



Authentication and Authorisation for Research and Collaboration

## **AARC Draft Blueprint Architecture**

Christos Kanellopoulos  
Architecture (JRA1) WP Leader, GRNET

AARC/CORBEL Workshop for Life Sciences AAI  
May 31 – June 1, Paris

# The starting point

- The scenario:
  - There is a **technical architect of a research community**
  - Her community is **distributed internationally**
  - **Increasing number of services** need authentication and authorization
  - Her job is to **find a solution**
  - She wants to **focus on research** and not reinvent the wheel
  - She starts googling
- So, there are some solutions available, but...



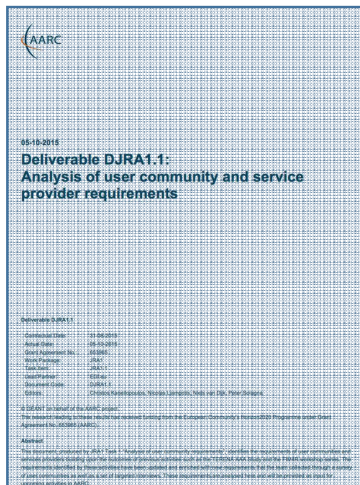
# The goals

---



1. Users should be able to access the all services using the **credentials from their Home Organization**
2. Users should have one **persistent non-reassignable non-targeted unique identifier**.
3. Attempt to **retrieve user attributes** from the user's Home Organization. If this is not possible, then an alternate process should exist.
4. Distinguish **(LOA)** between self-asserted attributes and the attributes provided by the Home Organization/VO
5. **Access** to the various services should be granted **based on the role(s)** the users have within the collaboration
6. Services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies.

# AARC: Analysis of User Communities and e-Infrastructure Providers

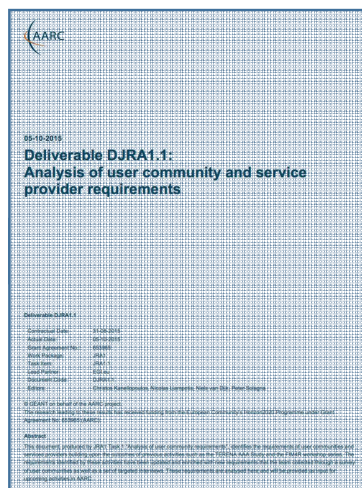


Attribute Release	Attribute Aggregation	User Friendliness	SP Friendliness
Credential translation	Persistent Unique Id	User Managed Information	Credential Delegation
Levels of Assurance	Guest users	Step-up AuthN	Best Practices
Community based AuthZ	Non-web-browser	Social & e-Gov IDs	Incident Response

