AARC2 SA1 Pilot Intake WLCG

Use this intake form to describe a pilot the AARC2 SA1 team should devote their attention to.

Contact data of AARC participants involved

Please provide contact details for AARC2 participants involved in this pilot

	Name(s)
Submitter name + email:	Mario Reale, mario.reale@garr.it Kostas Koumantaros kkoum at grnet.gr
AARC SA1 Pilot name:	WLCG-Pilot
AARC SA1 Pilot subtask:	SA1.1
Technical contact(s) in AARC:	Mario Reale / GARR

Contact data of Parties involved

Please provide names and contact details for additional organisations involved in this pilot

Organisation Name	**Person names**	**Person email**	**Role within pilot**
CERN/WLCG	Hannah Short	hannah.short@cern.ch	Contact for WLCG
STFC	Dave Kelsey		
NIKHEF	Mischa Salle		
NIKHEF	David Groep		
Spherical Cow	Benn Oshrin		CoManage
GRNET	Nicolas Liampotis		EGI Checkin
INFN	Andrea Ceccanti		Indigo IAM

Pilot description

Please describe the high-level goal of pilot, provide an overview of the activities and participants. Please also describe how commitment from various partners is warranted. Relate the description to requirements identified in JRA1.

Our main aims are

- Enable WLCG VO membership registration with non-certificate credentials, both new users and existing (credentials should have sufficient LoA and be integrated with our identity vetting process)
- Enable (largely) transparent command line functionality for non-certificate users

The overall idea is that digital certificates would be kept behind the scenes, and W-LCG users would not have to bother with them.

Expertise on identifying necessary components and integrating them with our production systems. We would like to see a production ready pilot that could be deployed by a suitable party (likely hosted at CERN). The solution needs to be easily rolled out (i.e. minimising enhancement work required by each service)

Pilot goals

*Please describe the goals of pilot, including activities, participants, the community(ies) that require a solution. Describe **when the pilot is done and how to measure the success of it**, in a SMART way.*

The pilot has the main goal of demonstrating how WLCG services will be accessed by users authenticated and autorized via SAML, using federated credentials. In particular, registration of users on VOMS by means of SAML federated credentials is a key objective.

Another relevant goal is to provide command line access to WLCG services making use of non X.509 credentials (SAML, OIDC)...

Most of the components required for implementing a pilot reference infrastructure are ready and available, although some bits require further clarifications.

The pilot will demonstrate the required functionality by implementing 2 options to address the requirements: INDIGO IAM and EGI Checkin service + COmanage. The 2 solutions will be compared. A reference comparison table is available at https://docs.google.com/spreadsheets/d/1mC2U2H12RDHsOtk1OHQM3_HVbbflHfj-Y1Fv0yW_0KA/edit?usp=sharing

A) Specify which of the following BPA architectural components will be run in the pilot :

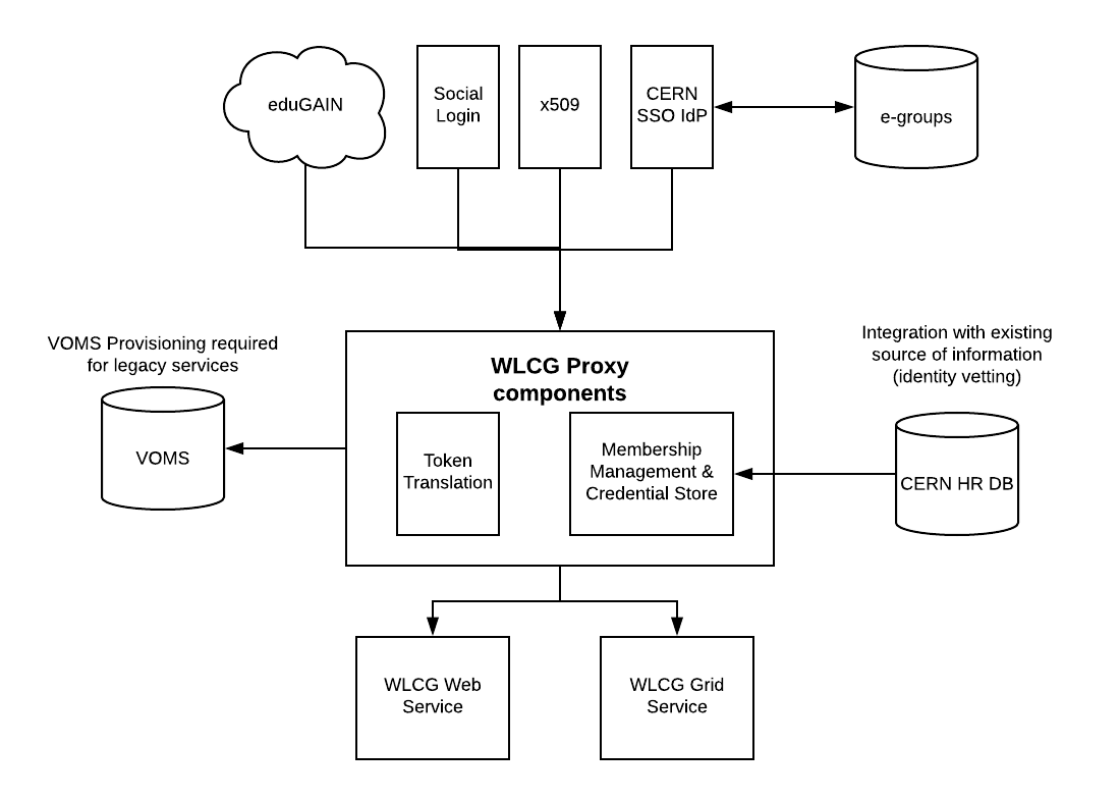
BPA architectural component	Have?	Need?	Product?	Description
Attribute Authority			IAM|CoManage	Must integrate with CERN's HR User Database and VOMS
Account linking tool			IAM|CoManage	
Group Management tool			IAM|CoManage	Aim is to replace VOMS Admin
CAS AuthZ tool				
Token translation service Credential translation			CILogon|WATTS|Master Portal & RCAuth	SAML to X.509 and to OAuth2 for future Grid Services (separate effort to define a JWT Schema across WLCG infrastructures)
Social ID plugin / gateway for AuthN				For LHC VOs (a subset of WLCG) it makes sense to use CERN SSO, but for others
eGov ID plugin / gateway for AuthN				
IDP/SP proxy			EGI Checkin|IAM	May wish to use CERN SSO as one IdP for LHC VOs and allow alternative login options. Ideally the solution will be generic, some WLCG VOs are not associated with CERN
Reputation Service				

