The EGI Identity and Access Management service

Check-in status and roadmap

Nicolas Liampotis

GRNET

Sept 20, 2022

EGI Conference 2022

Dissemination level: Public

Outline

- Introduction to Check-in
- What's new
- Roadmap

Check-in

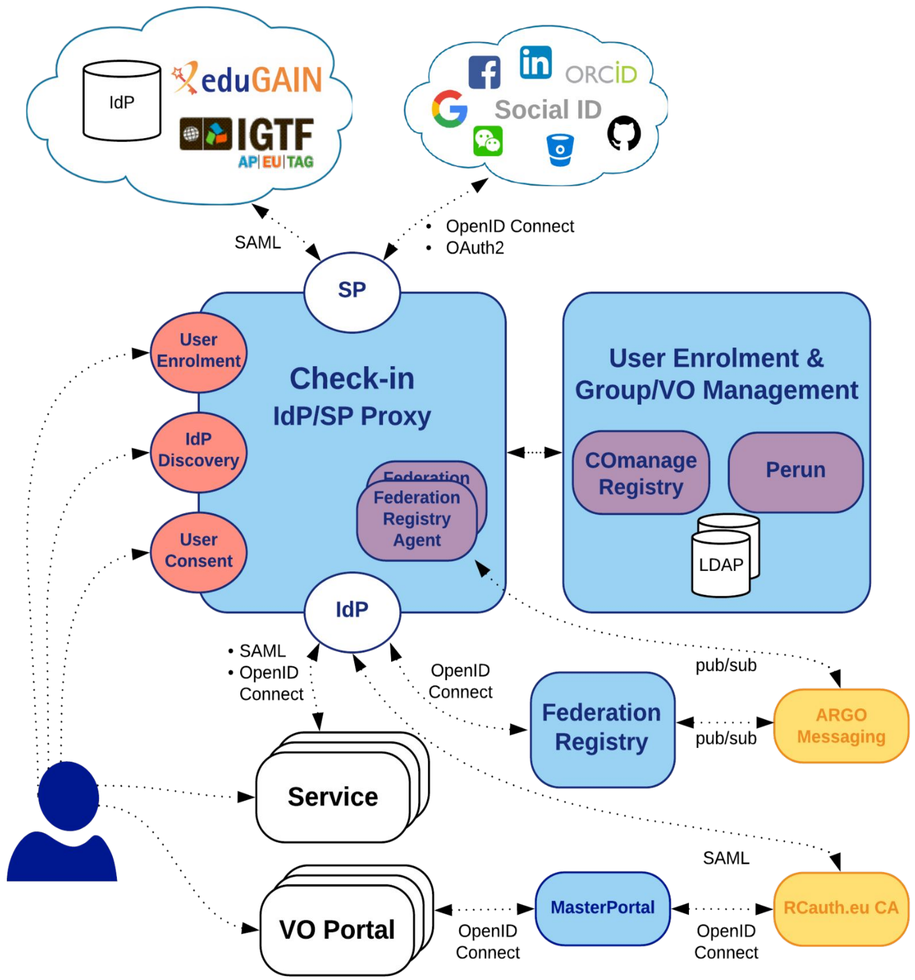
In a nutshell

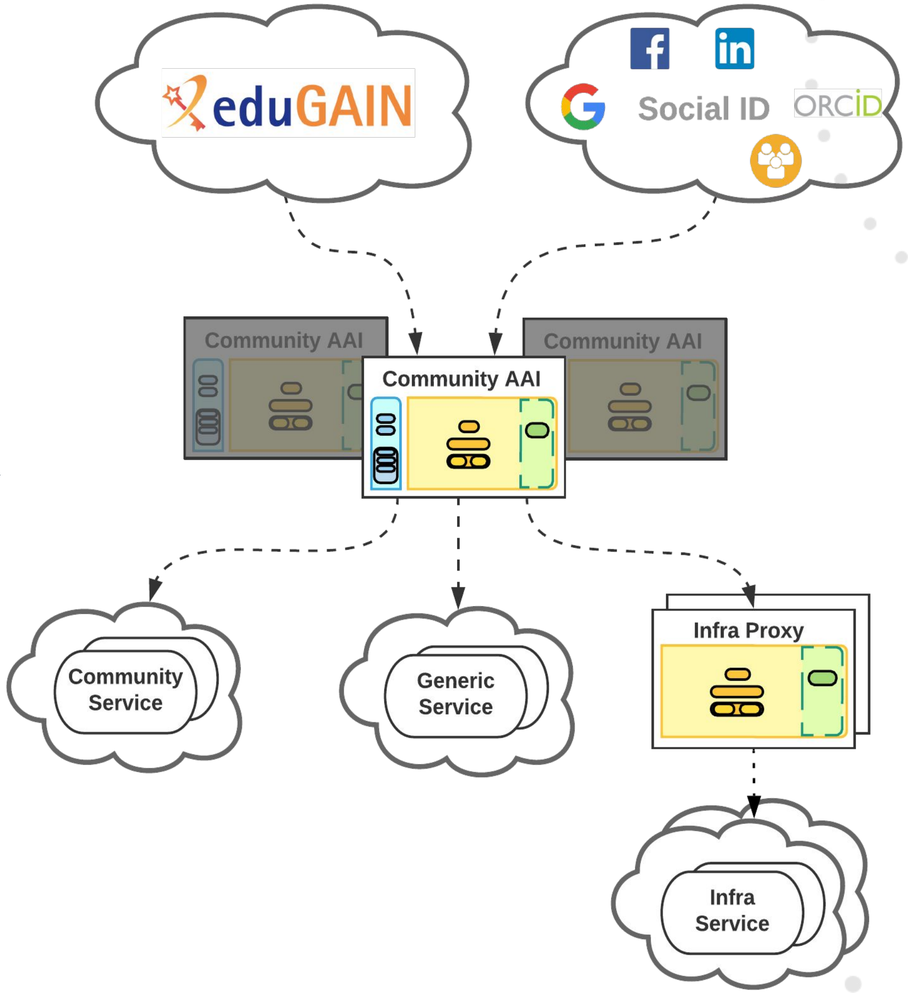
- Identity and Access Management solution that makes it easy to secure access to services and resources
- Single sign-on to services using existing credentials:
  - Academic (e.g. eduGAIN, ORCID)
  - Social media (e.g. Google, Facebook, LinkedIn)
  - Community-managed identities (e.g. EOSC)
- Federated access to multiple heterogeneous (web and non-web) service providers using different technologies (SAML, OpenID Connect/OAuth 2.0, X.509)
- Identity linking for accessing resources using different login credentials (institutional/social)
- Expressing the level of trust in the identity assertions
- Aggregation and harmonisation of authorisation information (VOs/groups, roles, assurance) from multiple sources

Check-in

Architecture

Implementation of the
[AARC Blueprint Architecture]





Check-in

Last year in numbers

803

Identity Providers

141

Services

67 K

Logins

4,5 K

+44 %

User Registrations

What's new?

The EGI Identity and Access Management service: Check-in

Migration to Keycloak

