

EGI-Engage JRA1.1

Authentication and Authorisation Infrastructure

Christos Kanellopoulos
skanct@grnet.gr



- **TASK JRA1.1: Description and draft roadmap**
[30'] (Christos)
- **Current status of the EGI AAI**
[30'] (Peter)
- **AARC Project and links with EGI-Engage**
[30'] (Peter)
- **Discussion**
[30'] (All)

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

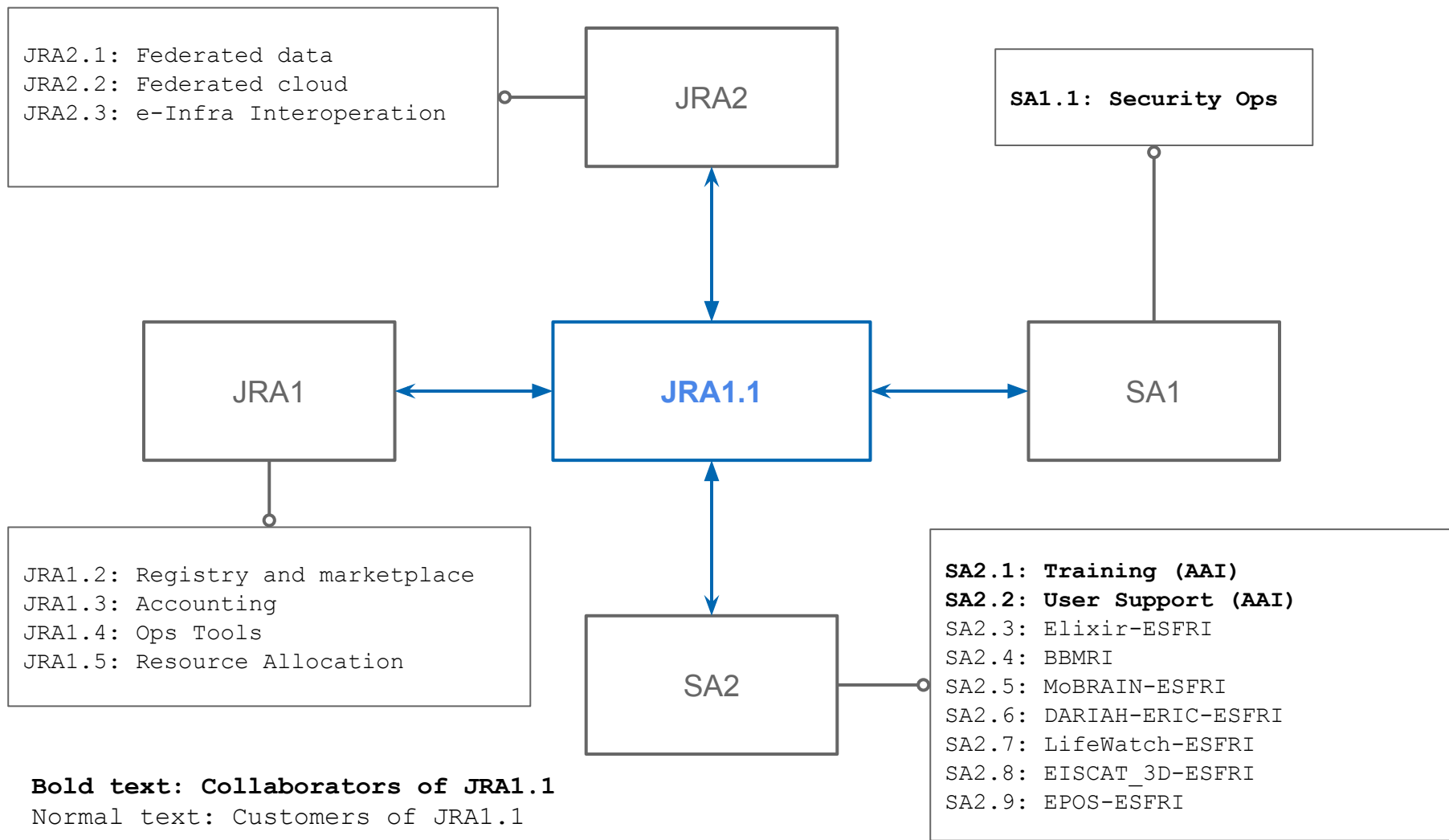
“The task will explore how to **integrate** suggested **AA methods** with current middleware and community services, guaranteeing a sufficient **Level of Assurance**, and the **use of credentials** issued by **other infrastructures** and services”

