Authentication and Authorisation for Research and Collaboration

LifeWatch Pilot Status

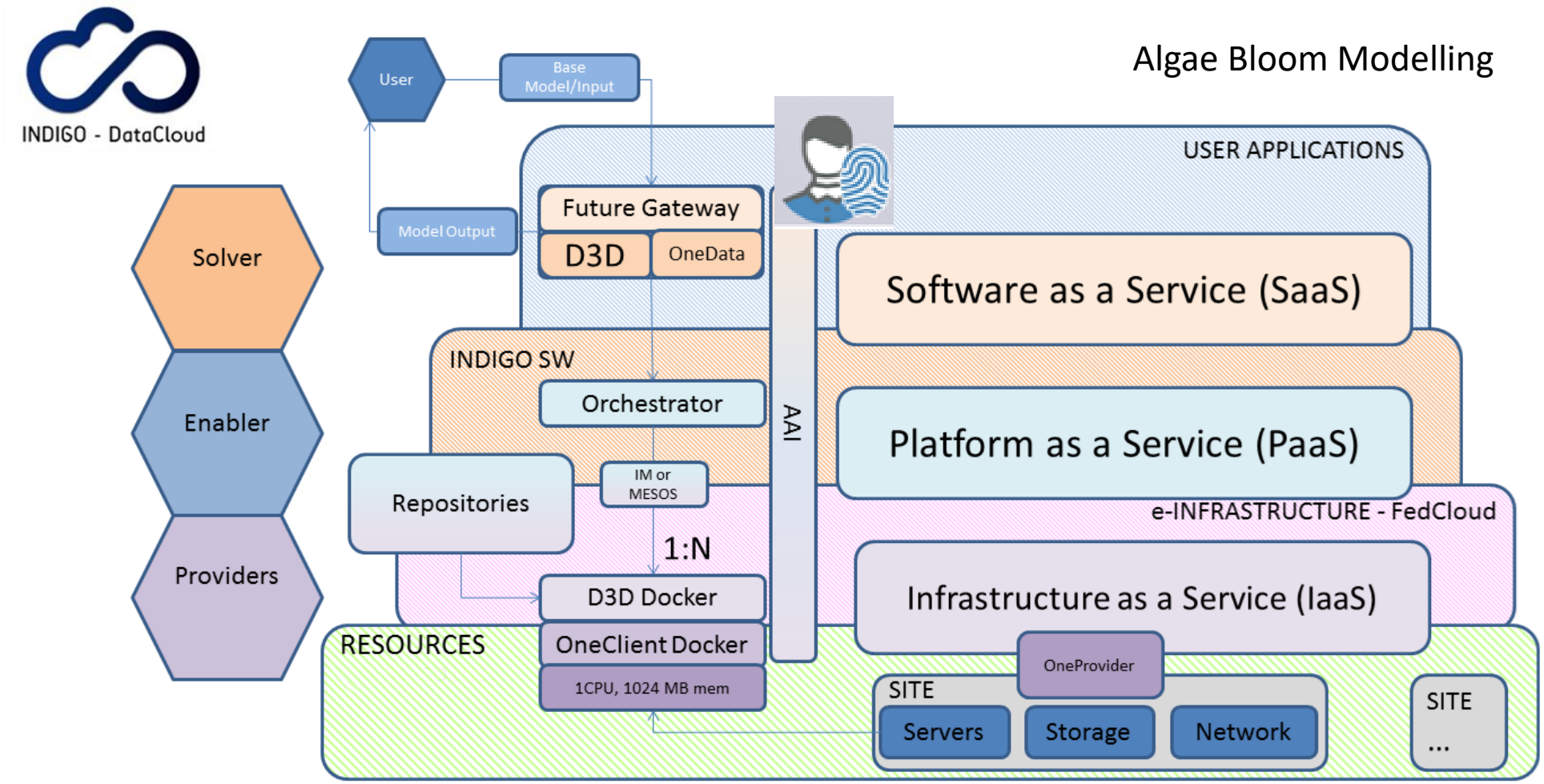
Pilots hands on session with LifeWatch

Fernando Aguilar

fernando.aguilar@lifewatch.eu

12 Apr 2018, Athens

Starting Point



Communities you represent

Who/Where are your users typically?

