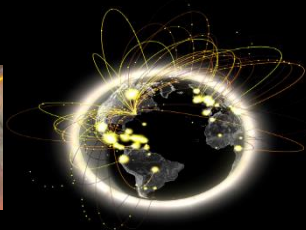


WLCG AuthZ WG

pre-GDB Summary

GDB, July 18th 2018

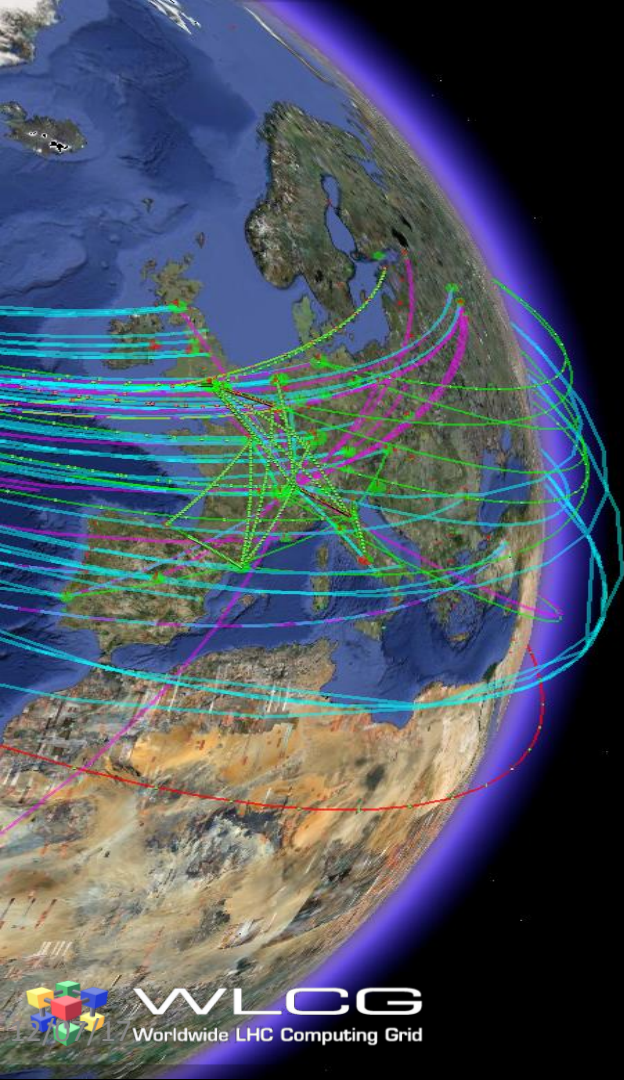


Agenda

- WG Background
- Activities
- Next Steps

Disclaimer: I made this deck to summarise our progress in the pre-GDB yesterday. Any errors are purely mine!

WG Background



Motivation

- Evolving Identity Landscape
 - User-owned x.509 certificates -> federated identities
 - Current grid middleware does not support federated identities
 - How can we shield users from the complexities of X.509 certificate management ?
 - Token-based (JWT) authorization widely adopted in commercial services and increasingly by R&E Infrastructures
- Data Protection
 - Tightening of data protection (GDPR) requires fine-grained user level access control, certain provisioning practices may need to be adjusted










Objective: Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments

Timeline

Face-to-Face Meetings

- July 26 2017 <https://indico.cern.ch/event/656027/>  Kickoff meeting, GDB
- November 2017 <https://indico.cern.ch/event/578976/>  pre-GDB, Requirements Gathering
- March 28 2018 WLCG Workshop <https://indico.cern.ch/event/658060/> 
- July 17 2018 pre-GDB <https://indico.cern.ch/event/651343/> 

