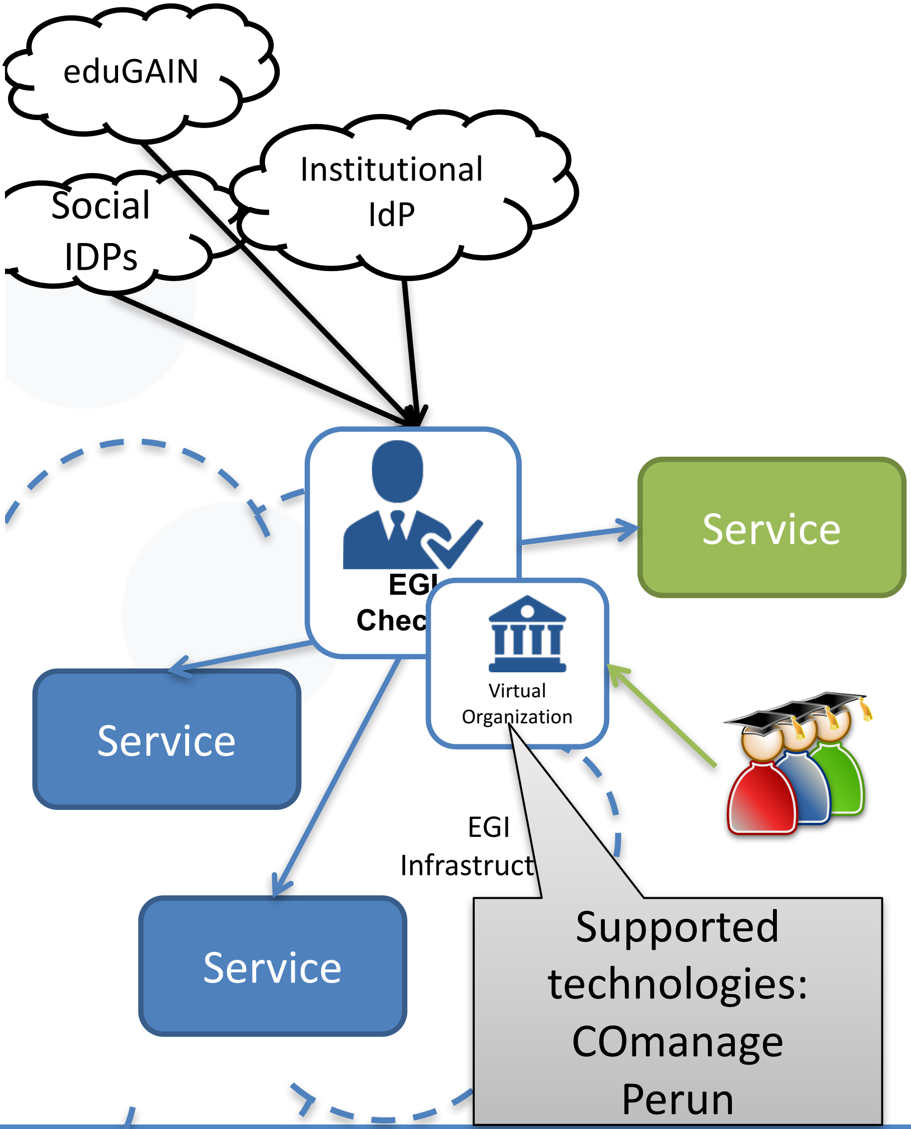


For communities in need of a ready-to-use group management solution

Communities that do not operate their own group management service can leverage the group management capabilities of the Check-in platform

- ✓ Ready-to-use solution
- ✓ Avoid overhead of deploying a dedicated group management service
- ✓ Support for multi-tenancy to allow authorised VO admins to manage the information about their users independently
- ✓ Easy connect to both EGI and non-EGI services

