Authentication and Authorisation for Research and Collaboration

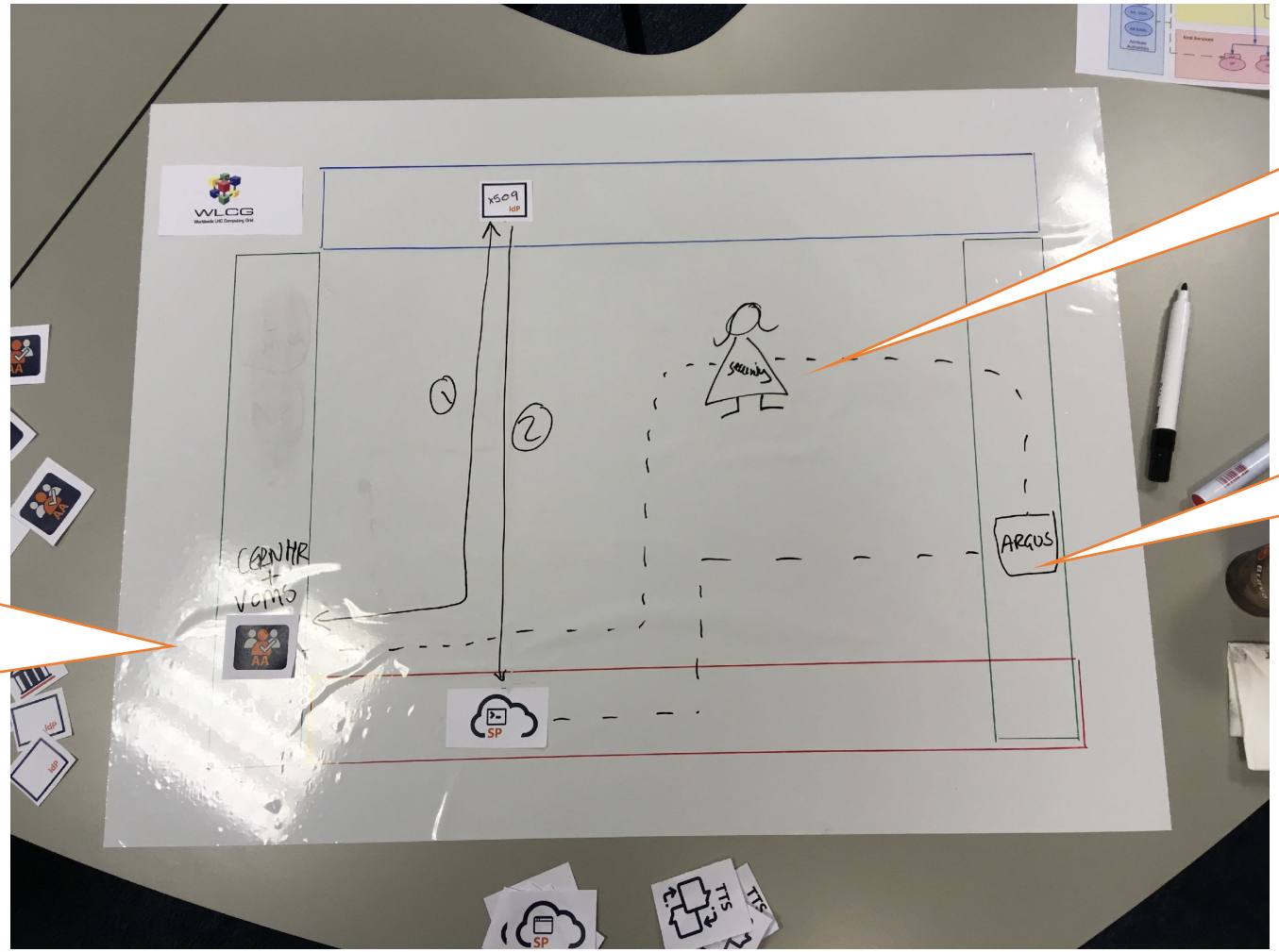
AARC2 WLCG Pilots

Authentication and Authorisation for Research and Collaboration