Video-Conference Meetings

- September 2017 <https://indico.cern.ch/event/669715/> 
- October 2017 <https://indico.cern.ch/event/670330/> 
- December 6th 2017 JWT <https://indico.cern.ch/event/684620/> 
- December 14th 2017 AAI Pilot Projects <https://indico.cern.ch/event/680452/>  Indigo IAM and EGI Checkin demos
- January 26th 2018 AAI Pilot Projects <https://indico.cern.ch/event/696286/>  Demo assessments
- February 15th 2018 JWT <https://indico.cern.ch/event/704478/> 
- February 21st 2018 AAI Pilot Projects <https://indico.cern.ch/event/706302/>  CRIC Authorization Workflow & AARC Pilots plan
- March 15th 2018 JWT <https://indico.cern.ch/event/710409/> 
- March 19th 2018 AAI Pilot Projects <https://indico.cern.ch/event/712343/> 
- April 10th 2018 JWT <https://indico.cern.ch/event/719148/> 
- April 26th 2018 AAI Pilot Projects <https://indico.cern.ch/event/719155/> 
- May 7th 2018 JWT <https://indico.cern.ch/event/725955/> 
- May 28th 2018 AAI Pilot Projects <https://indico.cern.ch/event/731164/>  [SciTokens](#) and Condor
- June 6th 2018 JWT <https://indico.cern.ch/event/734316/> 
- June 20th 2018 WLCG [AuthZ](#) <https://indico.cern.ch/event/737125/> 
- July 4th 2018 JWT <https://indico.cern.ch/event/739090/> 