B) Which of the following requirements and AAI features are of interest for you ?

BPA functional item / Requirement		Comment
1.User Friendliness	✔	
2.Homeless Users	✘	

3.Different Levels of Assurance	✅	Sirtfi required
4.Community Based AuthZ	✅	
5. Flexible and Scalable Attribute release policy	✅	
6. Attribute Aggregation	✅	
7. Account Linking	✅	
8.Open standards based technologies	❌	Not sure of the implications here
9. Persistent and Unique User Identifiers	✅	
10. User managed Identity Information	❌	
11. Up to date identity Information	✅	Link to CERN DB required for LHC VOs
12, Users groups and roles	✅	Pre-existing groups and roles in voms, must be maintained
13. Service Provider Friendliness	✅	
14. Step up authentication	❌	
15. Non browser (non web) based Fed access	✅	Legacy services rely on grid certificates but future services will likely rely on OAuth2. Solution should be flexible
16. Credential Delegation	✅	
16. Social Media Identities	❌	ORCID would be good. We need to continue to allow certificate based access for super users.
17. e-Government identies / Infrastructure	❌	
18. Effective resource usage accounting	✅	
19. Policy Harmonization	✅	Policies in place
20. Federated Incident Report Handling	✅	Capability in place
21. Sufficient Attribute Release	✅	R&S is OK
22. Awareness about R & E Federations	✅	OK
23. Semantically harmonized Identity Attributes	❌	

24. Simplified process for joining ID Federations	✅
25. Best practices for Terms and Conditions	❌



Technical details

A product translating from SAML to X.509 is CILogon, and could be used in this pilot.

INDIGO IAM could act as a OIDC client to the Master portal, get the certificate DN from RCAuth and provision it (user DN) into the VOMS server. Pre-provision of the user inside the VOMS is a crucial step to be clarified at this stage.

Possible Alternatives are COMANAGE and PERUN

On Master Portal there is the option to upload and SSH key, such that uses will be able to use CLI commands for WLCG.

Own infastructure

Do you have your own infrastructure? If yes, please indicate which elements of the AARC Blueprint Architecture you (intend) to run yourself.

Yes, WLCG has a production certificate based infrastructure in place and we intend to support the future iteration. Service maintenance is typically split across WLCG participants, including CERN.

e-Infrastructure

Do you (intend) to use an e-Infrastructure provider (e.g. EGI, EUDAT)? If yes, please indicate which and what you expect of them.

We use EGI for back end grid services (VMs for processing and storing data), as well as OSG and other small grid infrastructures

Pilot resources

Please describe required resources for the pilot, including VMs, DNS and certificates. Need for piloting in eduGAIN policy framework?

We need people with expertise to set the components up in a way that they can be supported and maintained by WLCG in the future as required

Sustainability

When this pilot is completed, do you intend to continue using the solution? If yes, can you describe how you intent to sustain it? (E.g. through own staff, by using an e-Infrastructure provider, ...)

Yes, through the WLCG Participants

Contact data

Date	Activity	Owner	Minutes
January 1, 2017	Kickoff meeting		

Documents:

(Attach any documents to this page to get them listed.)

- https://hshort.web.cern.ch/presentations/20170220%20FIM4R%20WLCG%20Update.pdf
- https://hshort.web.cern.ch/presentations/20171123-WLCG-Pilots.pdf
- https://hshort.web.cern.ch/presentations/20160928%20DI4R%20Enabling%20Federated%20Login%20to%20WLCG.pdf
- **https://hshort.web.cern.ch/presentations/20161010%20CHEP%20Enabling%20Federated%20Access%20for%20HEP.pdf**

Minutes:

(Attach sub pages to this page to get them listed.)

Q&A

Open Questions for discussion (external discussion or with other sub-tasks within AARC)

- ...?