Mario Reale & Hannah Short
AARC WLCG Pilot

WLCG AuthZ WG Meeting
21st February, Vidyo

AARC Analysis, November 2017: Current



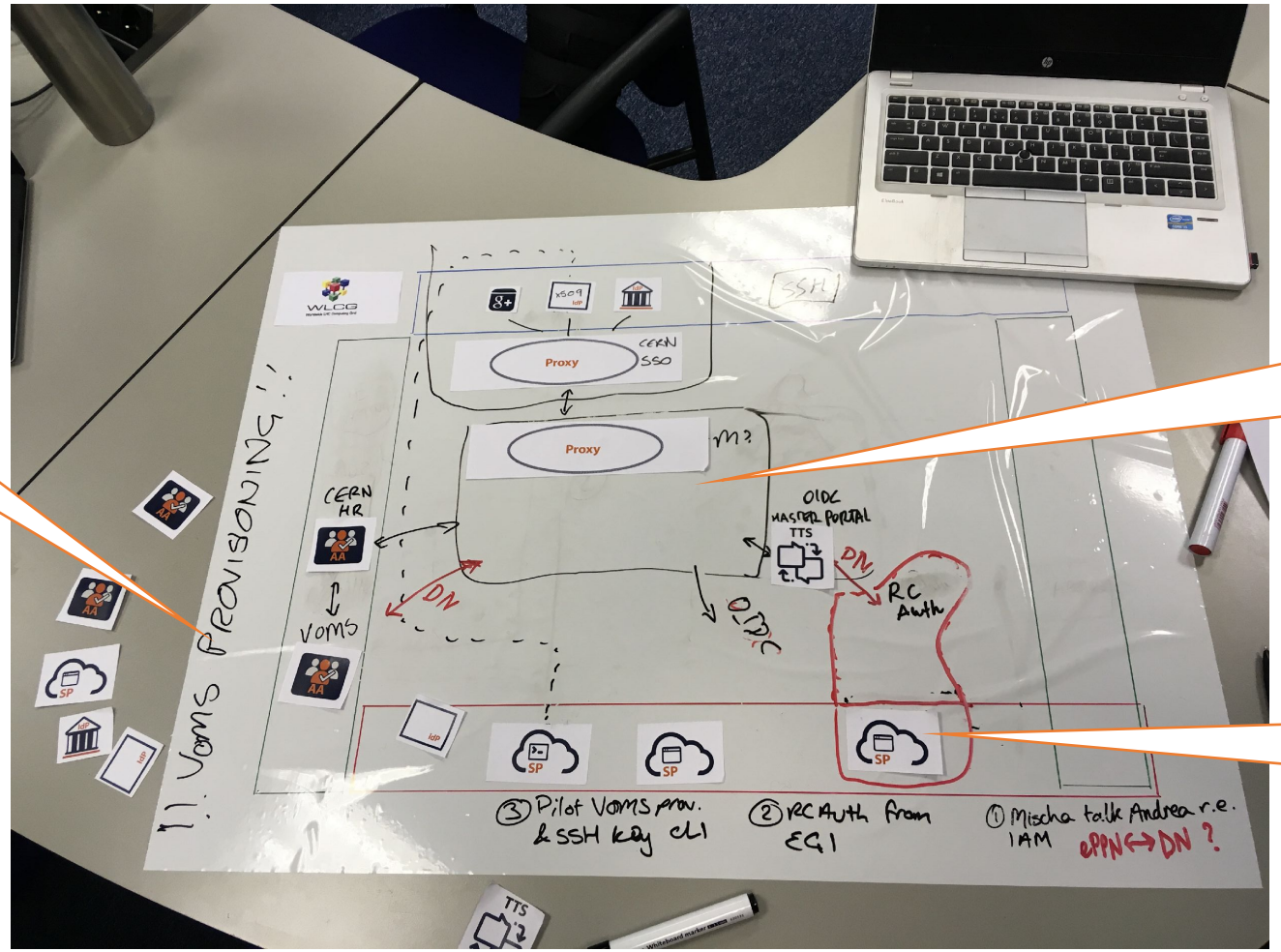
Group Management = VOMS-Admin, CERN HR DB

