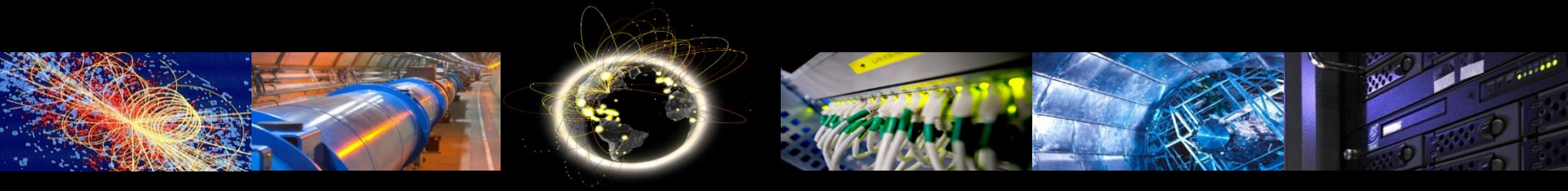
WLCG AuthZ WG – Update

GDB

March 13th 2019



WLCG
Worldwide LHC Computing Grid

CERN

WLCG AuthZ WG

- Current major users of tokens in HEP
  - INDIGO IAM
  - EGI Check-in
  - SciTokens
  - dCache
  - ALICE
- Pilot projects supported by
- Priority to stick to industry and R&E standards wherever possible
- Bi-monthly calls & 3 pre-GDBs since July 2017

What are we doing?

- Removing the need for researchers to manage x509 certificates
- Enabling token based authorisation (linked to DOMA work)
- Replacing VOMS-Admin

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. API layer developed by Andrea	Done	February 2019
Define JWT Schema for tokens (capability based & group based)	Converging and ironing out details	In Progress	April 2019
Enhance Pilot Options to match requirements	Pilots presented on March 5th	Done	March 2019
Interview experiments to match proposal to workflows	Questionnaire sent and completed for 3 LHC VOs (1 in progress)	Done	December 2018
Pilot progress review	Pre-GDB held. Pilots assessed their current state	Done	December 2018
Provide Recommendation to WLCG Management Board		Not Started	March/April 2019

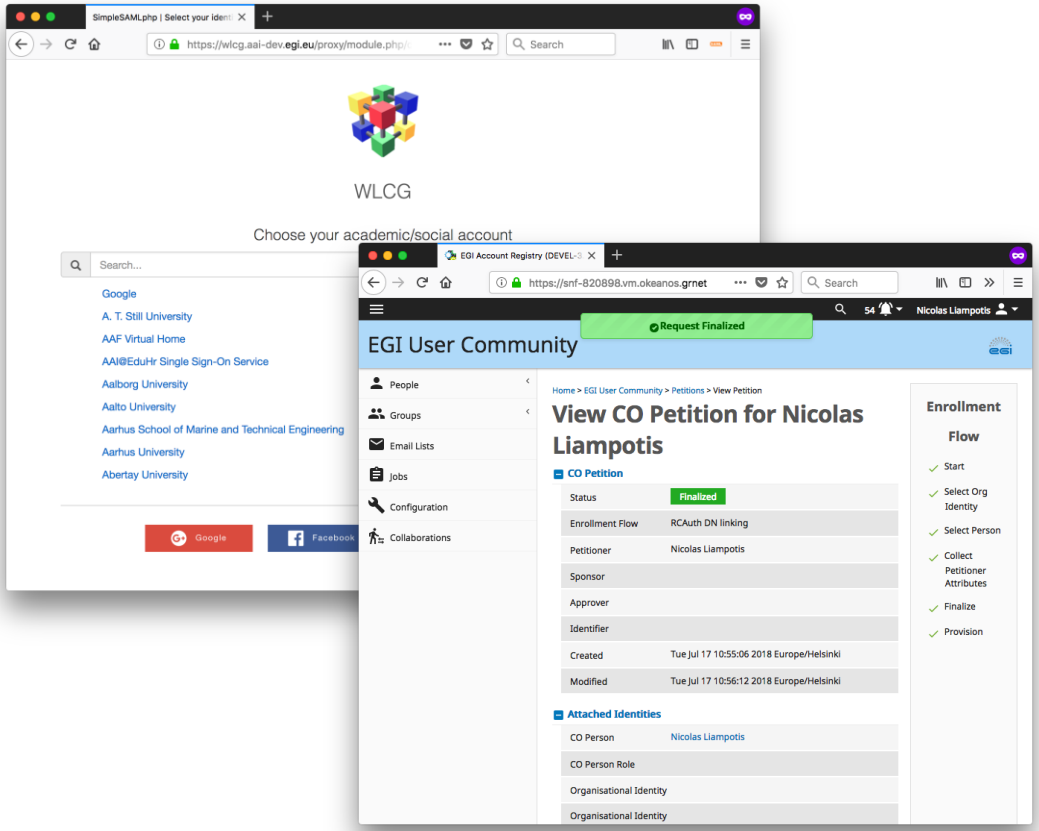
AAI Pilot Progress

Summary

- Both solutions
  - Are backwards compatible (i.e. VOMS provisioning)
  - Fulfill 90% of the Identified Requirements [1] (exception being 2FA that can be handled at the CERN SSO layer for LHC VOs)
  - Integrate IOTA Certificates from RCAuth.eu
  - Sustainability statements