Examples: *Training and Long Tail of Science communities*



Supported technologies:
COmanage
Perun

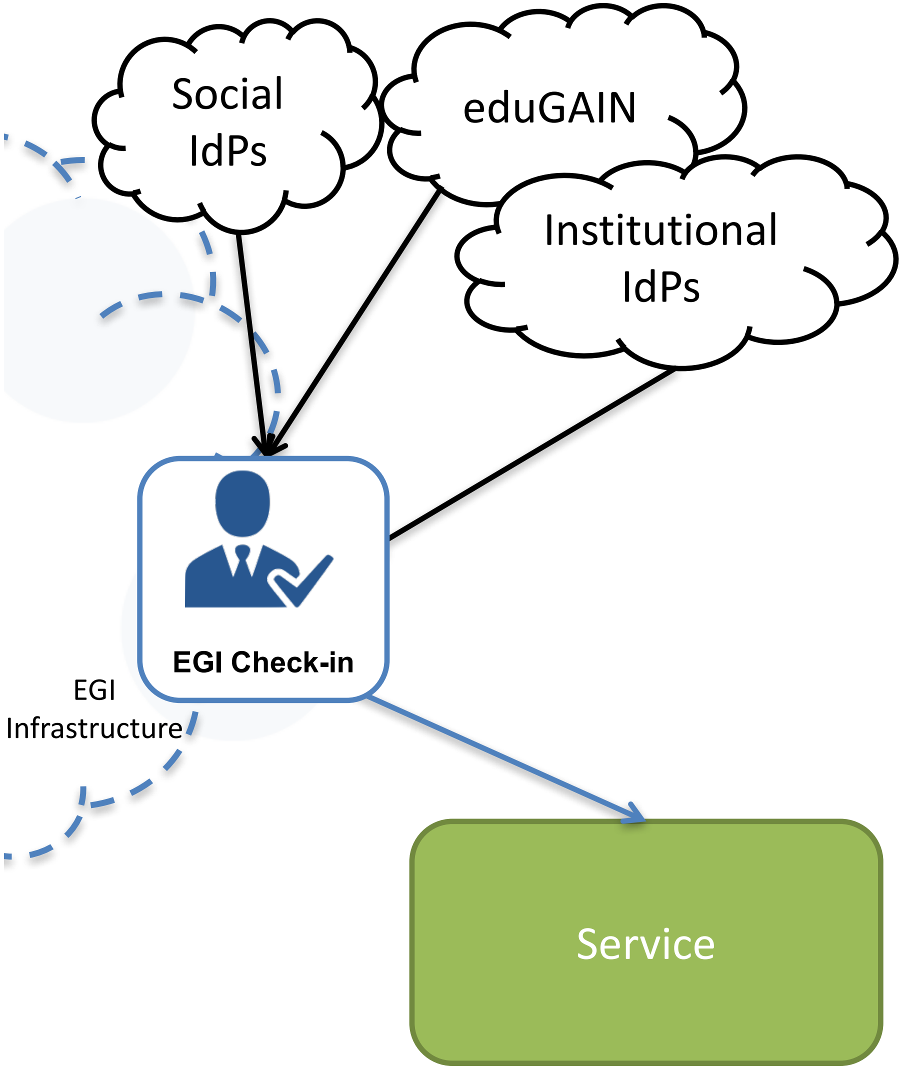
For service providers: AAI as a service

Check-in as an authentication proxy

- ✓ Enable login from institutional IdPs in eduGAIN and social media
- ✓ Minimal overhead for the service development
- ✓ All the other Check-in features are available for the SP: account linking, attribute aggregation, ..

