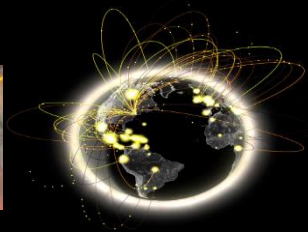


WLCG AuthZ WG

pre-GDB

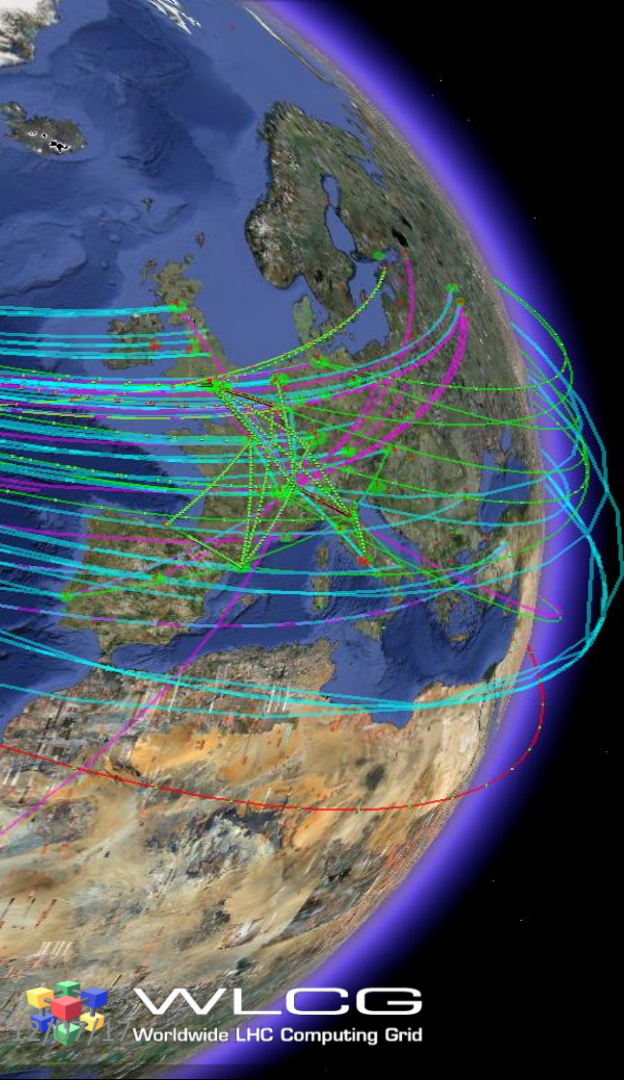
July 17th 2018



Agenda

- WG background
- Activities
 - JWT Schema
 - AAI Pilot Projects
- Next steps

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 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>

WLCG AuthZ Requirements

- VO Membership Management
 - Attributes? VO ID, ID of credential, Name, Email, Authorization
 - Support multiple federated credentials & their linkage
 - Active role selection
 - Token management achievable by the standard user
- Service Requirements
 - Attributes? Authorization plus traceability || 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

Splitting things more into “identity based” and “authorization based” approaches. Third-party services (e.g. storage) would primarily consume the latter.



WG Activities

WLCG AuthZ WG Activities

- Two separate activities were identified during the pre-GDB
 - Design and testing of WLCG Membership Management and Token Translation services (AAI Pilot Projects)
 - Definition of a JSON Web Token (JWT) profile for authentication and authorization for WLCG services and token issuers
 - See the [SciTokens](#) presentation for a pilot implementation

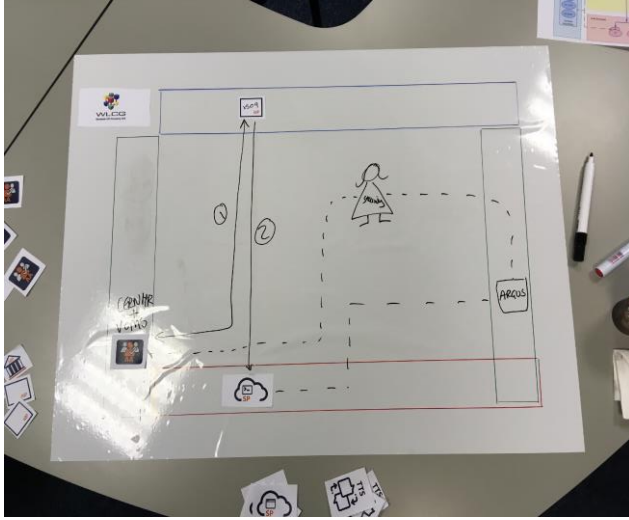
JSON Web Tokens

- Computing services are increasingly turning to token based authentication & authorization (OIDC, OAuth2...)
- Multiple infrastructure projects already using/supporting token based authorization but with diverging schemas or technologies
 - INDIGO IAM
 - EGI Check-in
 - SciTokens
 - dCache
 - ALICE tokens
- Is WLCG able to define a shared schema for participating infrastructures and services to agree?