# The functional Components



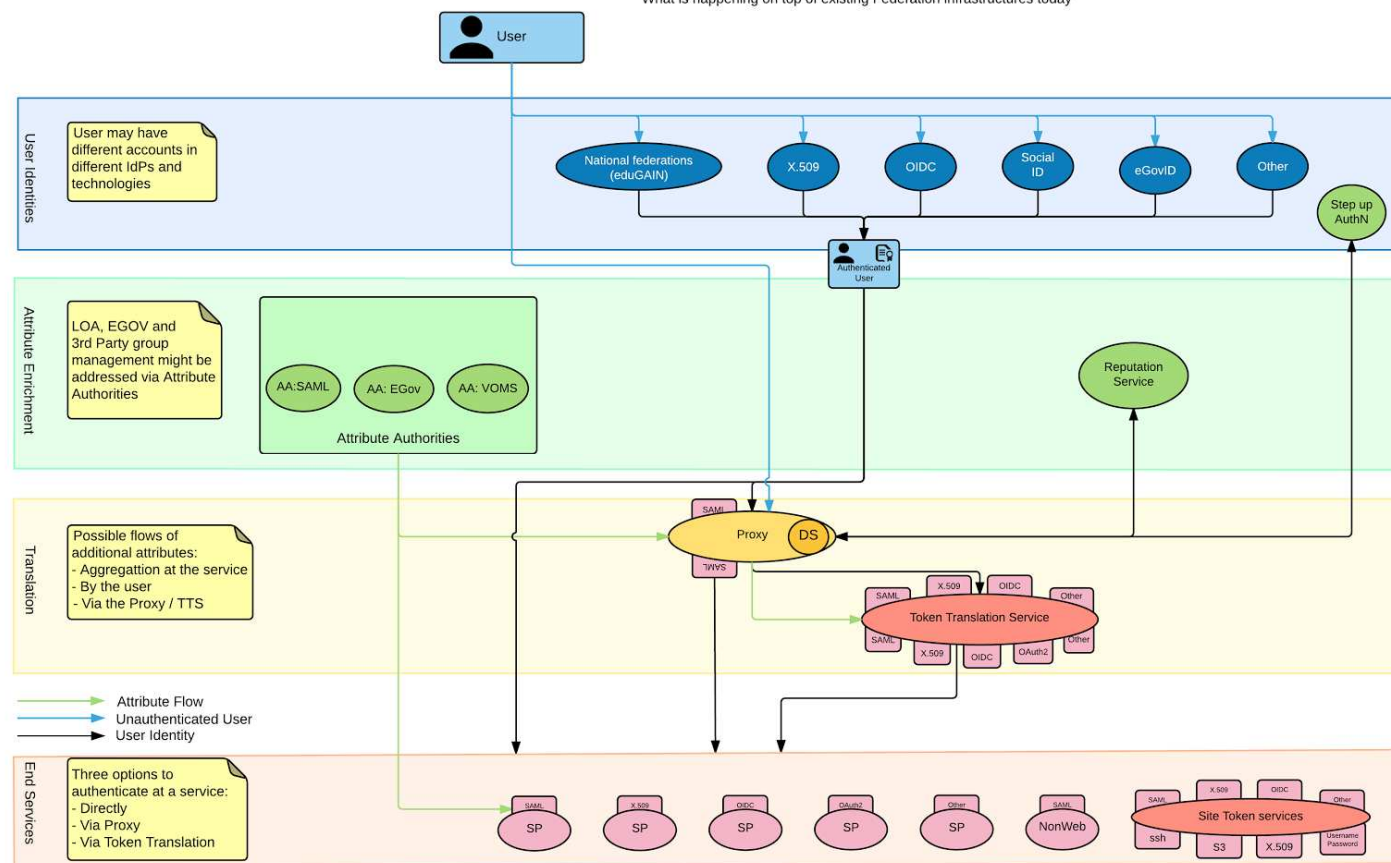
## User Community Requirements



<https://goo.gl/kSxENp>

## AAI: The e-Infrastructure view

What is happening on top of existing Federation infrastructures today



[aarc-project.eu](https://aarc-project.eu)

# Why the proxy model?

---

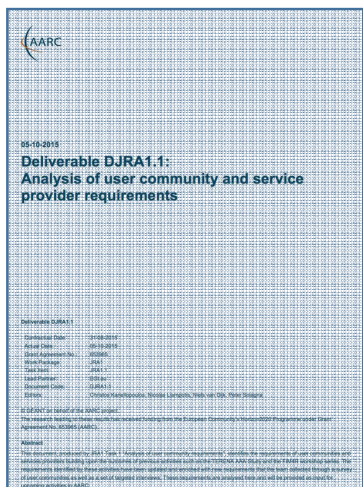
- All internal Services can have **one statically configured IdP**
- **No need to run an IdP Discovery Service** on each Service
- Connected SPs get **consistent/harmonised user identifiers**  
**and accompanying attribute sets** from one or more AAs  
that can be interpreted in a uniform way for authZ  
purposes
- External IdPs only deal with a **single SP** proxy