<https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG>

Outputs

Catalogue of JWT usage in Infrastructures

- Final changes pending

WLCG Authorisation Requirements

- Ready for comment

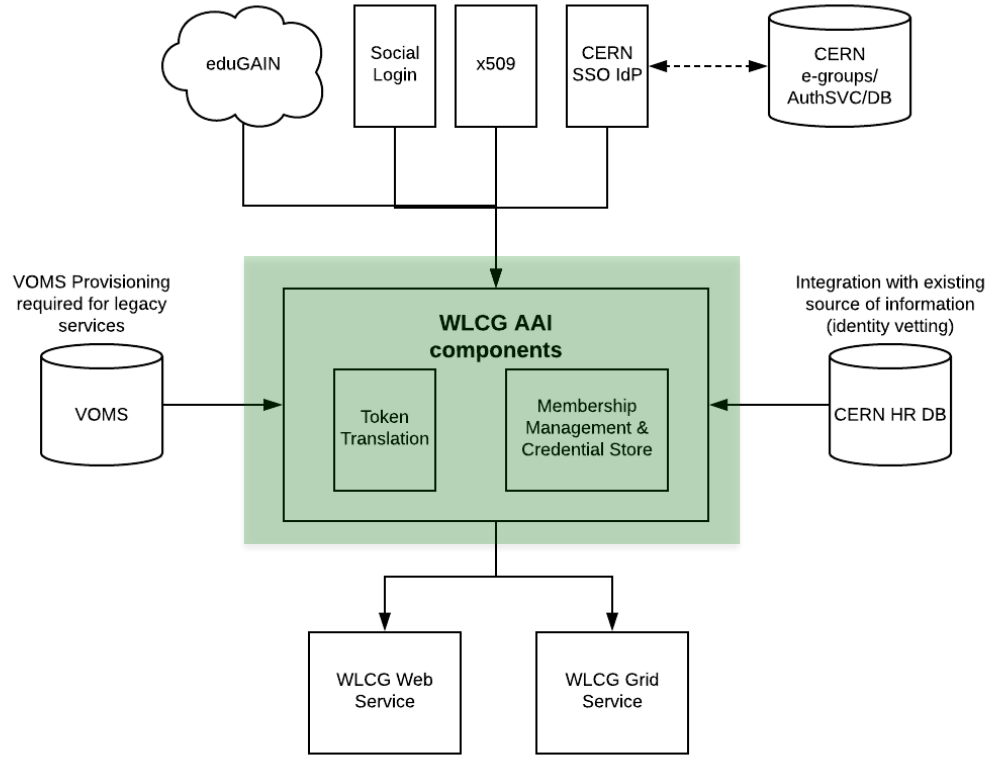
WLCG Common JWT Profiles

- Ongoing

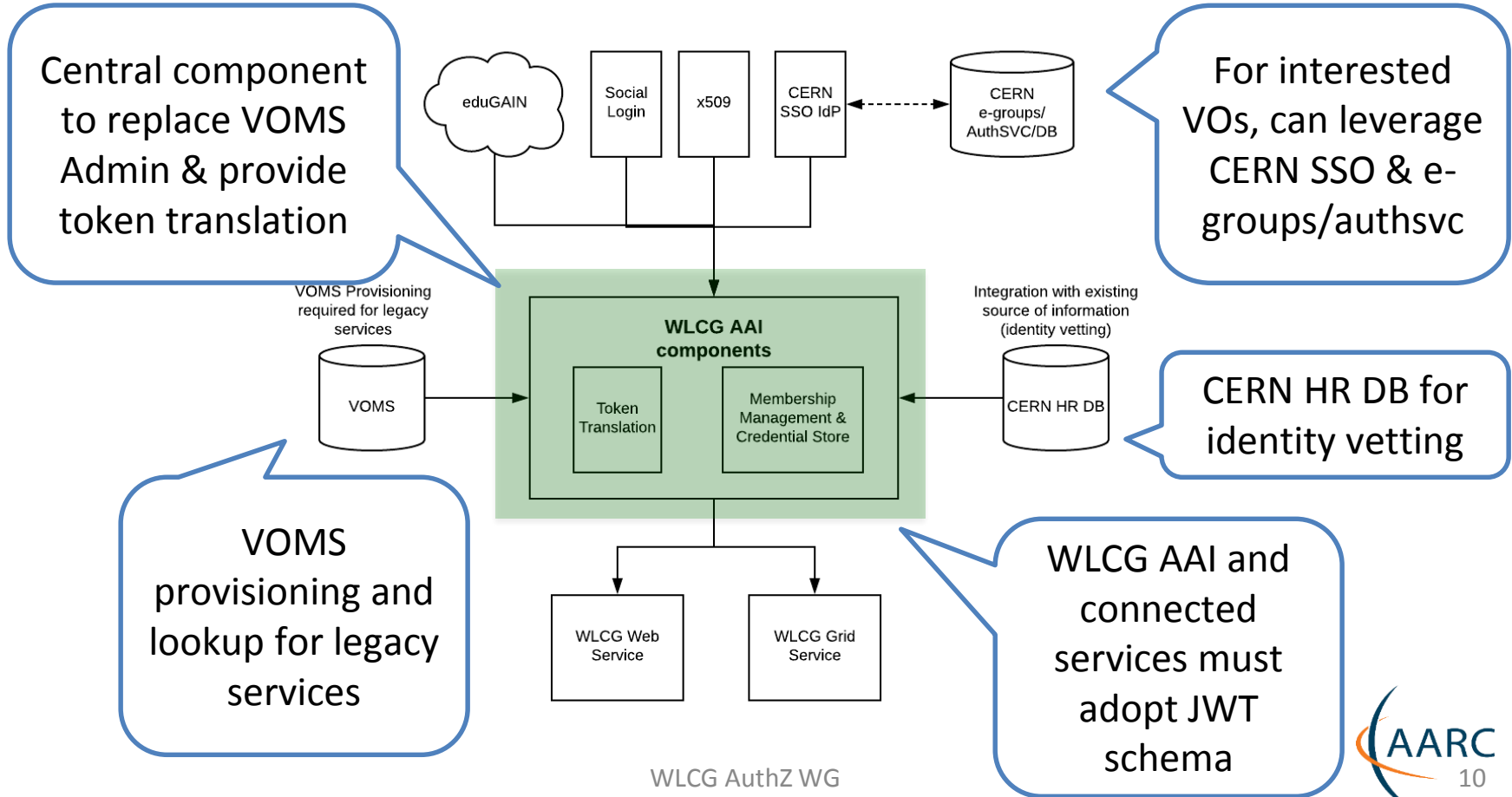
WLCG AAI Pilot Development

- Ongoing

AAI Pilot Projects



AAI Pilot Projects





Catalogue of Token Use

JWT Catalogue

- Objective: document existing use and identify best options for WLCG
- ALICE, dcache, EGI, INDIGO-Datacloud, SciTokens, input from XACML
- Final tweaks ongoing (updating to current status)

JWT use within the Community

Authors: M Martinez Pedreira, M Litmaath, P Millar, A Ceccanti, M Sallé, B Bockelman, H Short, N Liampotis

This document describes the current use of authorization tokens in projects of interest to the WLCG community. From here we aim to identify key functionality and best practices to contribute to the development of a shared JWT profile that is interoperable across infrastructures participating in WLCG. The proposed profile should be widely circulated and undergo a period of community consultation.