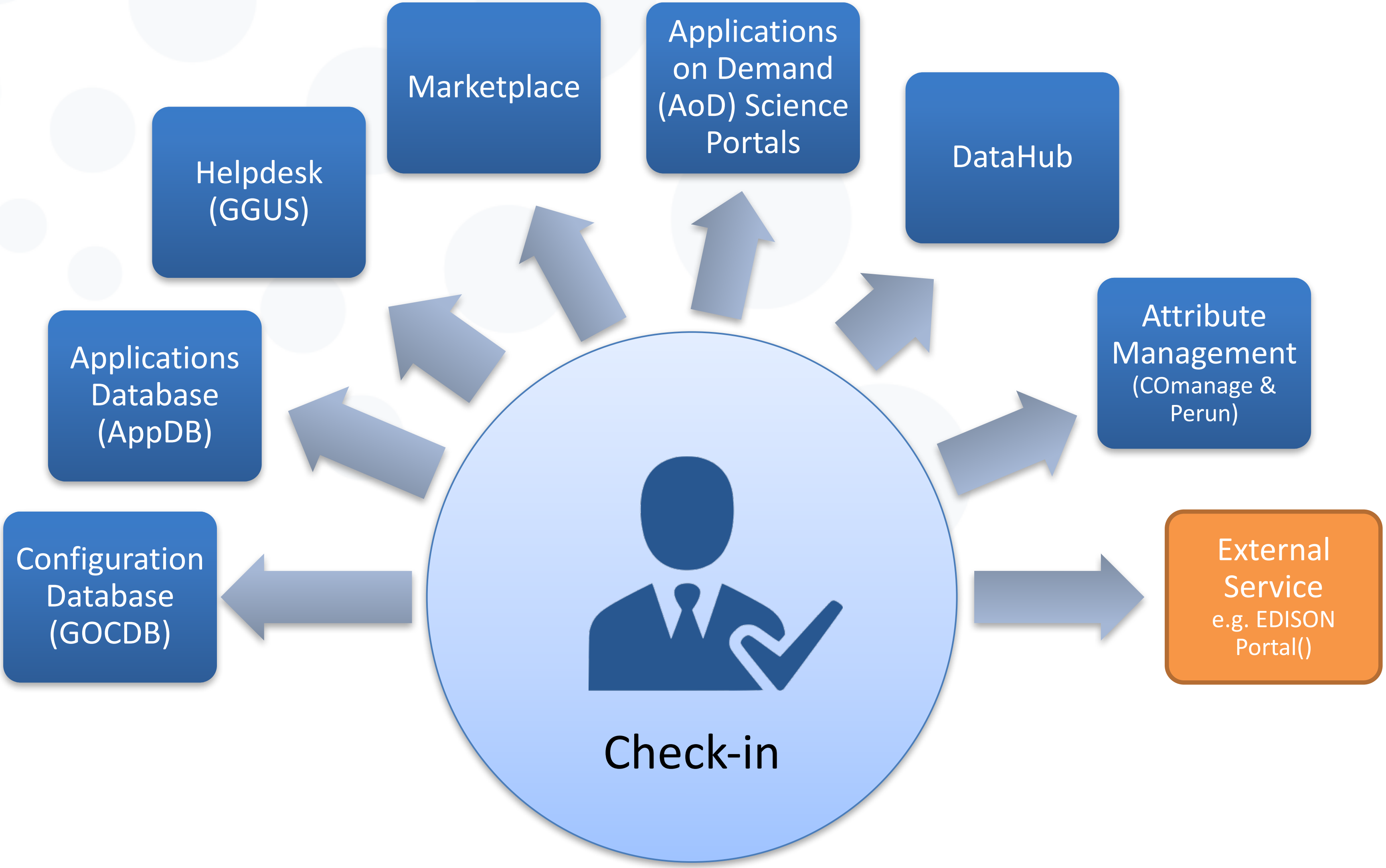
- Prerequisites:
  - ✓ Service provider must accept EGI policies on data protection