Operations

Argus policy engine

AARC Analysis, November 2017: Future

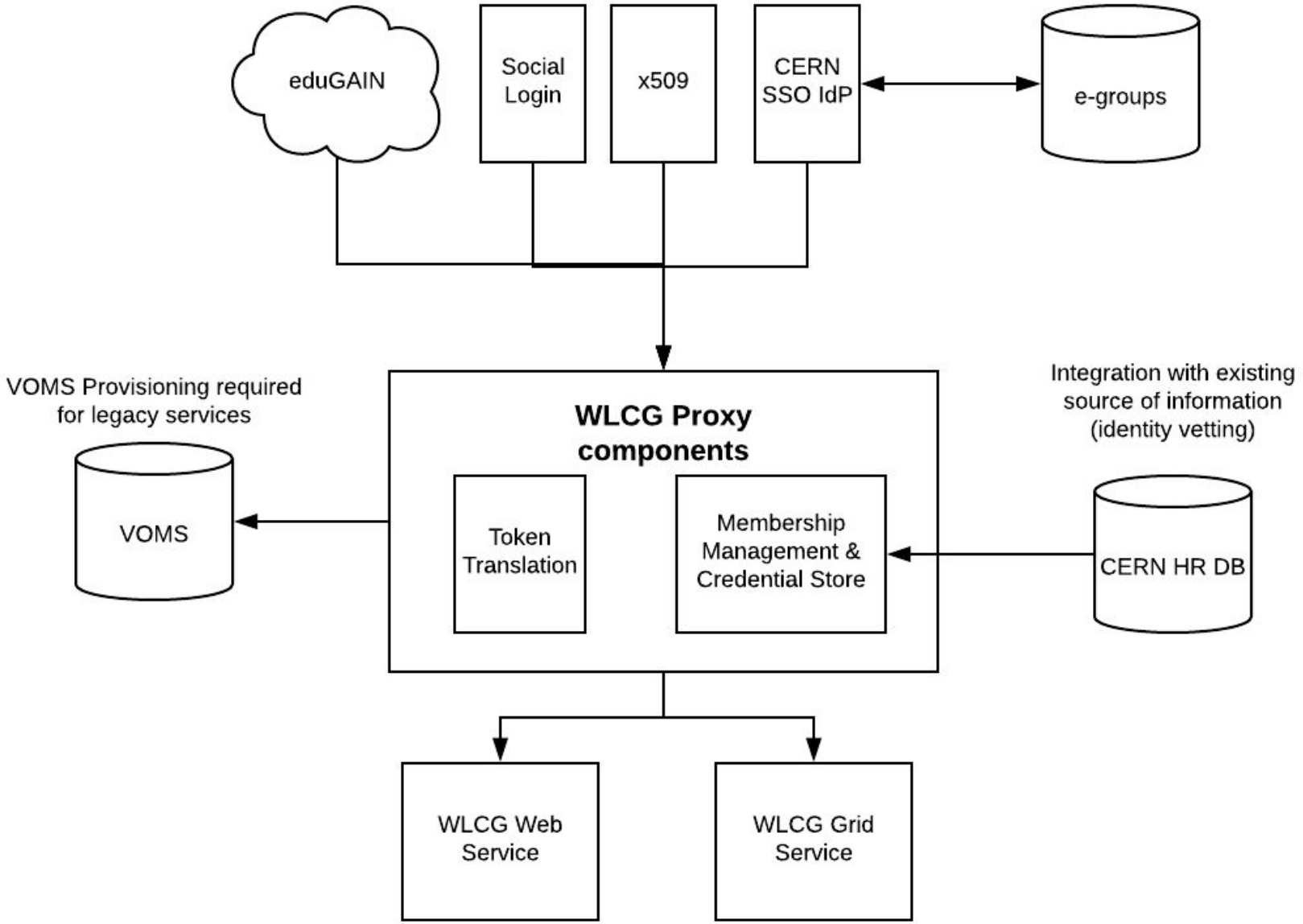
Unsolved bit…



Group Management Proxy element (e.g. IAM)

Master Portal

WLCG pilot structure



Main points from Analysis

Analysis based on momentum within WLCG to address AuthZ and enable Federated Identity.