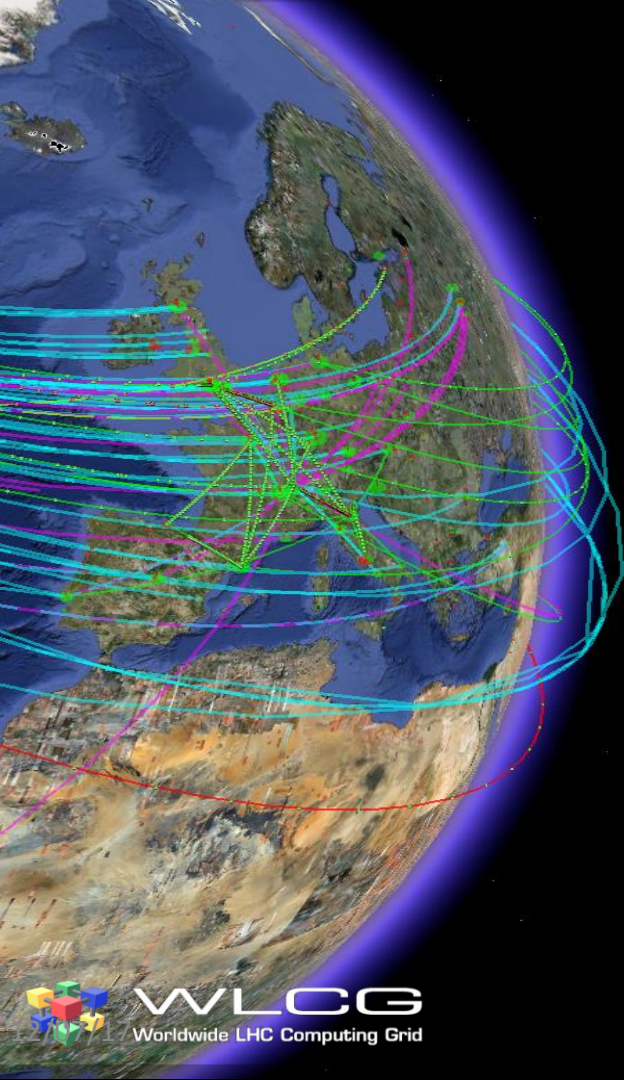
Use Cases	2
ALICE	2
dCache macaroons	4
The root caveat	5
The home caveat	6
The path caveat	6
The before caveat	6
The ip caveat	6
The activity caveat	6
Obtaining a macaroon	7
Using a macaroon	7
EGI	8
Entitlements	8
Resource-specific entitlements	9
Entitlements expressing VO/group membership and role information	9
Level of Assurance	9
INDIGO-Datacloud AAI and Identity and Access Management	10
SciTokens	11
Input from the AuthZ Interop WG (XACML attributes)	13
Comparison Table	14
Summary	15
References	15