***Examples:** EDISON Community Portal*



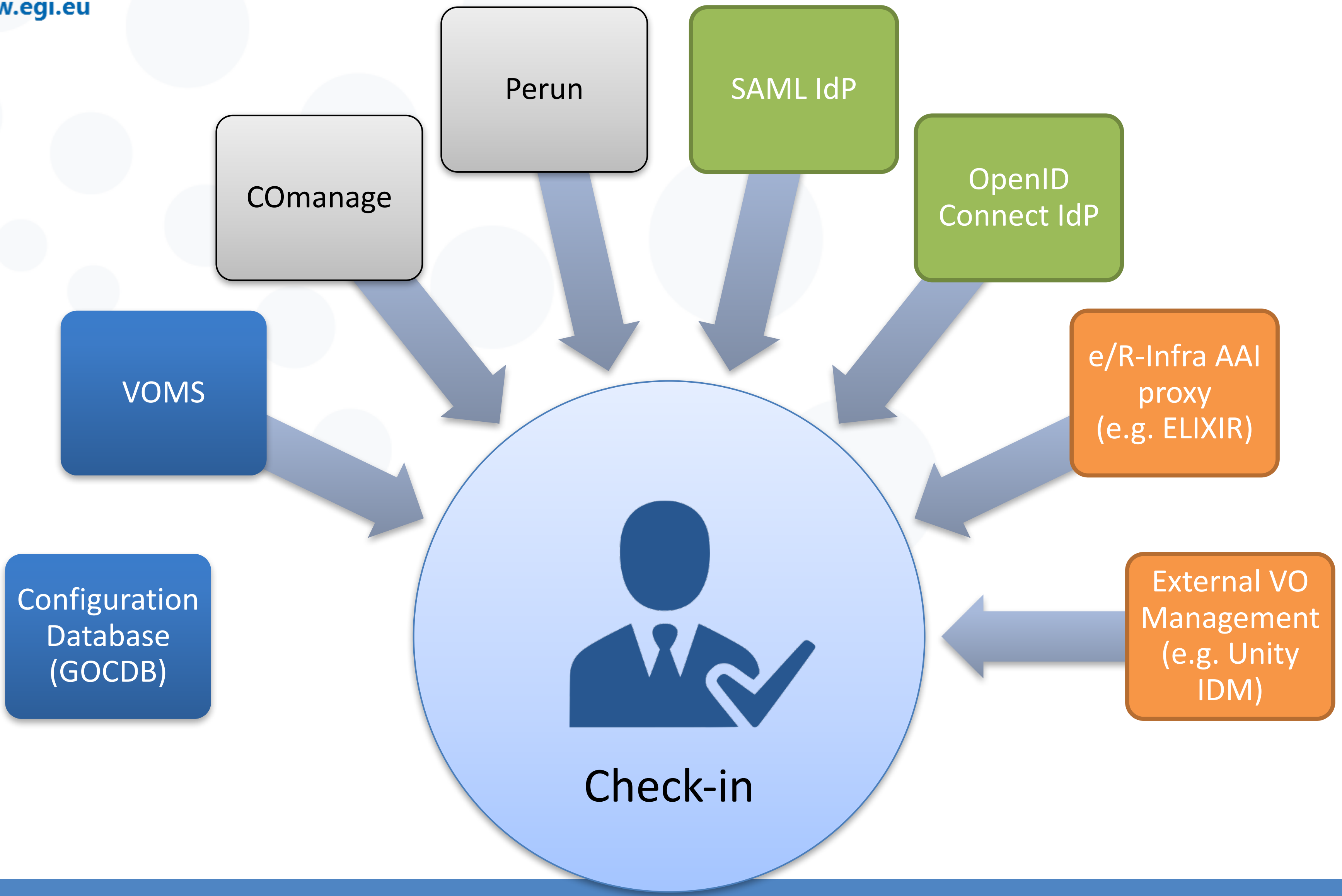
Check-in Status

Check-in enables access to several services



Marketplace
Applications on Demand (AoD) Science Portals
Helpdesk (GGUS)
DataHub
Applications Database (AppDB)
Attribute Management (COmanage & Perun)
Configuration Database (GOCDB)
External Service e.g. EDISON Portal()
Check-in