- LifeWatch ICT sites administrators
- LifeWatch Developers (Solvers)
- LifeWatch Researchers
- Citizen Scientists

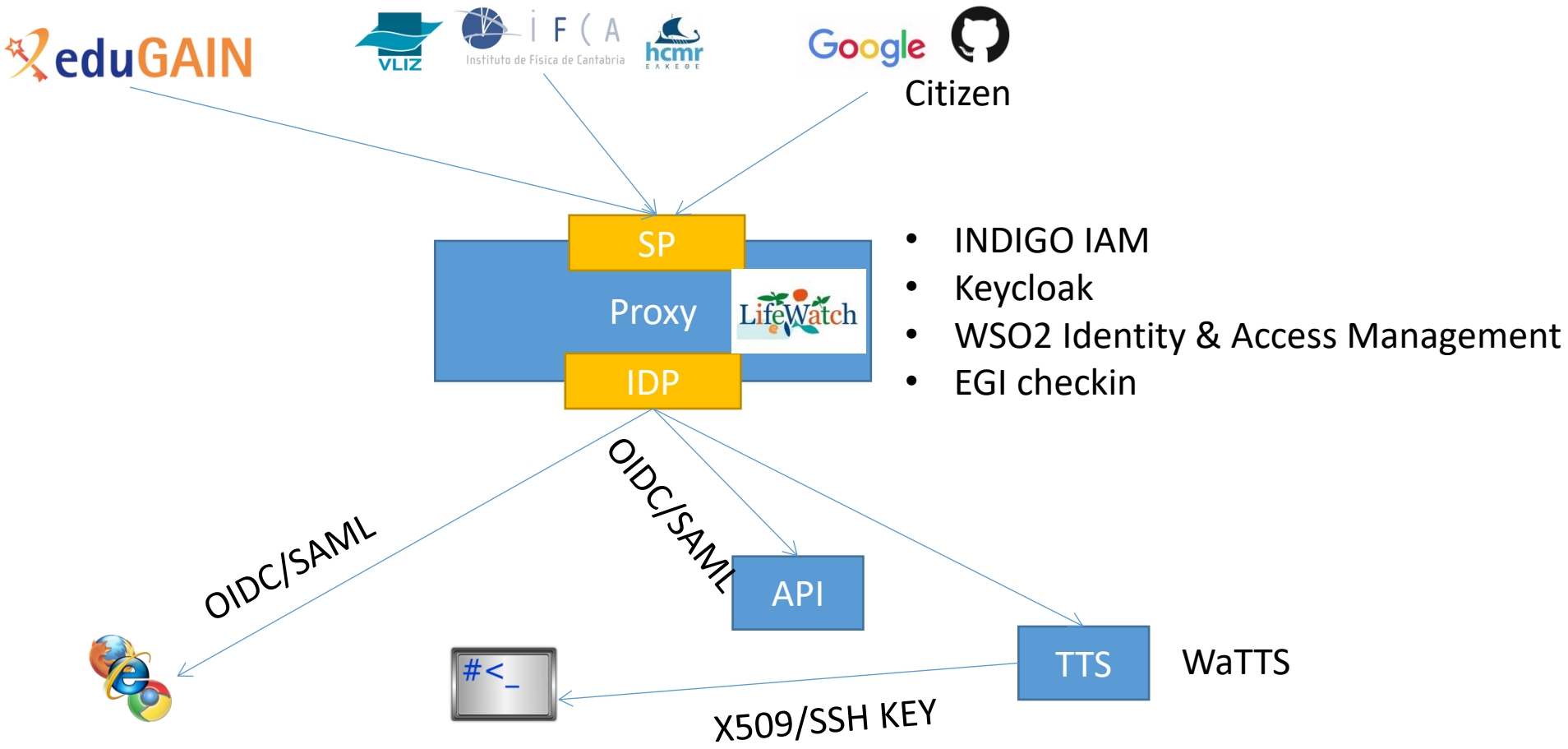
What kinds of resources do they need to access?