JWT

- Initial analysis has concluded that two separate schemas are required
 - Identity Schema (who is this person?)
 - EGI Check-in, INDIGO IAM, dCache, ...
 - Capability Schema (what is the bearer of this token authorized to do?)
 - EGI Check-in, INDIGO IAM, dCache, SciTokens, ALICE...
 - Work is ongoing to draft schema definitions

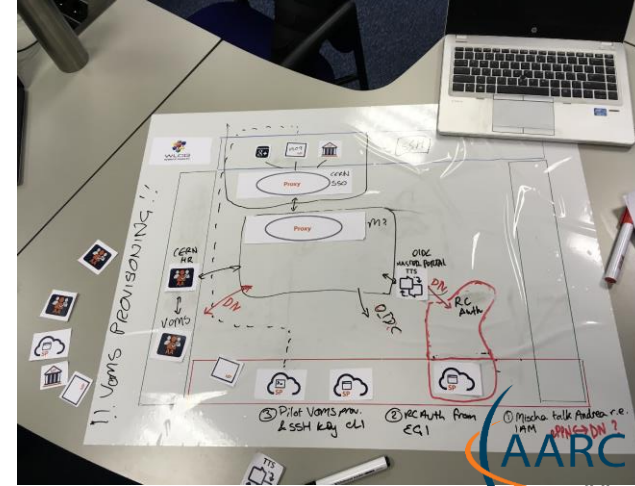
AAI Pilot Projects



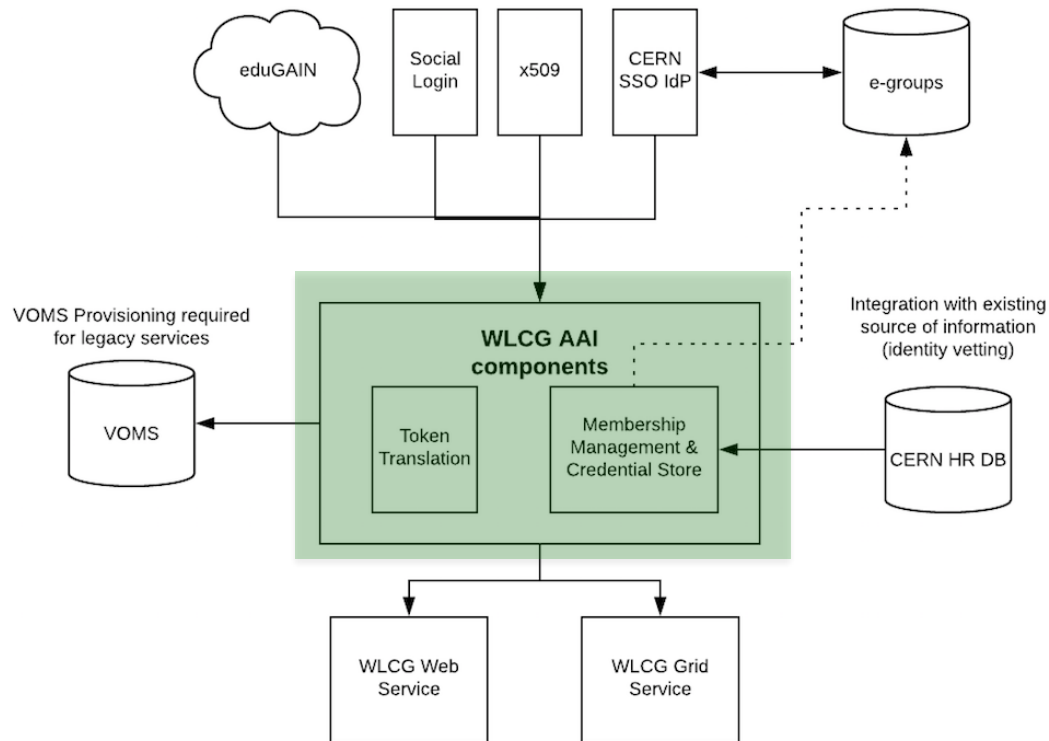
Current infrastructure allows access based on X509, including VOMS, CERN HR DB and Argus