Motivation

- Identity brokering (proxy architecture)
- Support for popular protocols (OpenID Connect, OAuth 2.0 and SAML)
  - OpenID Certified
  - Token Introspection
  - Device AuthZ Grant
  - Token Exchange
  - Client Credentials
- Clustering for scalability and availability
- Client adapters/libraries for popular languages/frameworks (Java, Python, etc)
- Stronger authentication mechanisms (MFA, W3C WebAuthn)
- Active open source community

Migration to Keycloak

Improved compliance with OIDC / OAuth 2.0 standards

OAuch.io – OIDC, SecBCP, RFC6749, RFC6750, RFC8628, RFC7636, RFC6819, RFC7523

A+ EGI Check-in - PROD/DEMO	A+ EGI Check-in - DEVEL	B EGI - MITREid
5,6%	4,2%	20,2%
Fail rate	Fail rate	Fail rate

Migration to Keycloak

New OIDC / OAuth 2.0 flows (EXPERIMENTAL)

- Support **Remote OAuth 2.0 Token Introspection** from trusted external Authorization Servers (see AARC-G052 draft specification & ESACO implementation)
- Support scope-based mechanism for a client to **request specific Claim values** (e.g. VO/group entitlements) a.ka. dynamic / parametric scopes
- Support scope-based mechanism for a client to directly **request the presence of specific claims** (e.g VO/group entitlements) **in JWT** access tokens

Enable *online* token validation across infrastructures → Integration with EOSC AAI Federation