- Infrastructures (IaaS): Site administrators
- PaaS: Solvers
- Applications (SaaS): Solvers Researchers, Citizen Scientists

Where are the resources hosted?

- ICT Core (Distributed). Links to EGI.

General Schema



General Information for the Solution

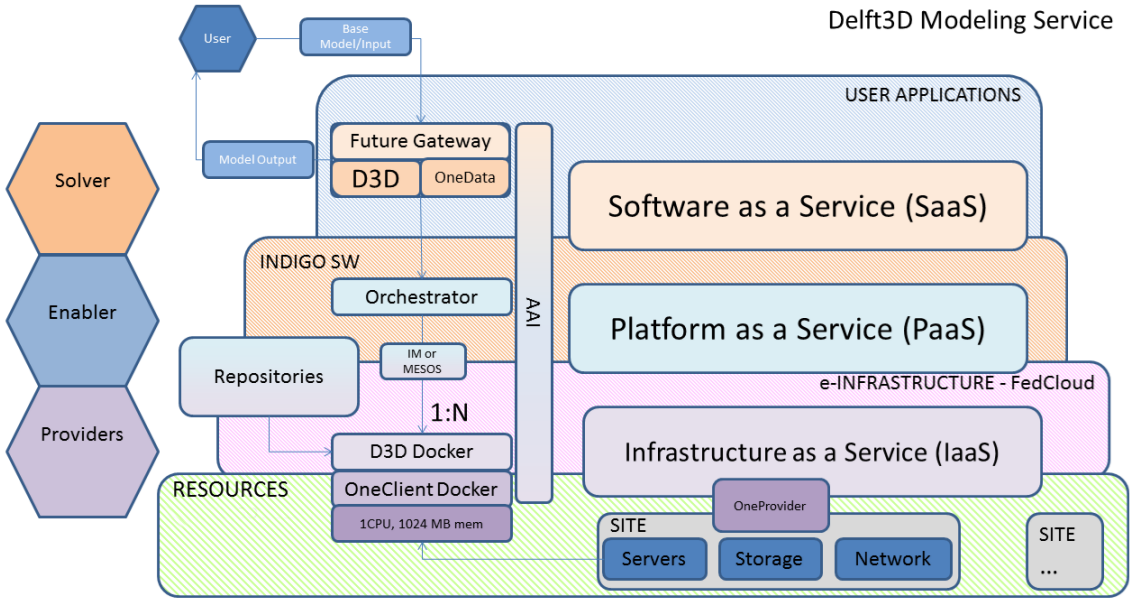
- The central system will run at the LW ICT Core in Spain
- It will provide authentication and authorization services for all LW central and distributed systems, as well as other interested e-infrastructures like EMBRC, DiSSCO.
- It will allow cross-authentication with other identity providers like eduGain, EGI, etc.
- Selected solution must be deployed in the LifeWatch ICT Core.
- The IDP will be used :
- to give access to restricted LW services. The services may be restricted because of processing power or storage demands.
  - to protect user data and scripts that are stored on the infrastructure (unix home folders,etc)
  - to give access to data not yet in the public domain. (data in databases , project moratorium period)
  - to distinguish between users uploading data to the system (RvLab , eLab, data explorer)
  - to give access to Openstack configuration interface and computing resources at infrastructure layer.
  - To manage roles/groups and authorize them to access specific services.
- Currently, the different user apps manage their own users. The institutional credentials could be federated in the Identity Provider.
- Two components suggested by AARC: **Identity Provider**, Token Translator System.