Check-in consumes information from many diverse sources


Perun
SAML IdP
COmanage
OpenID Connect IdP
VOMS
e/R-Infra AAI proxy (e.g. ELIXIR)
Configuration Database (GOCDB)
External VO Management (e.g. Unity IDM)
Check-in

Group membership and role information in Check-in

Use of URN-formatted entitlement values:

```
<namespace>:group:<group>[:<subgroup>*][:role=<role>]#<group-authority>
```

- <group> is the name of a VO, research collaboration or a top level arbitrary group; unique within a given <namespace>
- optional list of <subgroup> components represents the hierarchy of subgroups in the <group>
- optional <role> component indicates particular position of the user; scoped to the rightmost (sub)group
- <group-authority> indicates the authoritative source for the group membership and role information

Assurance information

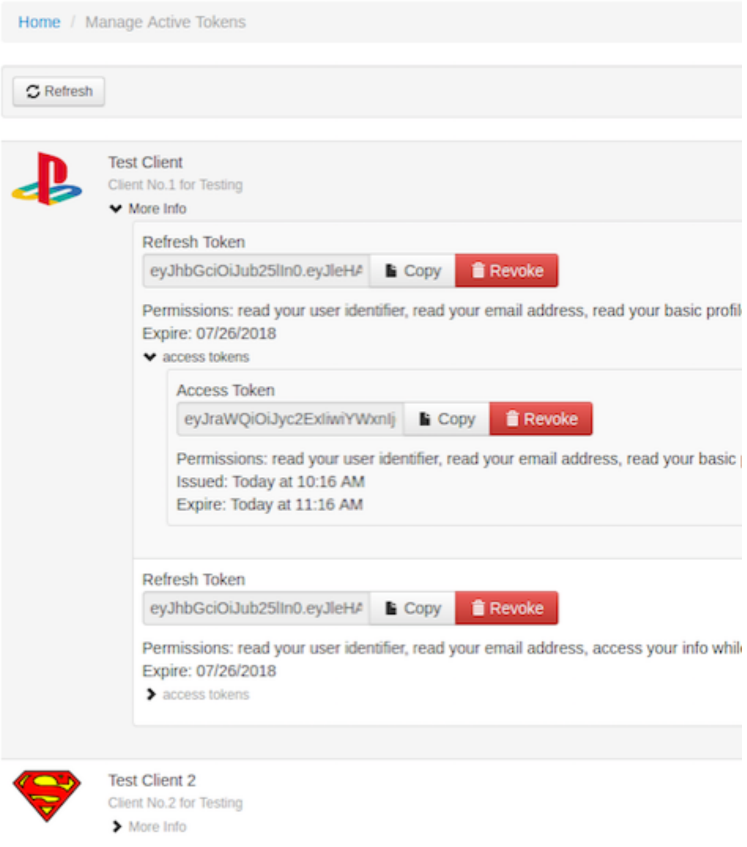
- Check-in conveys the assurance associated with the authenticated identity to SPs for authorisation purposes
  - Communicated through the eduPersonAssurance attribute in SAML or acr clain in OIDC
  - Translated into entitlements expressing the right of a user to access a particular resource (e.g. access Rcauth Onlince CA)

- Check-in will align with REFEDS/AARC Assurance Profiles:

Key features/ Profiles	*AARC-Assam*	IGTF-DOGWOOD	IGTF-BIRCH	AARC-Darjeeling
Unique ID		✓	✓	✓
Identity Vetting			✓	✓
Multi Factor				✓

Managing OpenID Connect/OAuth 2.0 tokens

- Provides users with an overview of all OpenID Connect/Oauth 2.0 services they have authorised to access their EGI account
- Allows users to see the specific permissions (e.g. read email, offline access, etc.) granted to each service
- Enables users to manage access/refresh tokens associated with each service:
  - Revoke access for individual tokens or service as a whole
  - Retrieve access/refresh tokens to be used for federated access to CLI tools/APIs