Enable *offline* token validation →integration with DIRAC, ARC-CE and HTCondor

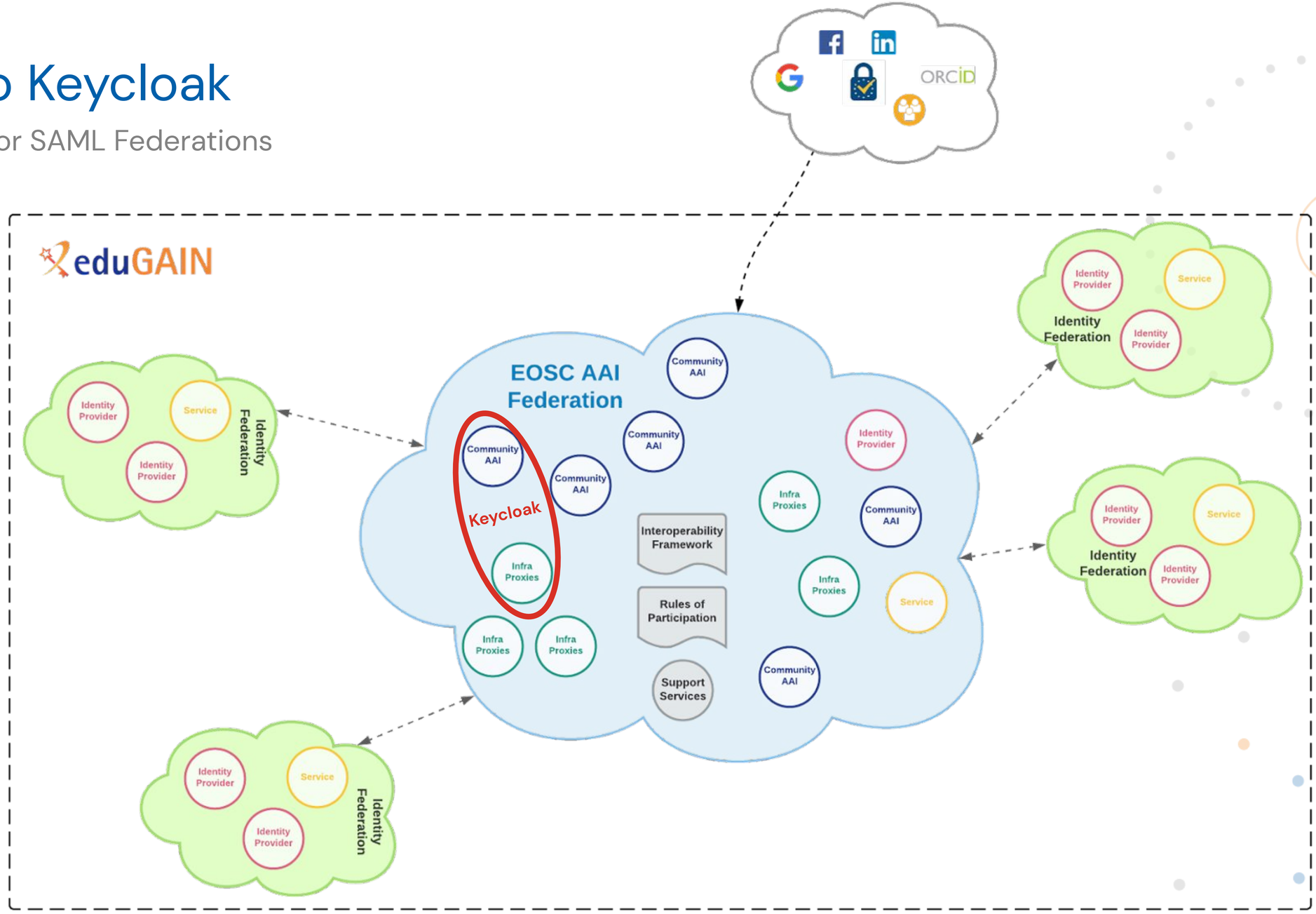
Migration to Keycloak

Extended support for SAML Federations

- Support for **SAML IdP Federations** (e.g. eduGAIN)

NEW

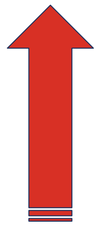
Support for **SAML SP Federations** (e.g. EOSC AAI Federation)



Migration to Keycloak

Phased approach

Phase I	Phase II	Phase III
Keycloak as Check-in OIDC Provider	Keycloak as Check-in SAML Identity Provider	Keycloak-based Check-in
ETA: Sept 2022	*ETA: Nov 2022*	*ETA: Q2 2023*