Types of services in the Stack

- Web based applications:
  - Rshiny, Rstudio
  - Data Portals: GBIF, Digital Knowledge Preservation Framework (EOSChub), Automatic Image Analysis, etc.
  - Citizen Science apps: Natusfera, PAIRQURS (with EUDAT services, B2ACCESS, B2SHARE).
  - Geoserver, GIS-based services.
- Applications with bridges to HPC.
  - RvLab
  - TRUFA (slurm batch system)
- Mobile Apps
  - Natusfera App
  - Plant classification
- Cloud Computing resources.
  - OpenStack
- Distributed storage solution (Onedata, EGI Data Hub) – Interesting for the future.
- ~~Grid resources: Not a priority (it was in the past).~~

Roles

- Citizen Scientists: Citizen Science apps and services.
- LifeWatch “Final” Users: Web-based apps, services, SaaS, access to computing resources.
- App Developers: Resources deployment, Configuration (e.g. connection to HPC, AAI), access to IaaS, PaaS.
- Managers, Virtual Organization Administrators: General services administration (Cloud stacks, IdP, TTS, etc.), IaaS, deployment management, etc.



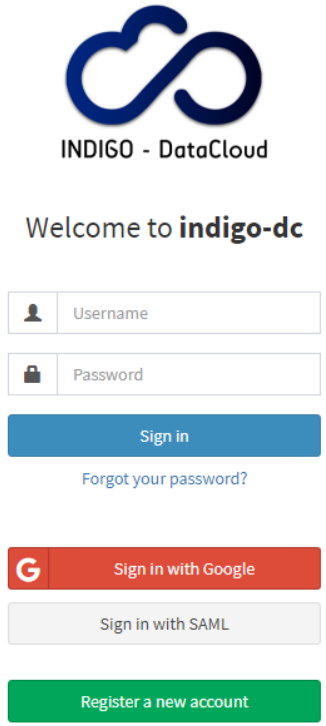
Identity Provider Requirements

- Compatible: OIDC (priority), SAML (interesting, eduGain).
- Federation of 1-N Institutions. Citizen Scientists (Social IDs).
- Roles Management. Role mapping (e.g. Google users to Citizen Scientist).
- Identity linking (optional).
- Group Management. Some groups are allowed to do…
- Distributed, clustered. High availability.

INDIGO IAM – First Choice

- Compatible: OIDC (priority), SAML (interesting, eduGain).
- Federation of 1-N Institutions. Citizen Scientists (Social IDs).
- Roles Management. Role mapping (e.g. Google users to Citizen Scientist).
- Identity linking (optional).
- Group Management. Some groups are allowed to do…
- Distributed, clustered. High availability. Via Database.

