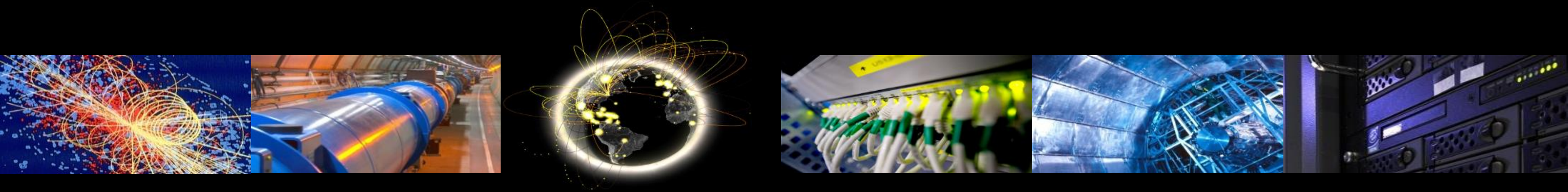
WLCG AuthZ WG – pre-GDB Summary

GDB

December 12th, 2018



WLCG
Worldwide LHC Computing Grid

CERN

Pre-GDB

- 18 Attendees
- Assessed the two Pilots
- Heard an update from DOMA
- Made important progress on the JWT Schema

WLCG AuthZ WG

- Current major users of tokens in HEP
  - INDIGO IAM
  - EGI Check-in
  - SciTokens
  - dCache
  - ALICE
- Pilot projects supported by AARC EOSC-hub EOSCpilot The European Open Science Cloud for Research Pilot Project
- Priority to stick to industry and R&E standards wherever possible
- Bi-monthly calls & 3 pre-GDBs since July 2017

Status

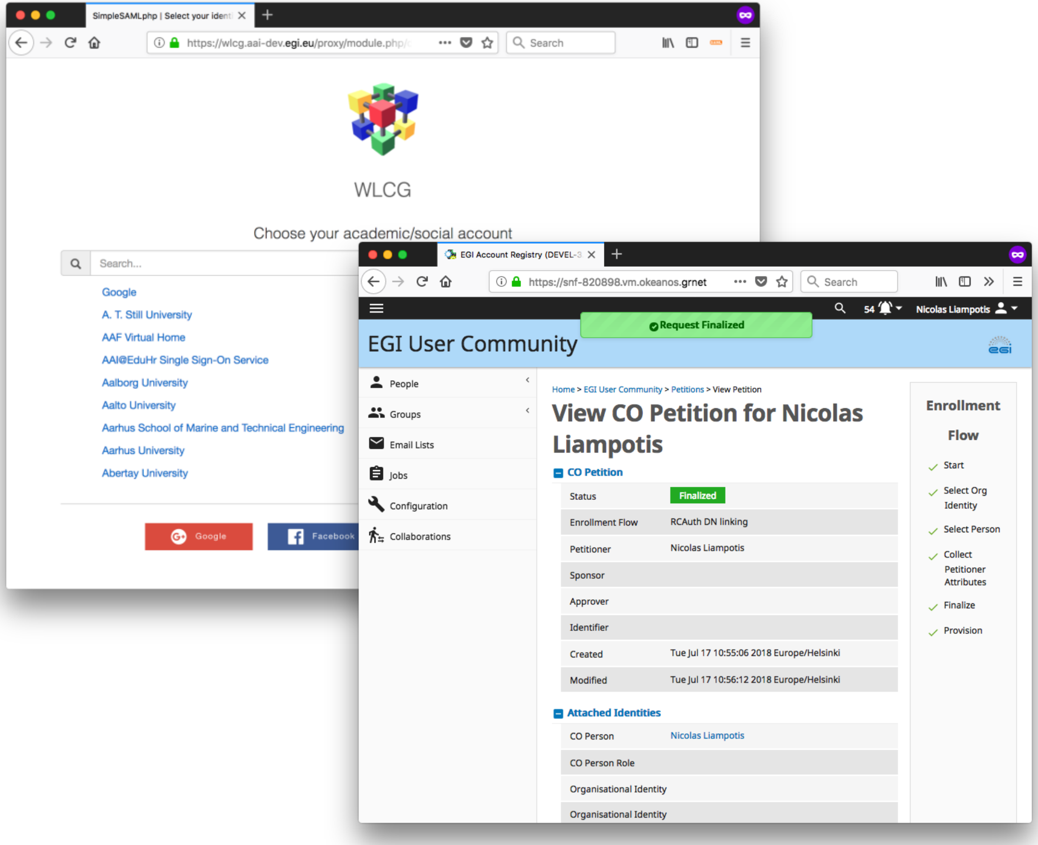
Step	Result	Status	Due/Completed
Create group of relevant people able to influence WLCG and make changes	WLCG AuthZ WG	Done	July 2017
Collect Requirements	Document completed and revised	Done	July 2018
Identify Pilot Options	EGI Check-in + COManage (EOSC-hub/AARC), INDIGO-IAM (EOSC)	Done	November 2017
Identify Certificate Authority for token translation	RCAuth.eu	Done	July 2018
CERN HR Identity Vetting integration	Must be on site, Privacy Statement approved, DB connected	In Progress	November 2018
Define JWT Schema for tokens (capability based & group based)	Converging and ironing out details	In Progress	December 2018
Enhance Pilot Options to match requirements	Significant progress made	In Progress	December 2018
Interview experiments to match proposal to workflows	Questionnaire sent and completed for 3 LHC VOs (1 in progress)	In Progress	November 2018
Assess Pilots	Pre-GDB held. Pilots assessed I their current state	Done	December 2018
Provide Recommendation to WLCG Management Board		Not Started	February 2019