# The Functional Components and available AAI tools



## Analysis of User Communities



## And Infrastructure Providers

IdPs

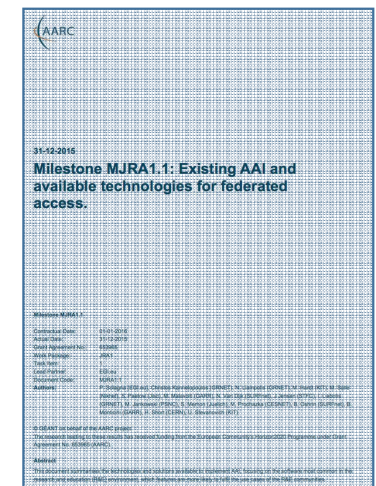
Attribute Authorities

Proxies

Token Translation

Service Provider

## Available AAI Components



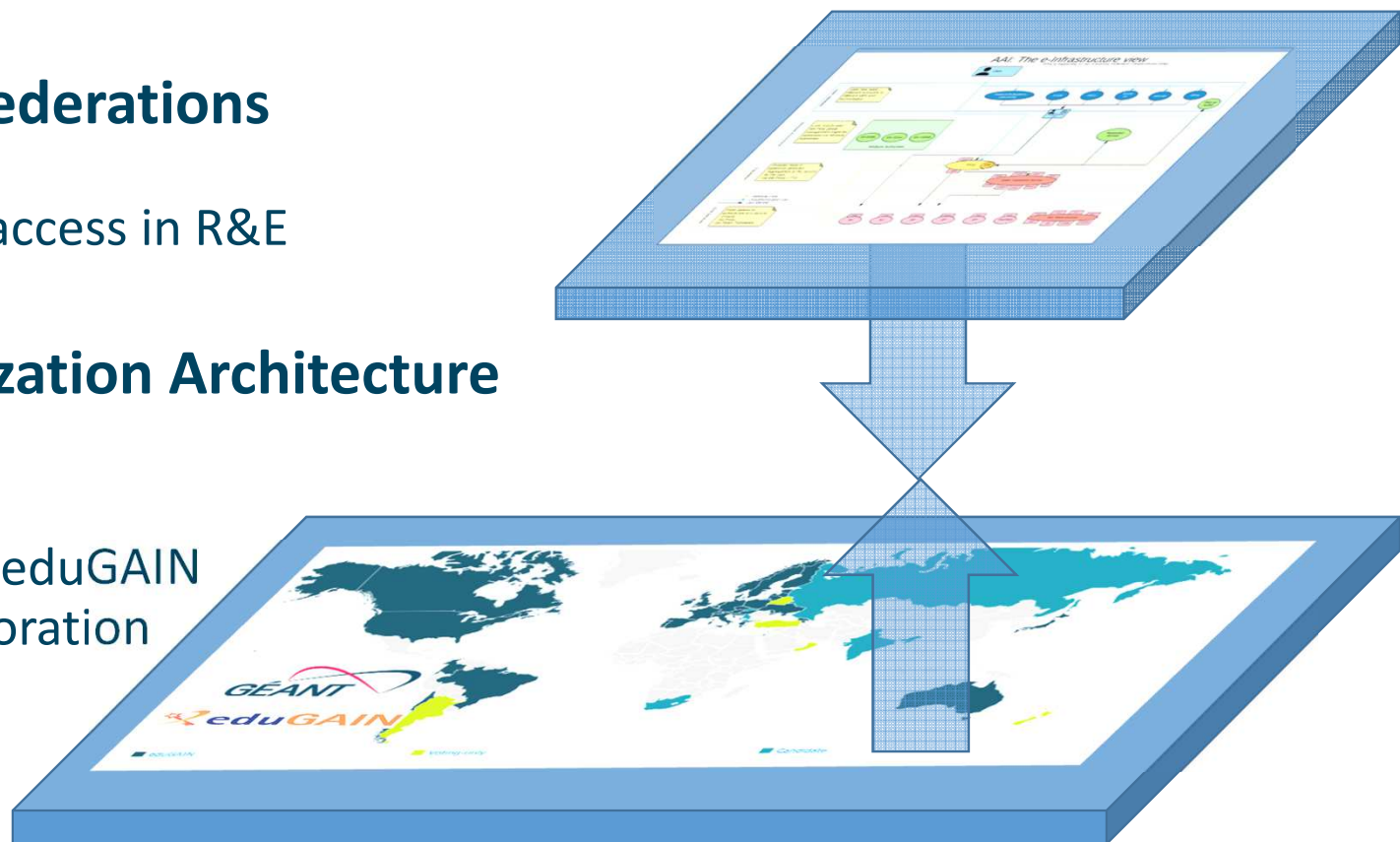
[aarc-project.eu](https://aarc-project.eu)