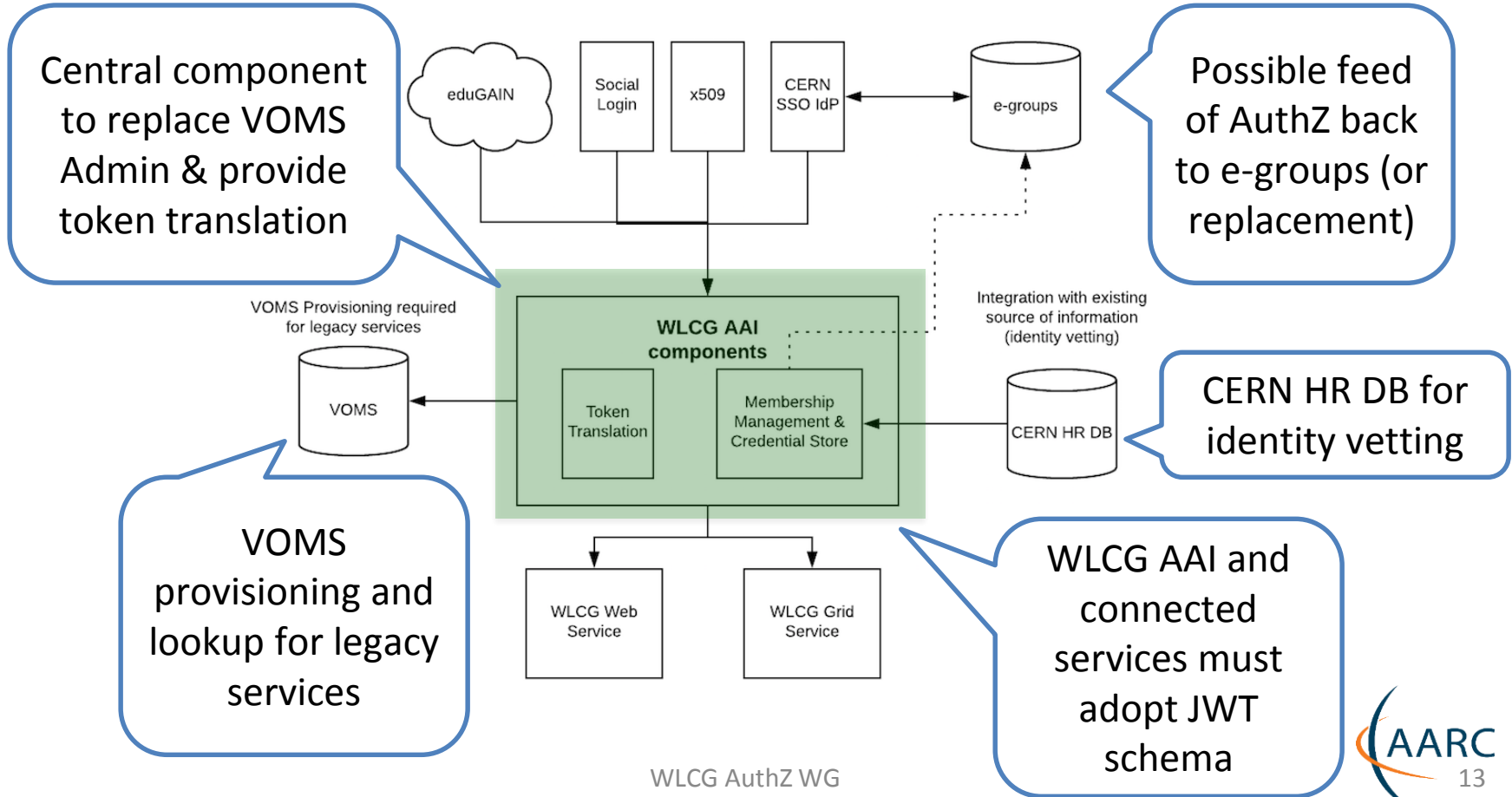
Future infrastructure should support a range of credential types for users and services and provide a user friendly experience