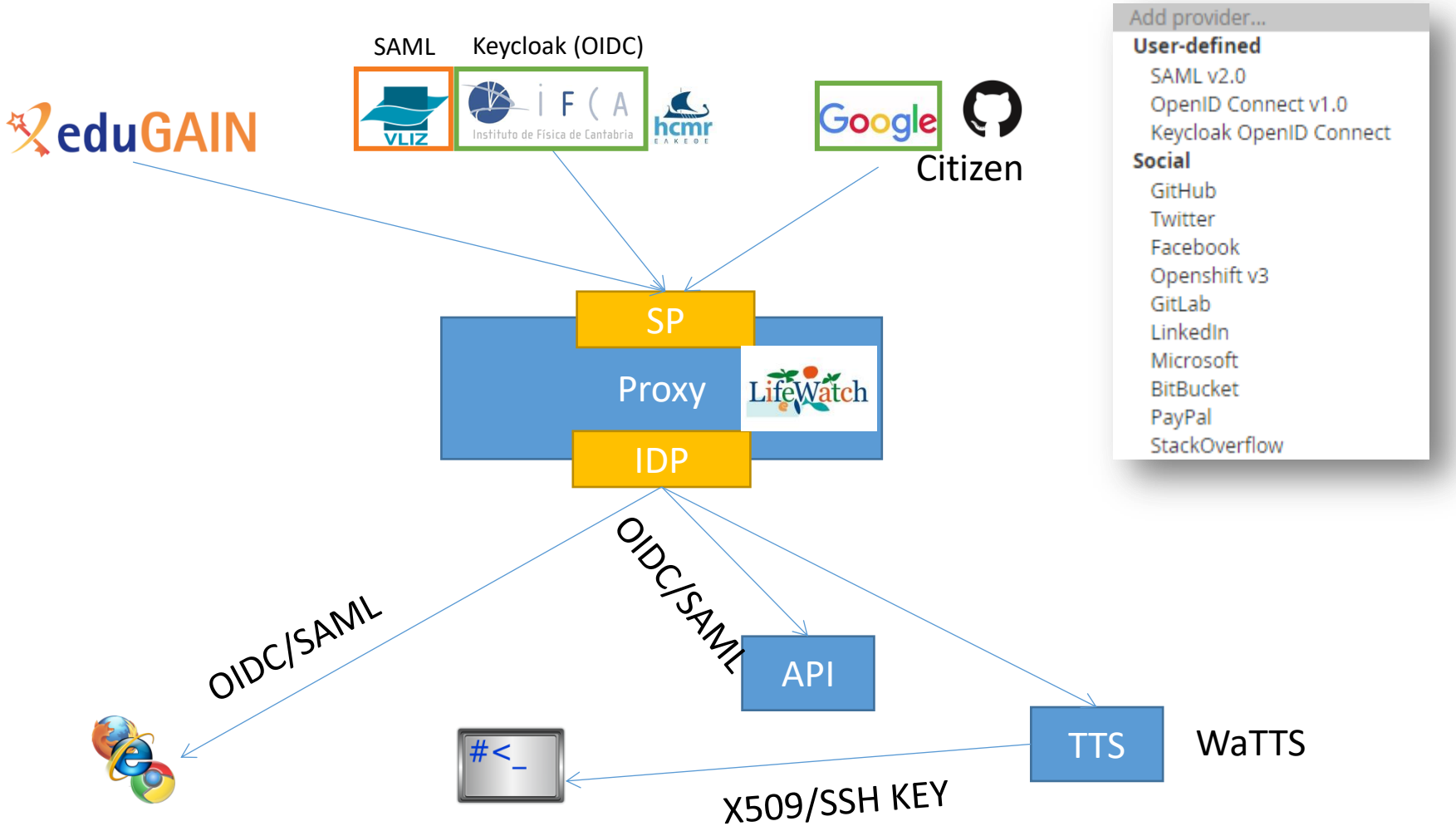
- Deployed, but problems with federating N IdPs.



Keycloak – Second Choice

- Compatible: OIDC (priority), SAML (interesting, eduGain).
- Federation of 1-N Institutions. Citizen Scientists (Social IDs).
- Roles Management. Role mapping (e.g. Google users to Citizen Scientist).
- Identity linking (optional).
- Group Management. Some groups are allowed to do…
- Distributed, clustered. High availability. NATIVE

Keycloak – Federation



Keycloak – App Configuration

- Web based applications:
  - Rshiny (OIDC under Apache), Rstudio (Native plugin in pro version)
  - Data Portals: GBIF, Digital Knowledge Preservation Framework (EOSChub), Automatic Image Analysis (OIDC under Apache), etc.
  - Citizen Science apps: Natusfera, PAIRQURS (with EUDAT services).
  - Geoserver (OIDC plugin), , GIS-based services.
- Applications with bridges to HPC.
  - RvLab (Internal User DB) – TTS needed
  - TRUFA (slurm batch system) – Internal User DB - TTS needed
- Mobile Apps
  - Natusfera App
  - Plant classification
- Cloud Computing resources.
  - OpenStack (OIDC compatible. Tested with IFCA SSO)

Token Translator System

- ON going… Deployed.
- Documentation: Plugin development as potential solution.
- TRUFA and RvLab:
  - Job submission to HPC
  - SSH user@hpc ‘submit_job foo’
  - SSH user@hpc ‘check_job_status foo’
- Inject SSH key? User must exist on the system

What we need…

- Support for defining the architecture – DONE! Who? VO Managers
- IdP – TTS deployment/configuration – DONE! Who? VO Managers
- Support on how to use TTS, how to create plugins. Who? VO Managers, Developers
  - Link to HPC resources
- Support to adapt the running services for IdP-TTS Who? Developers
  - Over Apache – OK
  - Native support – OK
  - How to adapt “incompatible” services?
- Guidance for developing new services taking into account the AAI Who? Developers

Thank you

Any Questions?

fernando.aguilar@lifewatch.eu

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).