EGI-Engage JRA1.1 Authentication and Authorization Infrastructure

Christos Kanellopoulos
Nicolas Liampotis - GRNET

WP3 Meeting - 2017.03.24

www.egi.eu

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

EGI-Engage Targets

- Explore approaches to **easier safe management of user credentials**
- Identify possibilities and requirements for user authentication against both **web and non web-based applications**.
- Identify **user registration and management requirements** from a VO perspective. **Engage with the CCs**, capture workflows and develop solution prototypes.
- **Explore current technical possibilities** and the usability of existing infrastructures covering identity management
- Develop **authentication solutions for use cases**
- Investigate **alternative identity-vetting approaches** to current practices
- **Liaise with other projects** focusing on AAI to share know-how and best practices.

Authentication and Authorisation Infrastructure

Task	JRA1.1
Start	M3 (May)
End	M27
Total PMs	24.5

"Provide viable methods for authentication and authorisation (AA) in the EGI ecosystem, addressing current shortcomings"

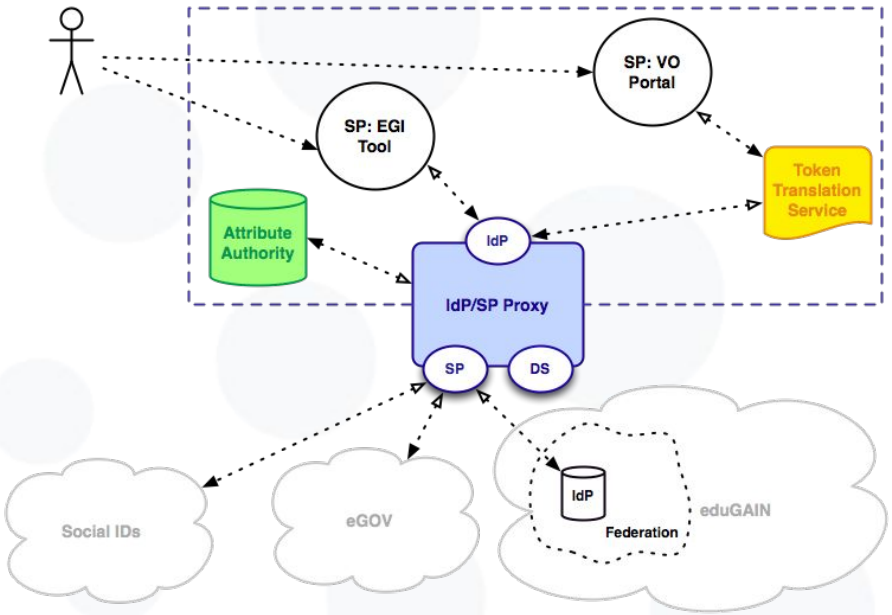
Partner	EGI.eu	CESNET	GRNET	NIKHEF	STFC
PM	7.5	4	7	4	2

Month	**Milestone - Deliverable**	**Title**
M16 Aug-2016	M3.4	Pilot services and best practices to enable federated AAI solutions released
M24 Feb-2017	D3.9	Identity Management for Distributed User Communities report

Roadmap

#	Task name	Start date	Release date
1.1	**Identification of and liaison with stakeholders** • WP3 F2F and EGI Conference ✓ • Liaise with AARC ✓ • Connections with GN4, EUDAT2020 and PRACE ✓ • Identification of initial set of tools ✓	**05/2015 (PM3)**	**06/2015 (PM4)**
1.2	**Requirements capturing** • Use FIM4R as the starting point and allign with AARC DJRA1.1 ✓ • Identify the most important use cases (CC) ✓ • Technical guidelines for enabling federated access in the initial set of tools ✓	**05/2015 (PM3)**	**08/2015 (PM6)**
1.3	**Technical architecture and pilot implementation** <u>Phase 1:</u> • Which AA services are needed ✓ • Design of the AAI Pilot Architecture ✓ • Pilot implementation Roadmap ✓ • Collaboration with the AAI pilot and the user portal activity for the LTOS ✓ • Pilot: Connection of the first set of EGI tools to the EGI IdP proxy ✓ <u>Phase 2:</u> • Expansion to EGI Tools and selected CCs ✓ • Interaction with SA2 (Training & User support) ✓ <u>Phase 3:</u> • Technology reassessment ✓ • Pilot services and best practices to enable federated AAI solutions released <u>Phase 4:</u> • Architecture and solution for the production EGI AAI services • Identity Management for Distributed User Communities report ✓	**09/2015 (PM7)**	**12/2015 (PM10)** **04/2016 (PM14)** **07/2016 (PM17)** **02/2017 (PM24)**