AAI Pilot Projects

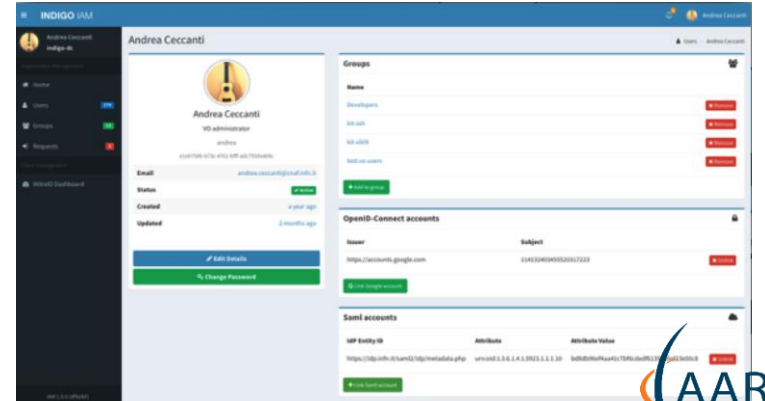
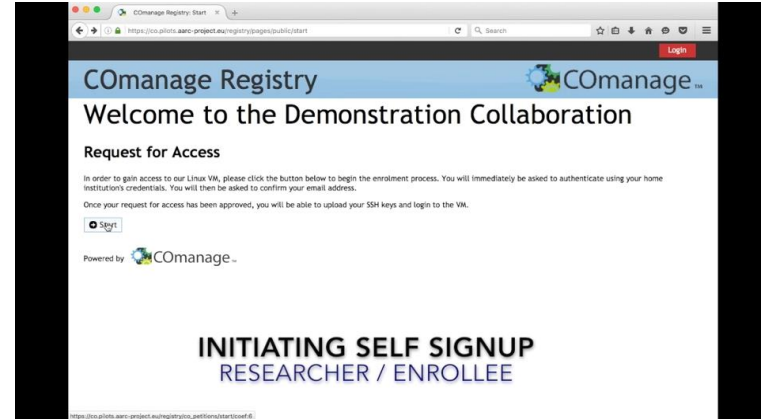


AAI Pilot Projects



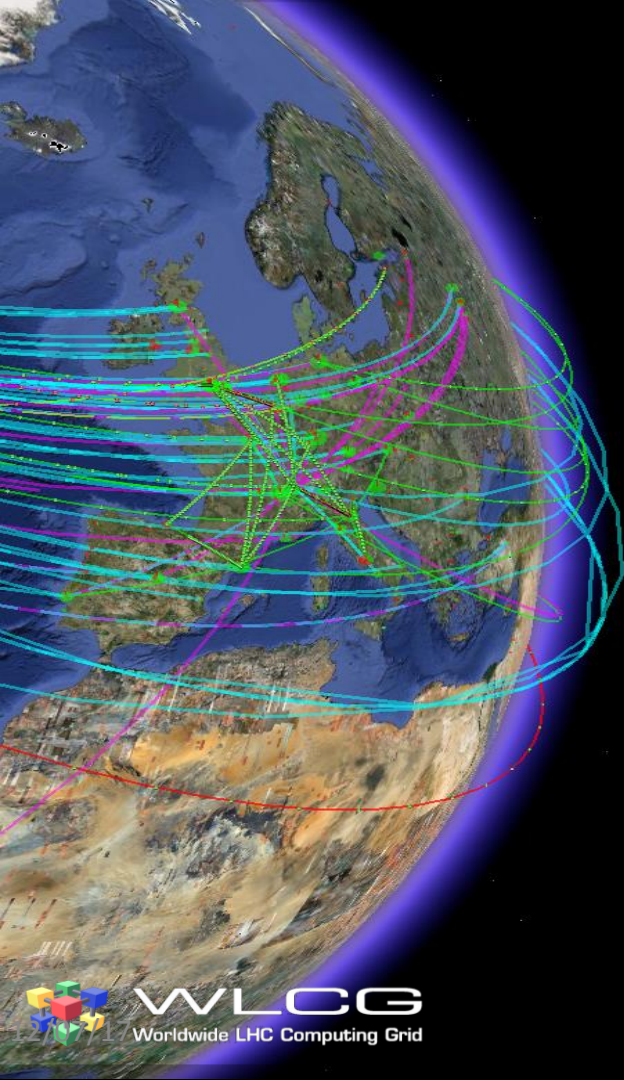
AAI Pilot Projects

- Two solutions appear to meet the majority of requirements
 - EGI Check-in & COmanage
 - INDIGO IAM
- Additional integration required for
 - VOMS provisioning & lookup
 - CERN HR DB integration
 - AUP re-signing