[1] https://twiki.cern.ch/twiki/bin/viewauth/LCG/WLCGAuthorizationWG

EGI-Check-in



Advantages

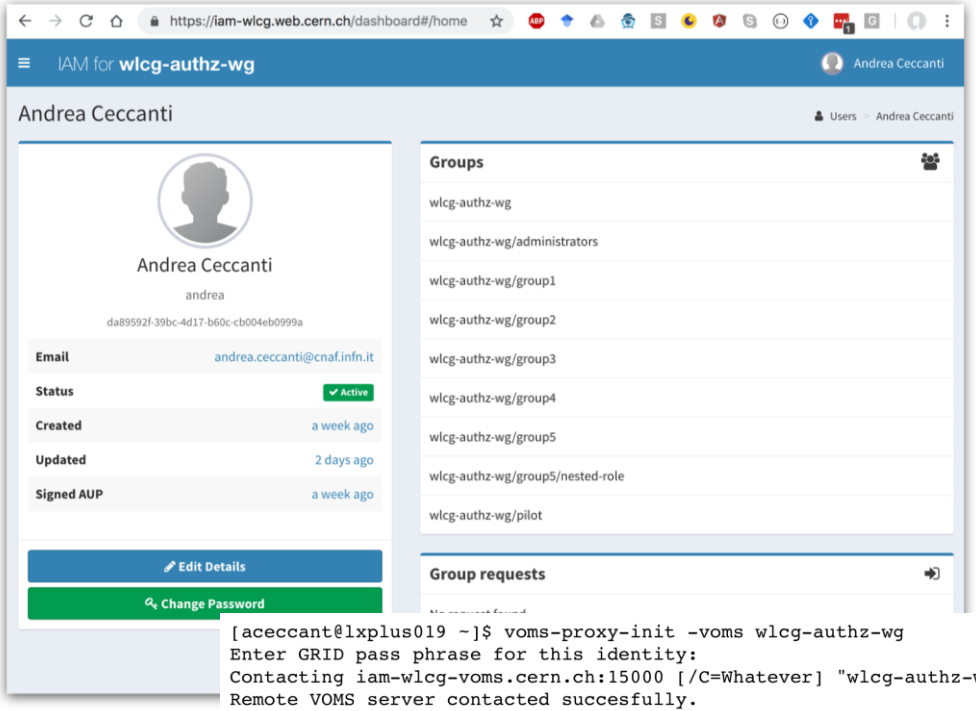
- Components in common usage (COManage, SimpleSamlPhP)

Disadvantages

- User friendliness
- Complexity
- Many components, deployment considerations

WLCG Worldwide LHC Computing Grid

INDIGO IAM




```
[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
```

Advantages

- User friendliness, particularly RCAuth integration and command line flow
- Ease of deployment

Disadvantages

- Fewer users
- Ongoing HR DB synch not yet implemented (but implementation path understood)

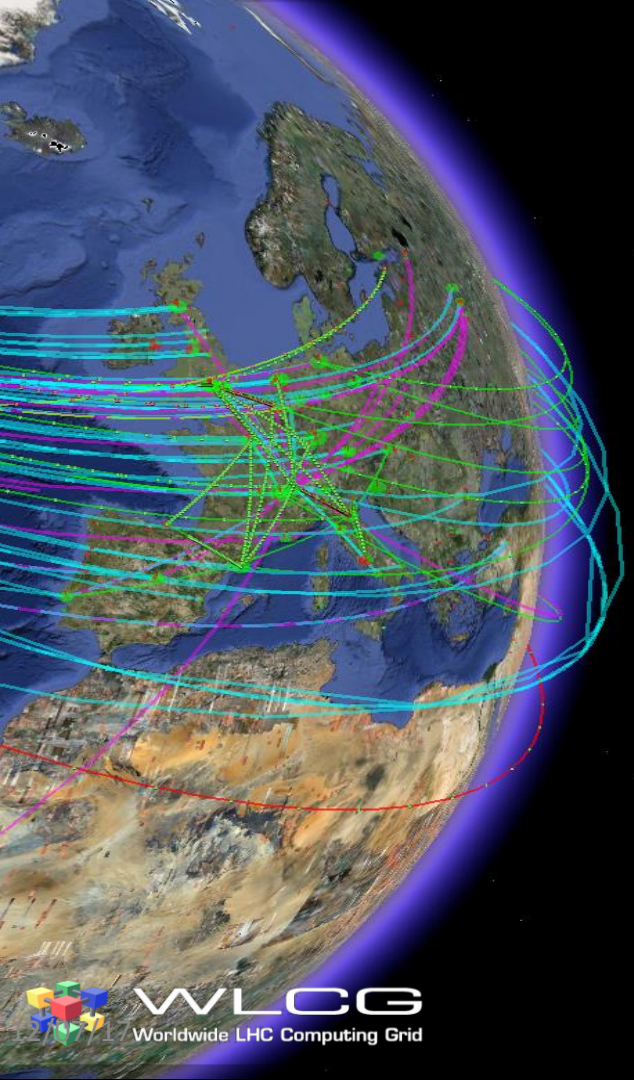
JWT Schema

- 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
- Work required to finalise token content
  - Bi-weekly calls scheduled

Next Steps

- Complete JWT Document
- Provide feedback to WLCG Management Board
- Deployment considerations
  - Assurance profiles for LHC VOs
  - Policies regarding Attribute Authority operations

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



Questions?