AAI Pilot & Architecture



- **Use case 0 - IdP/SP proxy**
- **Use case 1 - Attribute Authorities (Internal)**
  - Use case 1.1 - Perun
  - Use case 1.2 - GOCDB
- **Use case 2 - Token Translation**
  - Use case 2.1 - Token Translation with CILogon
  - Use case 2.2 - Token Translation with PUSP
- **Use case 3 - Hybrid stack SAML / OpenID Connect**

Pilot roadmap

Timeline	Expected Result
2015-Q4 **DONE**	EGI IdP/SP deployed (SimpleSAMLphp/OpenConext/COmanage)
2015-Q4 **DONE**	Interconnect the EGI IdP/SP with a SAML 2.0 IdP (EGI SSO & GRNET VHO)
2015-Q4 **DONE**	Interconnect the EGI IdP/SP with a SAML 2.0 SP
2015-Q4 **DONE**	Interconnect the EGI IdP/SP with Perun as attribute provider

Pilot roadmap

Timeline	Expected Result
2016–Q1 **DONE**	First pilot with EGI operational tools as SPs: - GOCDB - AppDB
2016-Q1 **DONE**	Add OIDC & OAUTH2 support to the EGI IdP/SP (for external identity providers)
2016-Q1 **DONE**	Enable support for logins using social IDs - Facebook (OAUTH2) - Google (OIDC) - LinkedIn (OAUTH2) - ORCID (OAUTH2)
2016-Q1 **DONE**	Deploy CILogon pilot service for X.509v3 certificates
2016-Q1 **DONE**	Deploy CILogon pilot service for PUSP

Pilot roadmap

Timeline	Expected Result
2016–Q1 **DONE**	Interconnect the EGI IdP/SP with GOCDB as attribute provider
2016–Q1 **DONE**	Interconnect the EGI IdP/SP with CILogon based Token Translation Services (x509v3)
2016–Q1 **DONE**	Interconnect the EGI IdP/SP with PUSPs based Token Translation Services

Development roadmap

Timeline	Expected Result
2016-Q2 **DONE**	User enrollment interface
2016-Q3 **DONE**	Support for account linking
2016-Q3 **DONE**	Support for OIDC services
~~**2016-Q3**~~ **2017-Q1** **IN PROGRESS**	Finalisation of user enrollment flows
~~**2016-Q3**~~ **2017-Q1** **IN PROGRESS** **(draft proposal)**	Finalisation of LoA mappings

Development roadmap

Timeline	Expected Result
~~2016-Q4~~ 2017-Q1 IN PROGRESS	Finalisation of OIDC client management UI (including token management for federated access to CLI tools/API clients)
2016–Q4 DONE	Entitlements for accessing services based on user's IdP metadata (e.g. REFEDS R&S, Sirtfi)
2017-Q1 IN PROGRESS	Mapping of user X.509 DN(s) to EGI UID in COmanage
2017-Q1 IN PROGRESS	Finalisation of VO membership information connectors
2017–Q1	Technology reassessment and definition of the roadmap until the end of the EGI-Engage project

Integration roadmap

Timeline	Expected Result
2016-Q2 **DONE**	Interconnection with ELIXIR IdP
2016-Q2 **DONE**	Integration with AppDB SP
2016-Q2 ~~**IN PROGRESS**~~ **DONE**	Integration with GGUS SP
2016-Q3 **DONE**	Integration with updated GOCDB AA REST API
~~**2016-Q4**~~ **2017-Q1** **DONE**	Integration with production RCauth.eu CA

Integration roadmap

Timeline	Expected Result
~~2016-Q4~~ 2017-Q1 IN PROGRESS	Interconnection with FedCloud SP
2016-Q3 DONE	Interconnection with DataHub SP
~~2017-Q1~~ 2017-Q2 IN PROGRESS	Interconnection with Operations Portal SP
2017-Q1 DONE	Interconnection with LToS (SP+AA)
2017-Q1 DONE(devel)	Interconnection with EPOS (SP)

Integration roadmap

Timeline	Expected Result
2017-Q1 **DONE(devel)**	Interconnection with EDISON Portal SP
2017-Q1 **DONE(devel)**	Interconnection with ARIA IdP
2017-Q1 ~~**IN PROGRESS**~~ **DONE(devel)**	Interconnection with EUDAT IdP
2017-Q1 ~~**IN PROGRESS**~~ **DONE(devel)**	Interconnection with EUDAT SPs (TBD)

Thank you for your attention.

Questions?

www.egi.eu