Pilot Progress

Summary

- Both solutions backwards compatible
- HR DB functionality encompassed in separate API, mock instance hosted at CERN ready for integration with new HR DB view (thank you, Andrea Ceccanti!)
- Both pilots have battled CERN's cloud infrastructure quirks, causing certain delays
- Further discussion required regarding using CERN's authentication infrastructure
  - Deploying RCAuth behind CERN SSO
  - Relying on PersonID from CERN SSO
- Need more guidance on which "bulk actions" are desired

EGI-Check-in


SimpleSAMLphp | Select your ident
https://wlcg.aai-dev.egi.eu/proxy/module.php/
Search
WLCG
Search...
Google
Facebook
EGI Account Registry (DEVEL-3
https://snf-820898.vm.okeanos.grnet
Search
54
Nicolas Liampotis
People
Groups
Email Lists
Jobs
Configuration
Collaborations

Choose your academic/social account

Google
A. T. Still University
AAF Virtual Home
AAI@EduHr Single Sign-On Service
Aalborg University
Aalto University
Aarhus School of Marine and Technical Engineering
Aarhus University
Abertay University

Request Finalized

EGI User Community

Home > EGI User Community > Petitions > View Petition

View CO Petition for Nicolas Liampotis

CO Petition

Status	Finalized
Enrollment Flow	RCAuth DN linking
Petitioner	Nicolas Liampotis
Sponsor	
Approver	
Identifier	
Created	Tue Jul 17 10:55:06 2018 Europe/Helsinki
Modified	Tue Jul 17 10:56:12 2018 Europe/Helsinki

Attached Identities

CO Person	Nicolas Liampotis
CO Person Role	
Organisational Identity	
Organisational Identity	

Enrollment Flow

- ✓ Start
- ✓ Select Org Identity
- ✓ Select Person
- ✓ Collect Petitioner Attributes
- ✓ Finalize
- ✓ Provision

Done

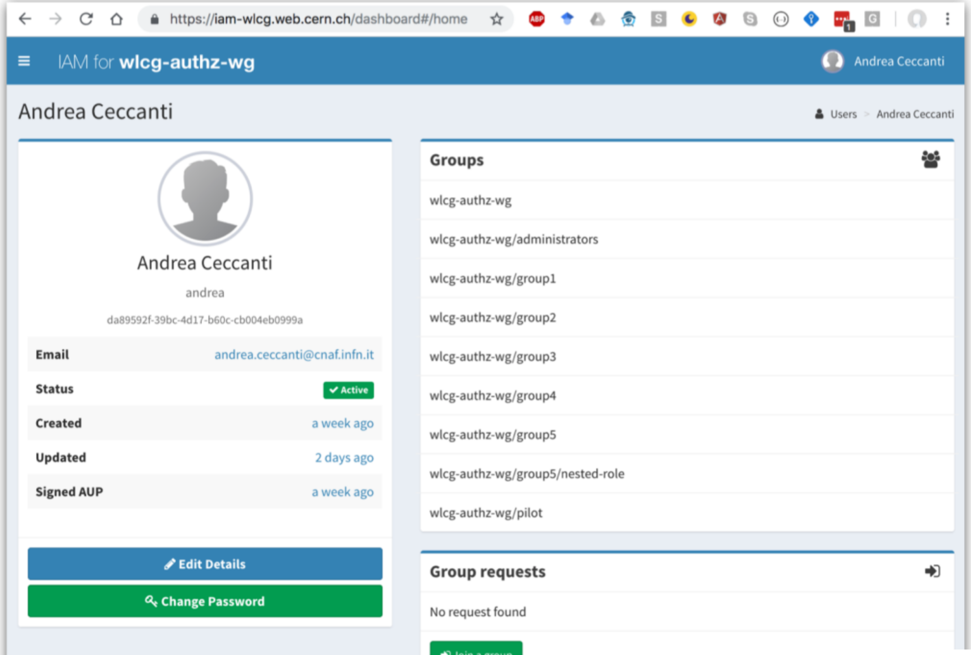
- User Enrollment
- Active role selection (via groups)
- VOMS provisioning

Pending

- Configure VO flows
- Complete pilot deployment
- CERN SSO
- RCAuth Integration
- HR DB integration through API