Migration to Keycloak

Phase I: Status

Phase I

Keycloak as Check-in OIDC Provider

ETA: Sept 2022

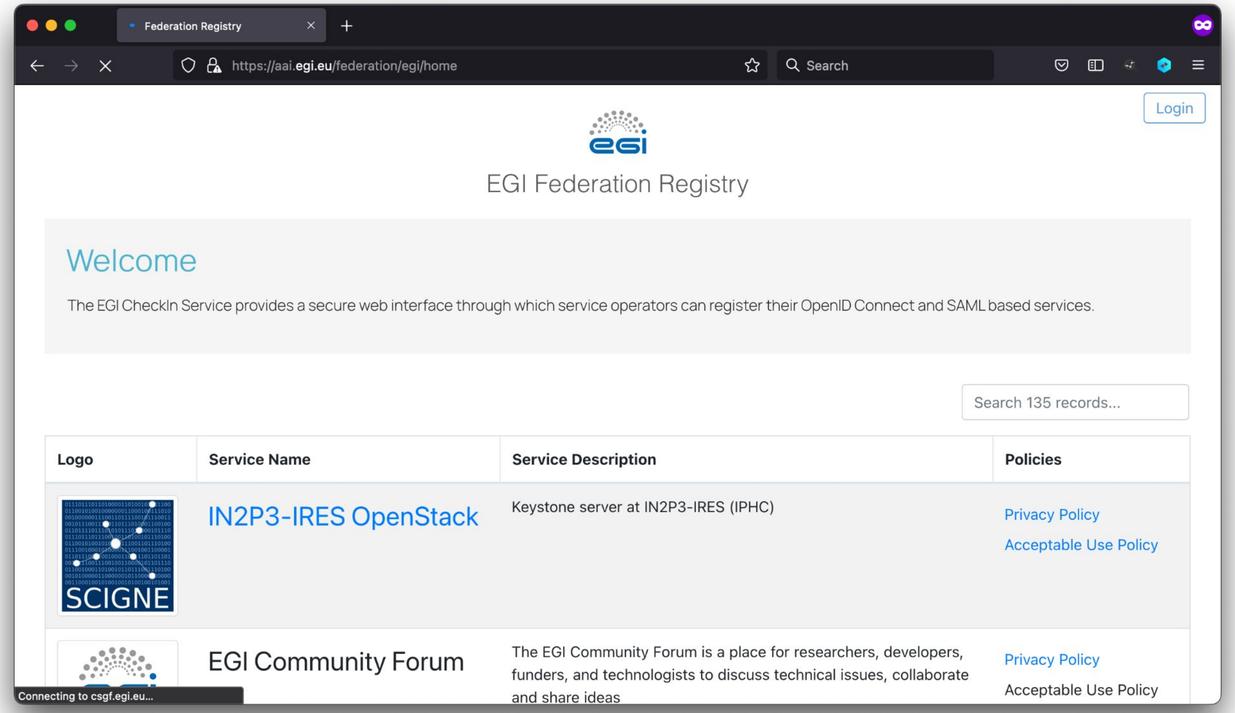
62%

Successfully Migrated Services

Streamlined service integration

Federation Registry

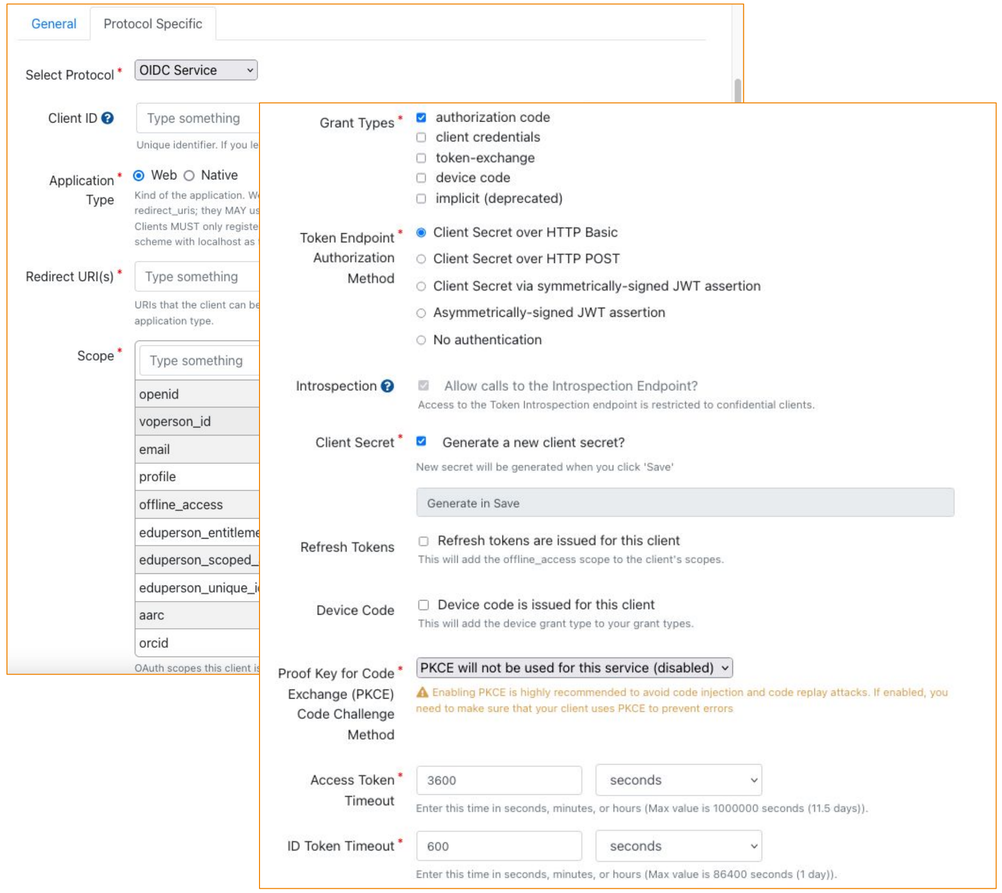
- Secure **registration**, **reconfiguration**, and **deregistration** of service providers
- **Uniform interface** regardless of the underlying protocol (OIDC or SAML)
- **Different AAI proxy technologies** (Keycloak, SimpleSAMLphp, MITREid Connect)