## eduGAIN and the Identity Federations

A solid foundation for federated access in R&E

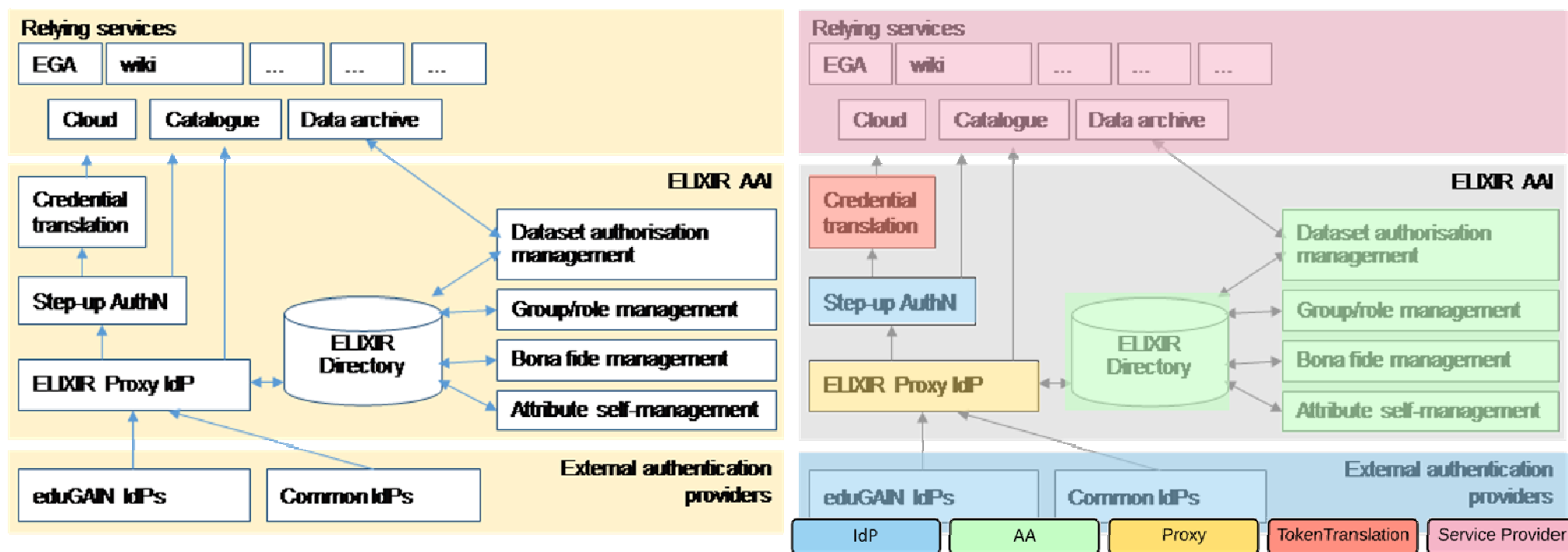
## Authentication and Authorization Architecture for Research Collaboration

A set of building blocks on top of eduGAIN for International Research Collaboration