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

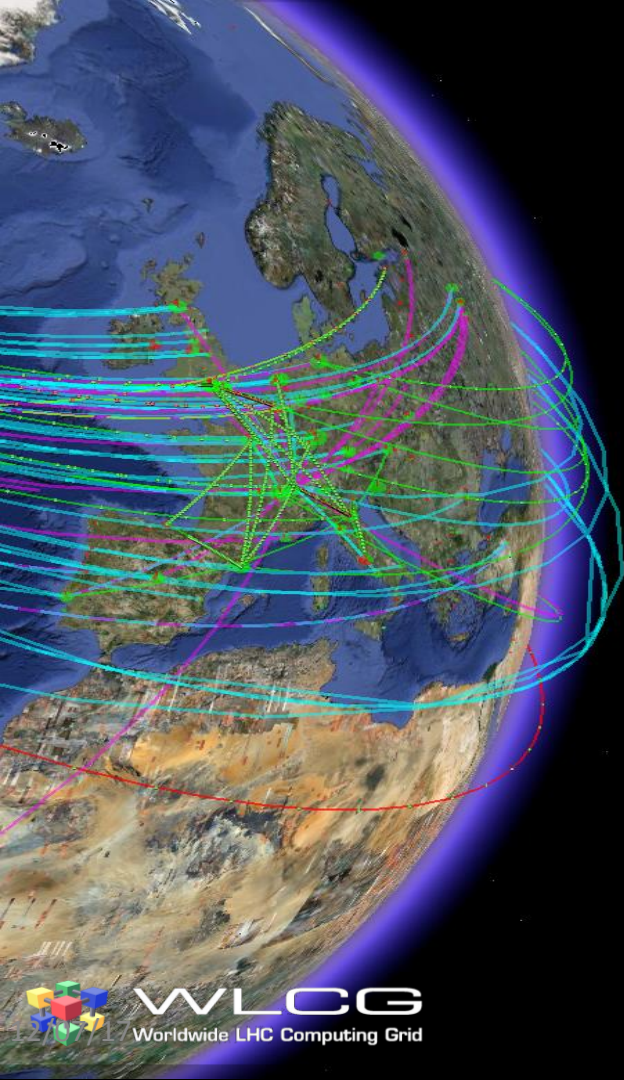
AuthZ WG Objectives

- Objectives have become clear over past year:
 - Agree on high level requirements for a WLCG AAI to provide Membership Management & Token Translation services
 - To facilitate transition to token-based credentials
 - Guide the development of AAI Pilot Projects
 - INDIGO IAM (pilot supported e.g. by EOSC-Pilot & AARC)
 - EGI Check-in & CManage (pilot supported e.g. by AARC)
 - Define a JSON Web Token (JWT) Schema for Authorization and agree to its use among WLCG Participants
 - Assess the AAI Pilot Projects against our requirements and move towards production deployment on a per-VO basis

Today

10:30	→ 10:45	Opening	🕒 15m	📄
10:45	→ 11:05	FIM4R - other Research Community approaches to AAI	🕒 20m	📄
11:05	→ 11:25	Requirements Document Sign-off	🕒 20m	📄
		🔗 Requirements Doc...		
11:25	→ 11:45	Token Catalogue Sign-off	🕒 20m	📄
		🔗 JWT Catalogue		
12:00	→ 13:00	Lunch	🕒 1h	
13:00	→ 14:00	JWT Schema	🕒 1h	📄
		🔗 WLCG JWT Schema		
14:00	→ 14:30	Pilot Update - Indigo IAM	🕒 30m	📄
		Speaker: Andrea Ceccanti		
14:30	→ 15:00	Pilot Update - EGI Checkin / CoManage	🕒 30m	📄
		Speaker: Nicolas Liampotis (Greek Research and Technology Network - GRNET)		
15:00	→ 15:20	Coffee	🕒 20m	
15:20	→ 16:00	Operational Impact	🕒 40m	📄
16:00	→ 16:20	Next Steps	🕒 20m	📄
		Discussion		
19:00	→ 21:00	No-Host Dinner	🕒 2h	

Cafe de la Place, Meyrin (just next to the tram stop)
We have a table reserved for 8 people, name "Short", outside if it's sunny.



Questions?