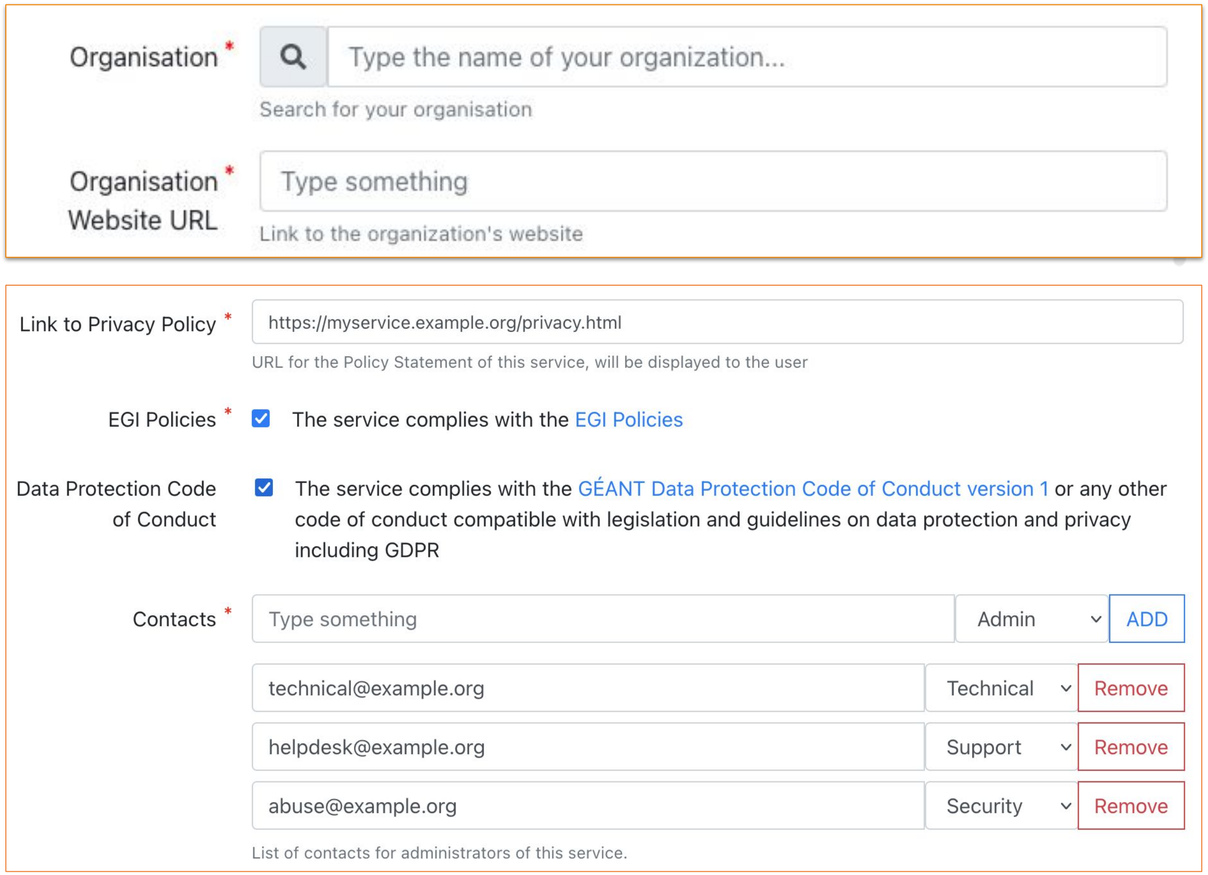
https://aai.egi.eu/federation

Streamlined service integration

Federation Registry: What's new for Service Owners?



Updated technical configuration (Keycloak + SecBCP)