- Explore approaches to **easier safe management of user credentials**
 - For example, trusted stores.
- Identify possibilities and requirements for user authentication against both **web and non web-based applications**.
 - Develop a solution for authorisation, which will be based on information provided by VOs and/or additional sources. Validate the solutions via their integration with the middleware and services used by the community.
- Develop **authentication solutions for use cases**
 - identified among the requirements generated by the communities supported by the SA2 tasks, which will then provide guidelines for other typical EGI scenarios. The solutions can combine usage of multiple credentials for a user.
- Identify **user registration and management requirements** from a VO perspective
 - VO managers, infrastructure operations, and resource providers. Design a solution for user registration and management, which will cover current shortcomings.

- Explore current technical possibilities and the usability of existing infrastructures covering identity management
 - such as eduGain, eduRoam, or STORK and their large-scale combined usage.
- Investigate **alternative identity-vetting approaches** to current practices
 - such as the IGTF IOTA profile, reputation-based methods.
 - Evaluate changes in the existing policies.
 - Identify security risks and aspects affecting the secure operations of the developed solutions. Ensure that proper security mechanisms to ban users with immediate effect are available.
- **Engage with the CCs**, capture workflows and develop solution prototypes.
- **Liaise with other projects** focusing on AAI to share know-how and best practices.
 - E.g. AARC, GN4

Month	Milestone - Deliverable	Title
M04	M3.1	Operational tools development roadmap agreed
M16	M3.3	Operational tools development roadmap revised
M16	M3.4	Pilot services and best practices to enable federated AAI solutions released
M24	D3.9	Identity Management for Distributed User Communities report

Links with other EGI-Engage Activities



- AARC
- GN4
- EUDAT
- PRACE
- FIM4R

- STORK(?)
- Tryggve(?)

- ESFRI projects (through the CCs)

Task number	Task name	Start date	Release date	Dependencies
1.1	Identification of and liaison with stakeholders <ul style="list-style-type: none"> • WP3 F2F and EGI Conference • Liaise with AARC • Connections with GN4, EUDAT2020 and PRACE 	05/2015 (PM3)	06/2015 (PM4)	
1.2	Requirements capturing <ul style="list-style-type: none"> • Use FIM4R as the starting point • Align with AARC DJRA1.1 • Identify the most important use cases (CC) • Requirements from Tools 	05/2015 (PM3)	08/2015 (PM6)	1.1
1.3	Technical architecture and pilot implementation <u>Phase 1:</u> <ul style="list-style-type: none"> • Which AA services are needed • Pilot implementation for selected CC(s) (Interaction with SA2) • Pilot implementation for selected Tool(s) (Interaction with JRA1) <u>Phase 2:</u> <ul style="list-style-type: none"> • expansion to other CCs and Tools • Interaction with SA2 (Training & User support) 	09/2015 (PM7)	12/2015 (PM10) 04/2016 (PM14)	1.2
1.4	Technology reassessment	05/2016 (PM15)	07/2016 (PM17)	1.3

- Capture status of previous EGI AAI activities
 - Identification of stakeholders
 - Identify existing AA components
 - Identify existing workflows
- FIM4R Requirements
 - Which are most useful
 - Are there any other?
- Updated roadmap

Current status of the EGI AAI

AARC project and links with EGI-Engage

- **How do you register new users?**
- **How do you authenticate users?**
 - Local username/password | EGI SSO | X509 certificates | Federated IDs
- **Do you require non-web access?**
- **How do you authorise user access?**
 - No specific authorisation
 - Internal groups and roles
 - Based on the attributes received by the IdPs/VOs
 - Other?
- **Would you consider lower LoA authn mechanisms?**
 - E.g. authentication with social network IDs