Authorisation Requirements

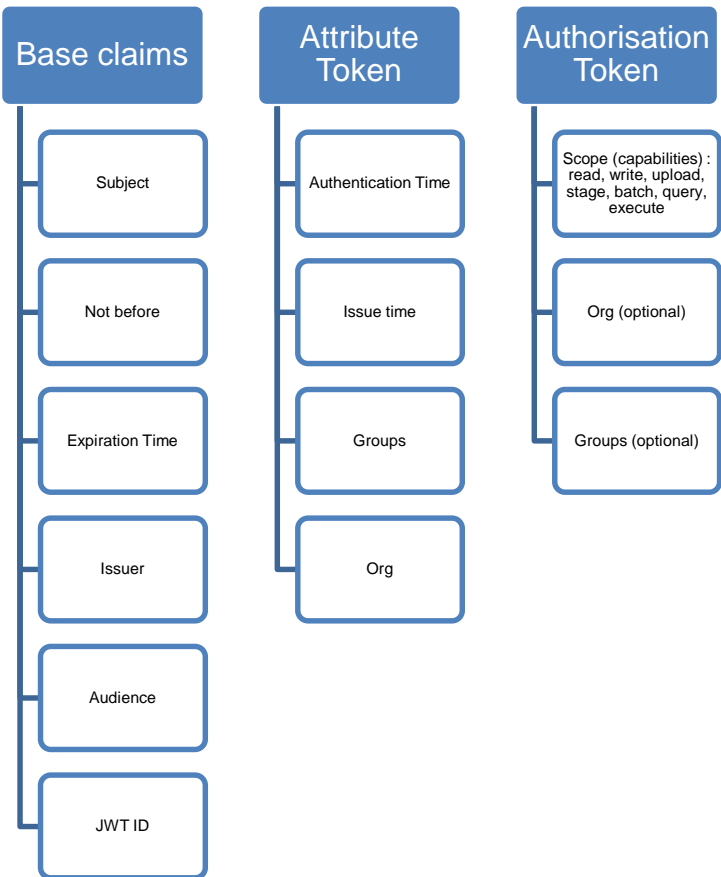
WLCG AuthZ Requirements

- VO Membership Management
 - Attributes? VO ID, ID of credential, Name, Email, Authorization
 - Support multiple federated credentials & their linkage
 - Active role selection (or equivalent)
 - Token management achievable by the standard user
- Service Requirements
 - Attributes? Authorization plus traceability (+ optional Groups/Roles) || Groups/Roles
 - Ease of implementation
 - Use standard approaches
 - Token integrity and validity verifiable
 - Without connecting to the issuer
 - For non-web, users should not have to manage identities in addition to their login session
- General
 - Support for fine grained suspension by sites, infrastructure and VOs
 - Smooth transition from current X509-based to token-based AAI



WLCG JWT Profiles

WLCG JWT Profiles



```
{
  "ver": 1,
  "sub": "e1eb758b-b73c-4761-bfff-
adc793da409c",
  "iss": "https://cms.wlcg.example",
  "groups": ["/cms/VO-Admin", "/cms",
"/cms/itcms" ],
  "preferred_username": "Researcher",
  "org": "cms",
  "nonce": "334b0e05b65a3",
  "aud": "cms-test-client",
  "auth_time": 1523363636,
  "name": "Researcher 26",
  "exp": 1523365436,
  "iat": 1523363636,
  "jti": "aef94c8c-0fea-490f-9027-
ff444dd66d8c",
  "email": "researcher26@cern.ch"
}
```

Example Attribute Token

WLCG JWT Profiles

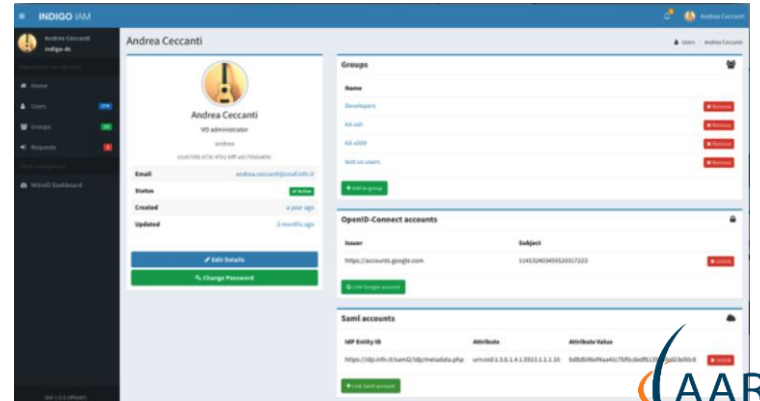
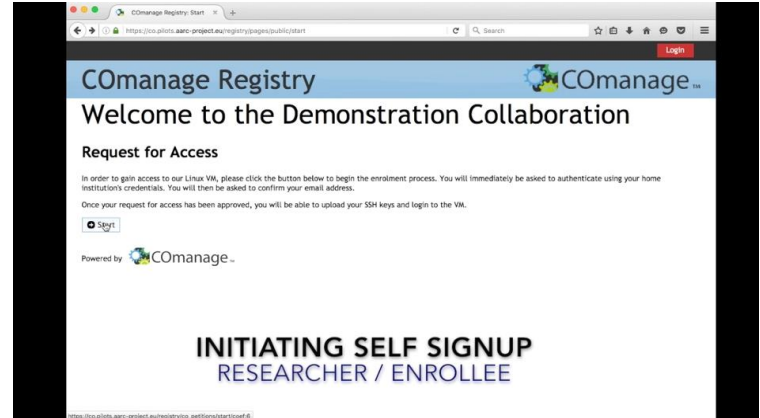
- Next steps
 - Check alignment with common practices (AARC, REFEDS) for e.g. claim names, syntax
 - Define recommended token lifetimes
 - ... still quite a lot to do here!