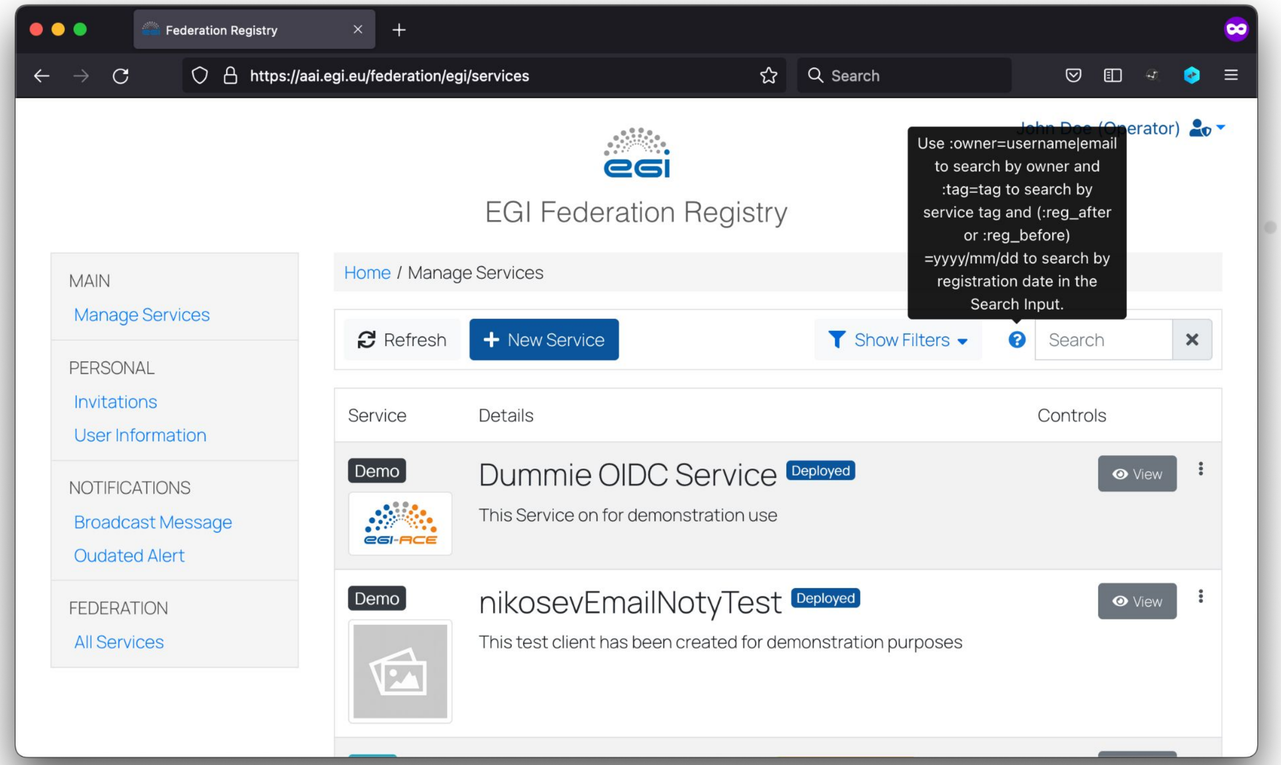


Extended non-technical configuration (organisation info, required contacts)

Streamlined service integration

Federation Registry: What's new for Check-in admins?

- Support for adding tags to services
- Extended search filters:
  - protocol (OIDC, SAML)
  - status (e.g. pending deployment)
  - protocol identifier (OAuth 2.0 Client ID / SAML entityID)
  - registration date (before/after)
- Support for broadcasting messages to service owners based on:
  - protocol (OIDC, SAML)
  - integration environment (development, demo, production)
  - contact type (admin, security
- Support for highlighting changes between snapshots in service configuration history



Improved interoperability

- Initial support for expressing affiliation with Home Organisation via voPersonExternalAffiliation attribute (AARC-G025) → Enable registration of Check-in as *Community AAI* in EOSC AAI Federation
- Redirect users to Community Sign-up flow based on IdP tag in metadata → Enable registration of Check-in as *Infrastructure Proxy* in EOSC AAI Federation
- Support for expressing extended profiles attributes managed in Perun as capabilities (AARC-G027)