- Membership Management
  - The VOMS backend will need to be maintained for some time, however VOMS-Admin can/should be replaced
  - **VOMS provisioning** is not included in existing solutions (e.g. IAM, Checkin+CoManage)
  - Integration with CERN HR DB must be maintained for identity vetting purposes
  - CERN's SSO will potentially be a single IdP for LCG VOs
- Token Translation
  - Required to produce x509 for users
  - Using RCauth with either COManage+Checkin or MasterPortal will let us use the ssh-key command line flow (MasterPortal demoed by Mischa, COManage+Checkin by Nicolas)
- Authorisation Schemas
  - Necessary to define, agree to and test an **interoperable schema for JWT** tokens between EGI, OSG and other contributing infrastructures

AARC Pilots

Objective: Demonstrate a pilot solution for a researcher **without a certificate** to **register** in a WLCG VO and **access** a **grid service**:

- Introducing the minimal required new components to allow smooth user experience
  - Central IDP/SP proxy
  - Token Translation Service
  - Attribute Authority
- Managing authentication and authorization to comply with WLCG requirements and standards
  - HR db integration
  - Acceptable level of assurance in line with IGTF profiles
- Minimizing the number of new developments required by WLCG Services

Pilot Intake Form available on AARC wiki at

https://wiki.geant.org/pages/viewpage.action?spaceKey=AARC&title=AARC2+SA1+Pilot+Intake+WLCG

New Authentication model and required pilot components

- Current AuthN model: : users' X.509 certificates (IGTF)

- ***New:***
  - ***user federated credentials released by Home Institutes (eduGAIN IDPs)***
  - ***X509 for legacy users***

- ***Newly required components:***
  - ***IDP/SP proxy (proxying OIDC/OAuth2 IDs, allowing attribute aggregation..)***
  - ***Token Translation Service (SAML to X.509)***
  - ***Attribute Authority + Group Management***

Current Authorization model vs new one

- Current Authorization is managed via VOMS proxy extension to user proxy presented to the Grid services (Roles)

- ***New: Based on user attributes released by IDP + additional ones provided by Group Mangement/AA mapped to VOMS proxy extension (or JWT claims in future)***

Implementation strategy

- Main idea is to be able to compare and benchmark 2 options
  - EGI Checkin Service + CoManage
  - INDIGO IAM

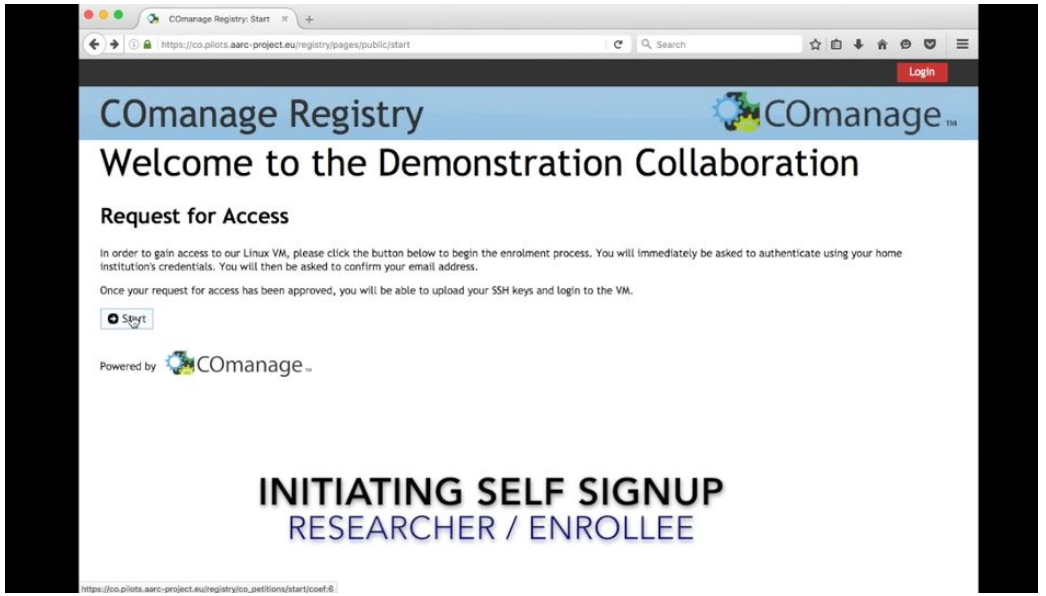
- Provided components:

	INDIGO Solution	EGI Checkin solution
Proxy	INDIGO IAM layer	SimpleSAMLphp EGI Checkin Service
Token Translation service	INDIGO - WaTTS + RCAuth.eu	RCAuth.eu + Master Portal
Attribute Aggregation	INDIGO IAM layer	COMANAGE
Integration to VOMS	INDIGO IAM layer	COMANAGE VOMS plugin