Test Client
Client No.1 for Testing
More Info

Refresh Token
eyJhbGciOiJub25lIn0.eyJleHA
Permissions: read your user identifier, read your email address, read your basic profil
Expire: 07/26/2018
access tokens

Access Token
eyJraWQiOiJyc2ExIiwiYWxnIj
Permissions: read your user identifier, read your email address, read your basic
Issued: Today at 10:16 AM
Expire: Today at 11:16 AM

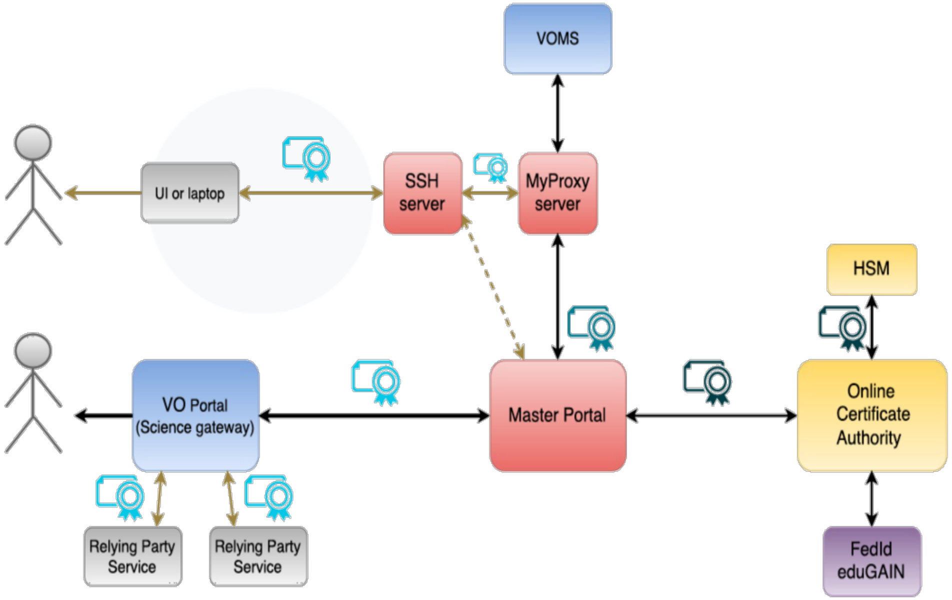
Refresh Token
eyJhbGciOiJub25lIn0.eyJleHA
Permissions: read your user identifier, read your email address, access your info whil
Expire: 07/26/2018
access tokens

Test Client 2
Client No.2 for Testing
More Info

Integration with RCauth.eu Online CA

- Check-in has been integrated with the production RCAuth.eu Online CA
  - Users can retrieve X.509 proxies by authenticating through Check-in

- Check-in Master Portal retrieves end-entity certificate from RCauth.eu
- Long-lived proxy certificate stored in backend MyProxy server
- Short-lived proxies provided via:
  - Science Gateways via OIDC (so-called VO-portals)
  - users e.g. via SSH key authentication



Next steps

Check-in next steps

- Align with AARC guidelines on expressing group membership and role information
- Align with REFEDS/AARC Assurance Profiles
- Complete integration with EUDAT AAI
- Complete integration with GÉANT AAI
- Support for (de-)provisioning and continuous update of user account information

Check-in in EOSC-hub

- Check-in will be one of the pillars of the AAI services for EOSC-hub
- EOSC-hub AAI platform will be interoperable with several RIs and thematic services:

CLARIN
ELIXIR
ENES
ICOS
LifeWhatch
ICOS

CMS
EISCAT
EPOS
ITER
LNEC
WeNMR

DARIAH
EIDA
GEOSS
IFREMER
LOFAR

Thank you for your attention.

Questions?

www.egi.eu