Roadmap

The EGI Identity and Access Management service: Check-in

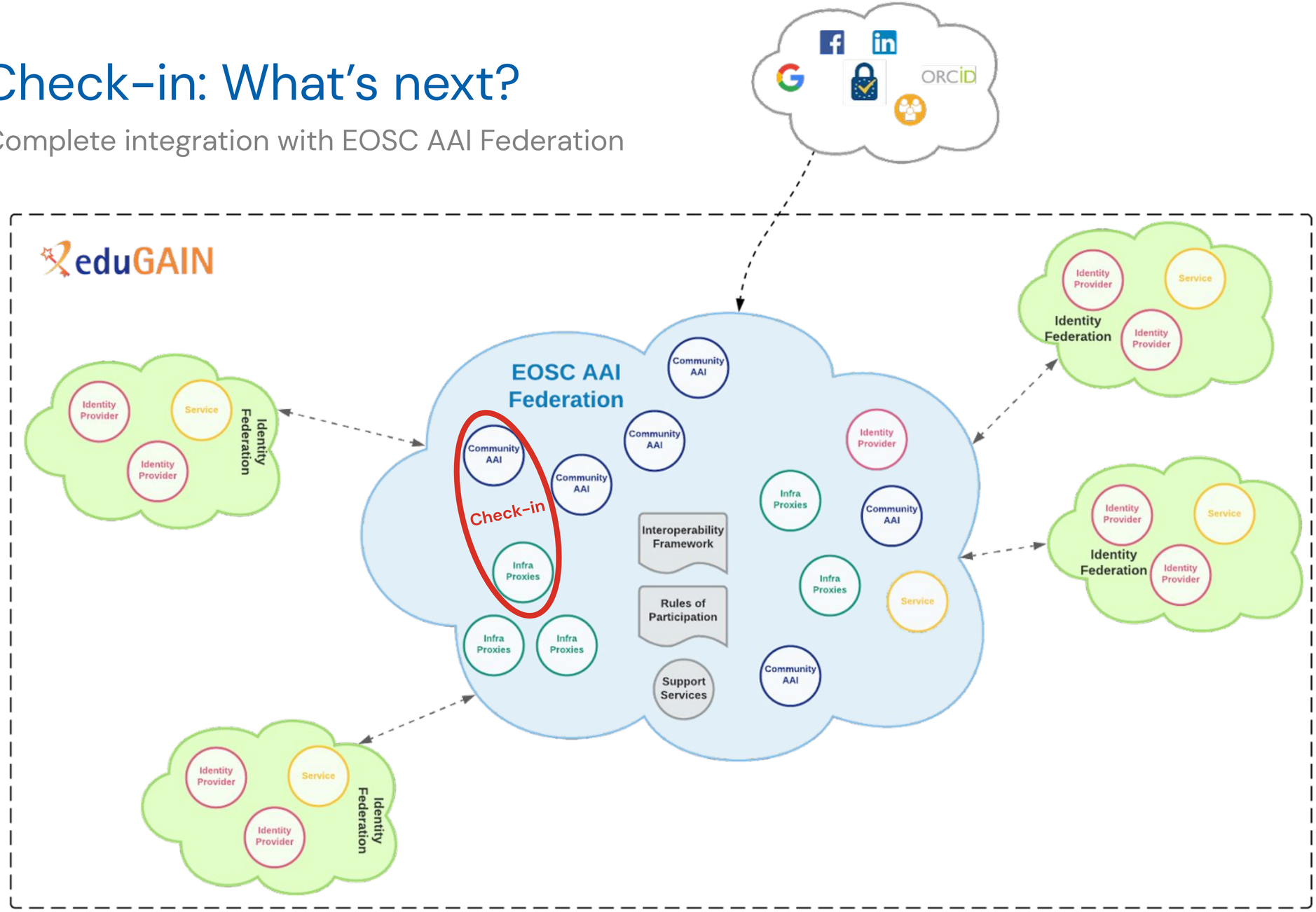
Check-in: What's next?

Overview

- Complete integration with EOSC AAI Federation
- Integrate Check-in Proxy with new dedicated instance of Perun
- Assert compliance with SIRTFI Security Framework on the Identity Provider interface of the Check-in Proxy ⇒ Enable MasterPortal/RCauth Online CA to expand its user base
- Update Privacy Policy to comply with Data Protection Code of Conduct v2
- Provide AARC/Check-in compliant token validation plugin for ARC-CE and HTCondor CEs
- Complete migration to Keycloak
- Support decentralised identity management - Self Sovereign Identities (SSI)

Check-in: What's next?

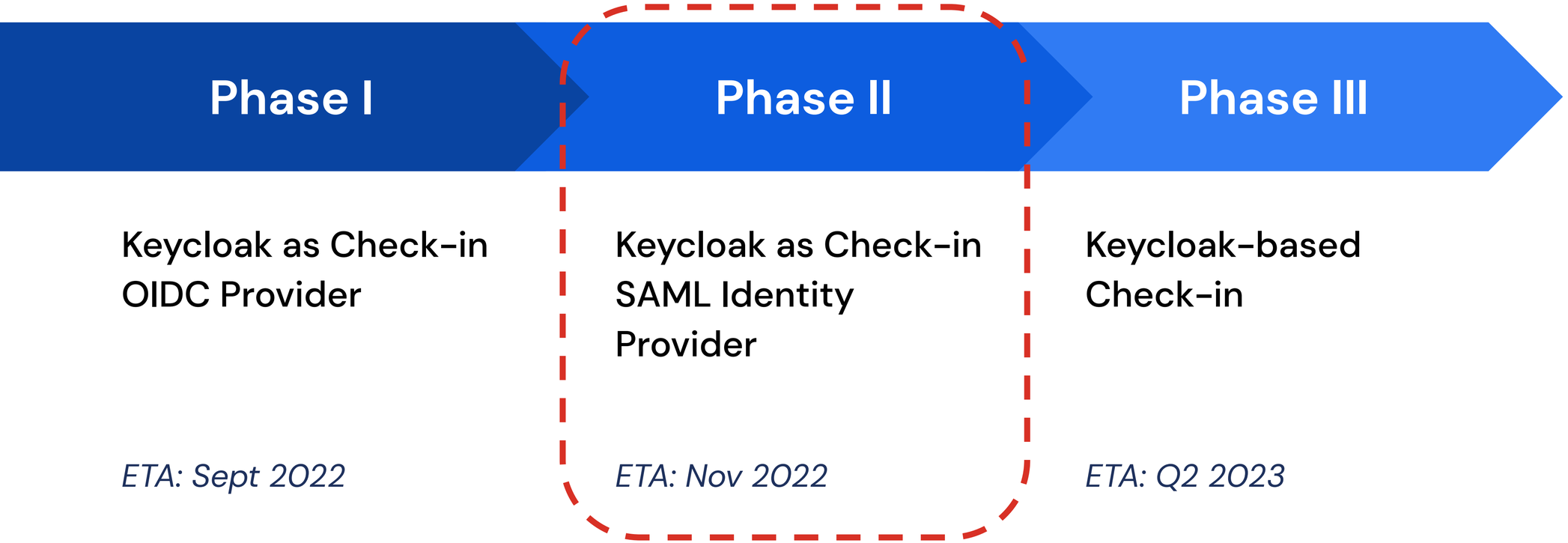
Complete integration with EOSC AAI Federation