Option 1 : COmanage

Option 1: Development of COmanage VOMS admin plugin

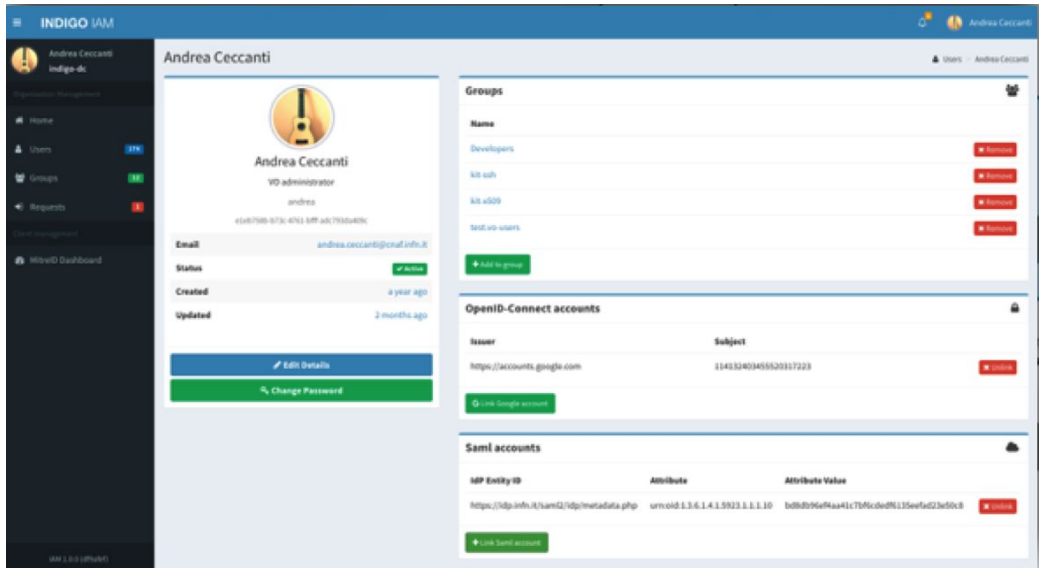
- Use EGI Checkin with CoManage as WLCG Proxy
- Use CoManage as VO membership store
- Development work includes
  - Push DNs, Roles & Groups into VOMS to maintain x509 authorisation for legacy services
  - Retrieve DNs from RCAuth or Master Portal
  - Manage AUP resigning through CoManage



Option 2 : INDIGO IAM

Option 2: Development of IAM to support VOMS

- INDIGO IAM can be used as comprehensive Proxy
- IAM can store DNs directly and could replace VOMS immediately, backwards compatible endpoint but services relying on VOMS api would need to adapt
- INFN CNAF has funding through EOSC-Hub or INFN to do WLCG specific development for IAM, there are 3 developers + contributions
- WaTTS has recently been integrated with RCAuth
- Development work includes
  - Create link to HR Db
  - VOMS provisioning plugin
  - Retrieval of DNs from RCAuth or Master Portal



Pros and Cons:

This is a non-exhaustive list that should become more clear thanks to the work of this WG

	INDIGO	**EGI Checkin + COmanage**
PROS	Integrated solution Direct VOMS replacement	COmanage widely adopted tool
CONS	South of proxy, OIDC/OAuth2 only Required additional developments (VOMS plugin for IAM)	COmanage heavy to use for mobile clients Requires additional developments (COmanage VOMS-admin plugin)

Outcome & timeline

- Outcome of the pilot will be to provide the WLCG PMB with hands-on feedback on the two possible solutions capable of paving the way towards X.509-free WLCG:
  - Both approaches required additional developments
  - Both strategies will have to ensure sustainability of these developments in the forthcoming years
- Timelines:
  - Need to start the missing developments ASAP to be able to provide results within AARC2 lifetime (ends April 2019)
    - Require clarification: a possible timeline could be:
      - **Finalization of new required developments for 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 and actions

Summary: AARC will run 2 pilots that will provide a good baseline solution for production adoption by WLCG

INDIGO IAM (key person = Andrea++, Mischa)

- Give access to WLCG IAM instance
- Work on VOMS provisioning : design & develop functionality
- Could authenticate through CERN SSO

EGI Check-in Service + COmanage (key people = Nicolas, Benn, Mischa, Andrea)

- Start design and implementation of VOMS plugin for COmanage
- Give access to WLCG COmanage instance

Thank you

Any Questions?

hannah.short@cern.ch or
mario.reale@garr.it

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).