WLCG AAI Pilots

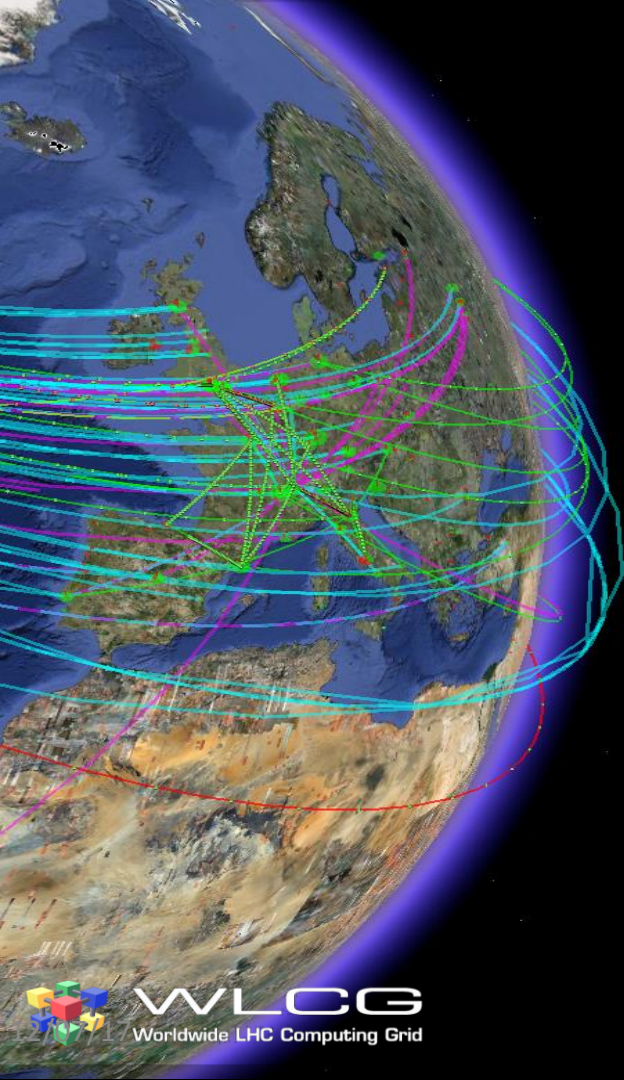
AAI Pilot Projects

- Two solutions appear to meet the majority of requirements
 - EGI Check-in & CManage
 - INDIGO IAM
- Additional integration required for
 - VOMS provisioning & lookup
 - CERN HR DB integration (postponed until autumn)
 - AUP re-signing
- RCAuth.eu for x509 generation
 - High availability setup in progress



AAI Pilot Projects

- Aim: provide the WLCG MB with hands-on feedback on two possible solutions capable of taking the first step towards X509-free WLCG
 - Both approaches require additional developments
 - Both strategies will have to ensure sustainability of these developments in the forthcoming years
- Proposed timeline
 - Finalization of new required developments for EGI Check-in, COmanage and INDIGO IAM: **March-July 2018**
 - Deployment and pilot testing **August-September 2018**
 - Reporting / Benchmarking: **October-December 2018**
 - Final dissemination on pilot: **January-March 2019**



Next Steps

Comment on Requirements

- Please take a look!
- This represents the view of the WG, iterated over 9 months

WLCG Authorisation Requirements

This document includes requirements for authorisation for WLCG as agreed within the WLCG AuthZ Working Group. It aims to record specific needs in the context of token based authorisation. An initial set of Requirements was gathered in November 2017 and updated in July 2018.