- Enable EOSC AAI Federation metadata feeds *[ETA: Sept 2022]*

Migration to Keycloak

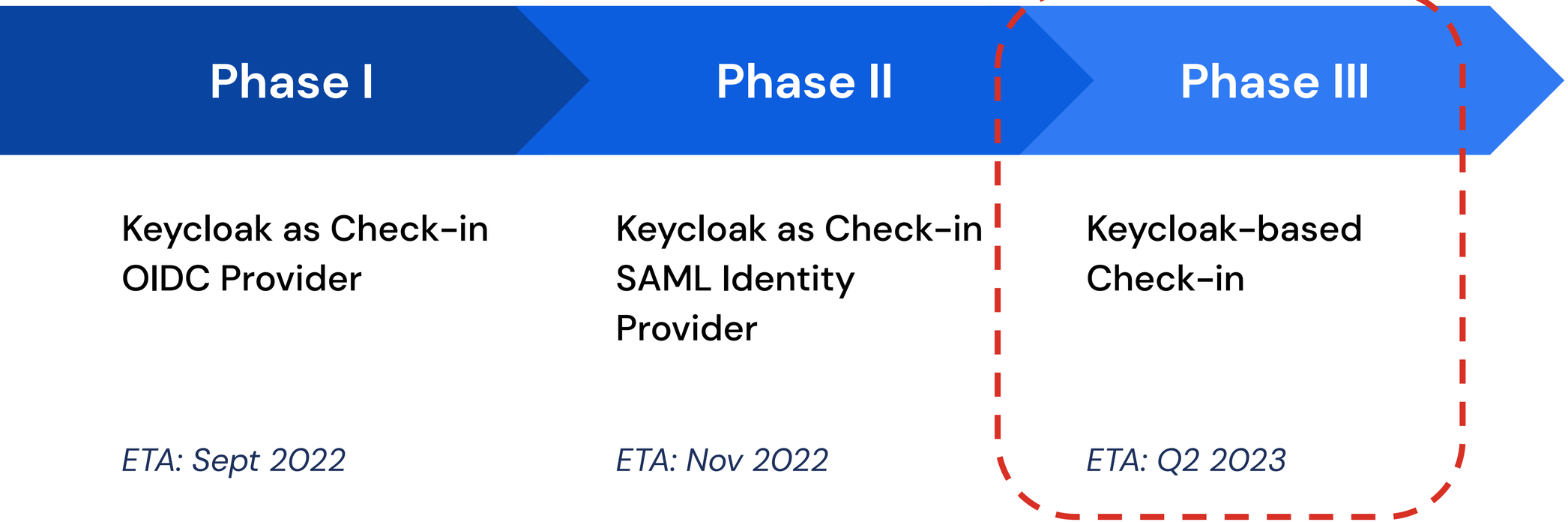
Phase II



- Extend SAML service model in Federation Registry to allow Service Owner to specify required attributes
- Migrate SAML services from SimpleSAMLphp to Federation Registry
- Communicate migration plan to SAML service owners

Migration to Keycloak

Phase III



- Extend Keycloak to support advanced group management (VO enrollment flows, AUP mgmt)
  - Provide SCIM-compatible VO/group API
- New statistics dashboard for Keycloak (Prometheus + Grafana)
- Integrate with Perun (LDAP)
- Integrate with GOCDB (new Keycloak extension)

Thank you

Nicolas Liampotis

nliam@grnet.gr | check-in@egi.eu

www.egi.eu

This work is partially funded by the EU research and innovation programme