WLCG
Worldwide LHC Computing Grid

INDIGO IAM



https://iam-wlcg.web.cern.ch/dashboard#/home

IAM for **wlcg-authz-wg**

Andrea Ceccanti

Andrea Ceccanti

Users > Andrea Ceccanti

Andrea Ceccanti

andrea

da89592f-39bc-4d17-b60c-cb004eb0999a

Email	andrea.ceccanti@cnaf.infn.it
Status	✓ Active
Created	a week ago
Updated	2 days ago
Signed AUP	a week ago

Groups

- wlcg-authz-wg
- wlcg-authz-wg/administrators
- wlcg-authz-wg/group1
- wlcg-authz-wg/group2
- wlcg-authz-wg/group3
- wlcg-authz-wg/group4
- wlcg-authz-wg/group5
- wlcg-authz-wg/group5/nested-role
- wlcg-authz-wg/pilot

Group requests

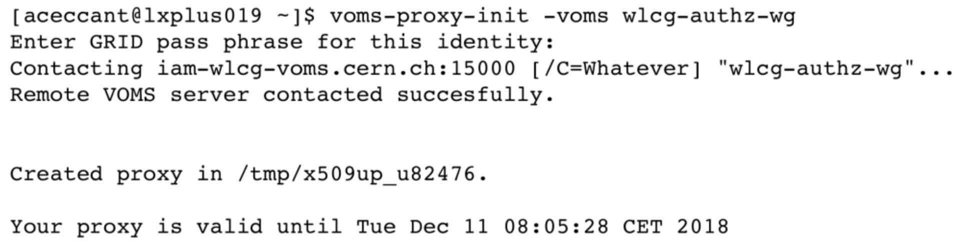
No request found

Done

- User Enrollment
- CERN SSO
- VOMS Provisioning including role selection (user has X509 cert)
- HR DB integration (currently mock data)

Pending

- RCAuth Integration
- HR DB with new DB view



```
[aceccant@lxplus019 ~]$ voms-proxy-init -voms wlcg-authz-wg
Enter GRID pass phrase for this identity:
Contacting iam-wlcg-voms.cern.ch:15000 [/C=Whatever] "wlcg-authz-wg"...
Remote VOMS server contacted succesfully.


Created proxy in /tmp/x509up_u82476.

Your proxy is valid until Tue Dec 11 08:05:28 CET 2018
```

JWT Schema

- Document has been significantly restructured to a clearer format
- Many of the trust and security aspects are now well understood
- Convergence that tokens will primarily be provisioned over OIDC (comments welcome!)

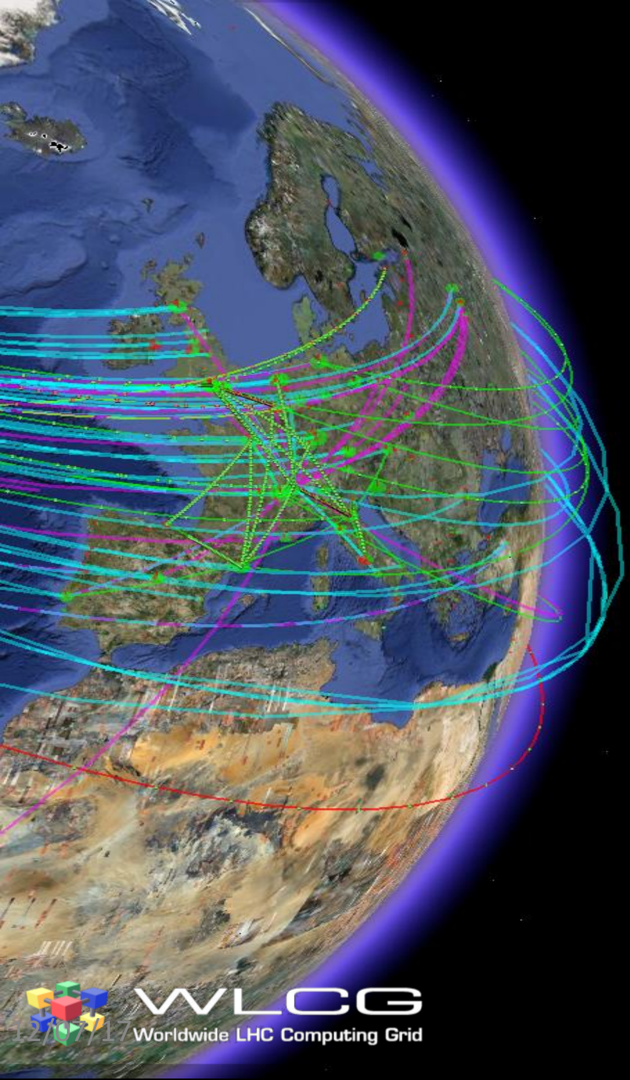
Next Steps

- Complete JWT Document
- Call with VOs tomorrow (second in January)
- Provide recommendations to WLCG Management Board

All information at https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

Q for GDB

- Do all VO members have a CERN account?



Questions?