Contributors: H. Short, A. Ceccanti, M. Sallé, N. Liampotis, B. Bockelman, R. Wartel, V. Brillault, M. Litmath

Endorsers (agreement with the requirements expressed here): Hannah Short, Andrea Ceccanti, Mischa Sallé, Nicolas Liampotis, Brian Bockelman

WLCG Authorisation Requirements	1
VO Membership Management	2
VO Membership Management Overview	2
Required User Attributes (for the VO to operate)	2
User Credential types (i.e. Authentication, not server-server auth tokens)	2
Assurance profiles for home organisations/credential authorities (See WLCG Policy on Acceptable Authentication Assurance and AARC Guidelines)	3
Token provisioning workflow	3
Usability	3
Service Providers	3
Service Requirements Overview	3
Required User Attributes (for the services to operate)	4
Non-web	4
General	4
Operational Requirements	4
Change Management	4
References:	5
Appendix	5
Cataloguing Existing Support	5

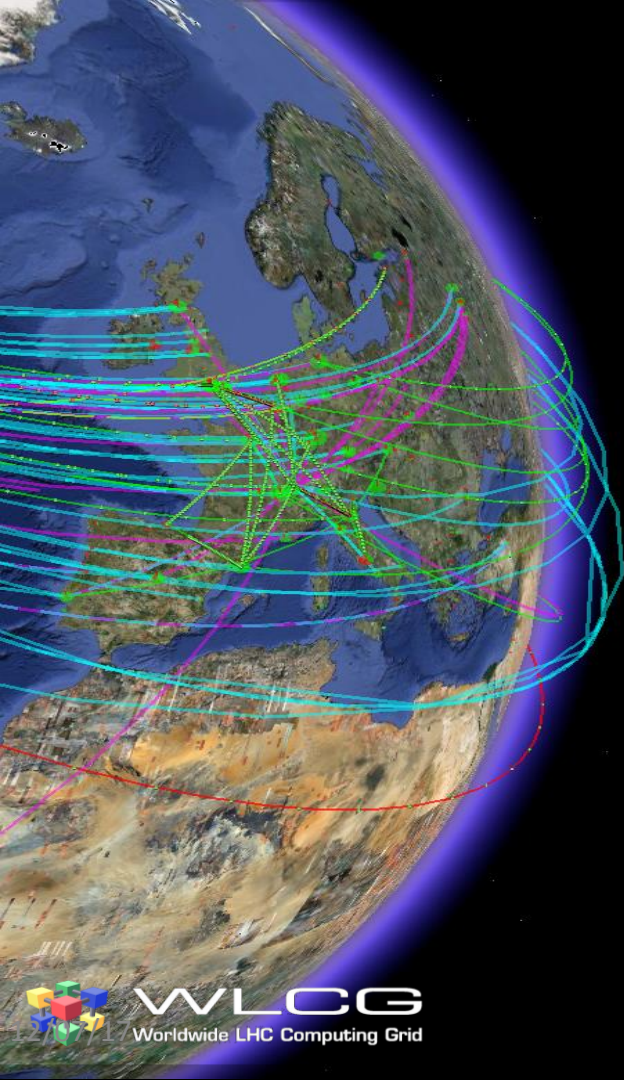
Experiment Interviews

- We have a pretty good idea of the technology stack
- We don't know the experiment workflows (as well as you!)
- Would like to have individual interview meetings with each experiment to
 - Present our ideas for future authorisation
 - Understand how they could fit with your workflows
 - Get a first estimate of a transition plan (if you see value in the new authorisation system!)

JWT Workflow (?)

1. Job submitted with access token and refresh token
2. Access token verified as job executed
3. Access token expires
4. Once job concludes, refresh token used to generate a new access token for returning the output

*This could be (and probably is) completely wrong!
How do you see tokens fitting into experiment workflows?*



Questions?