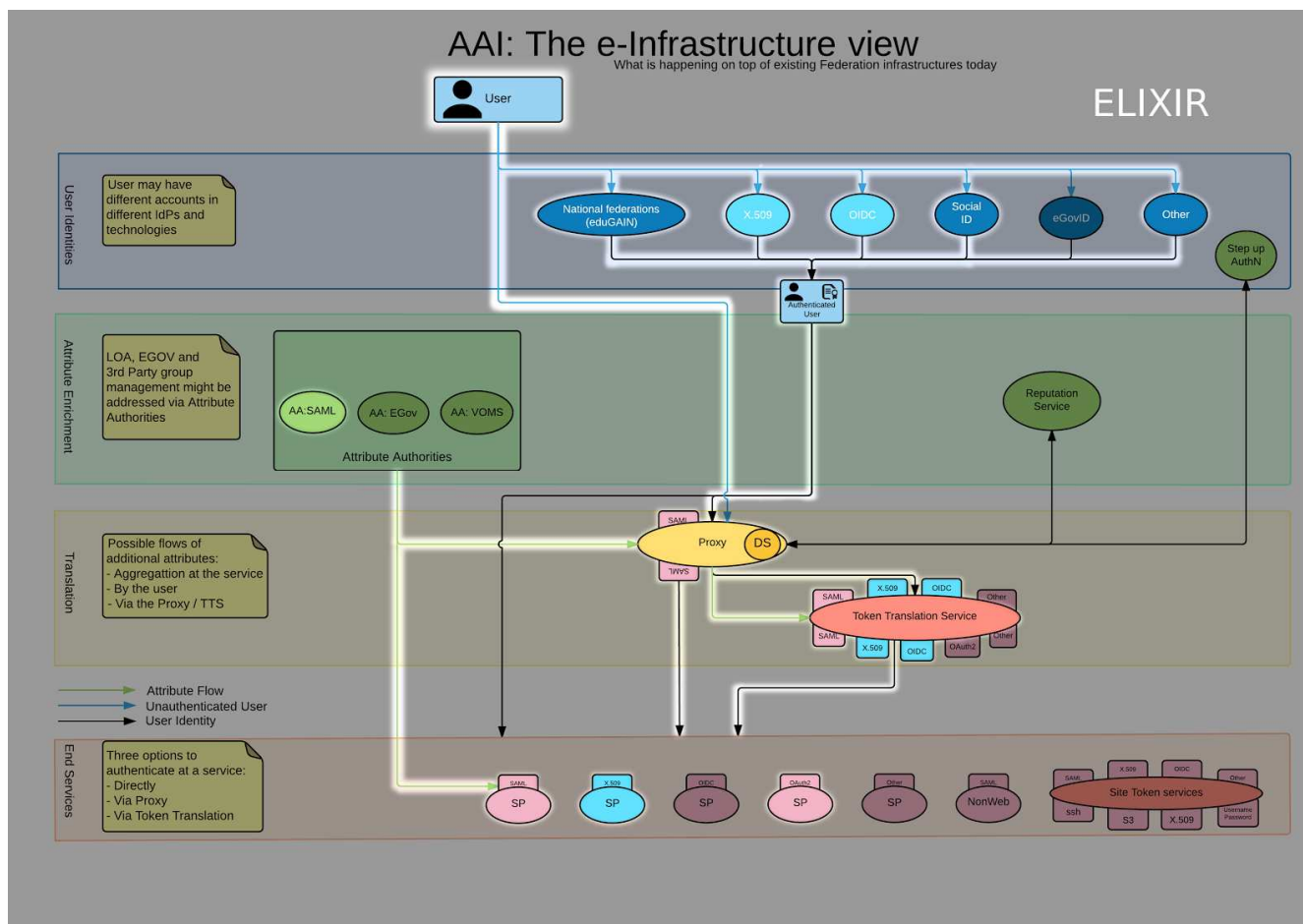




# AARC Blueprint Architecture & ELIXIR



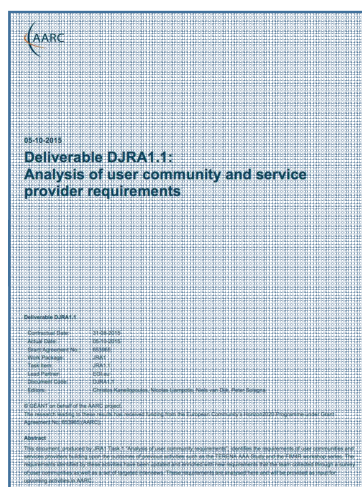
# AARC Blueprint Architecture & ELIXIR



# Pilots

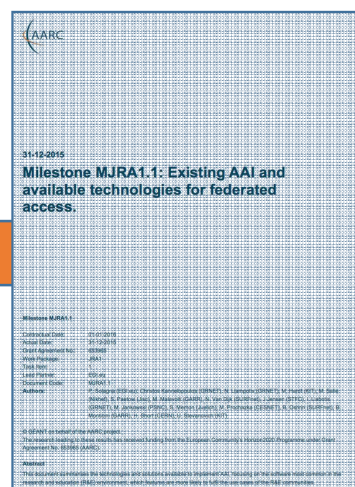


## Requirements User Community



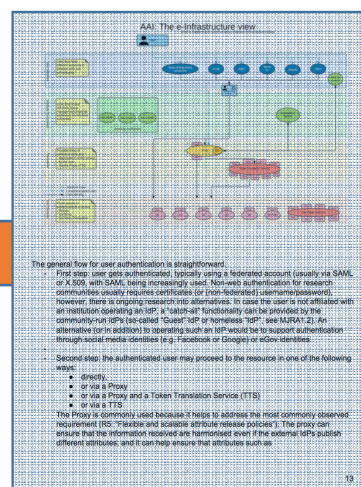
<https://goo.gl/kSxENp>

## Overview Available AAI Components



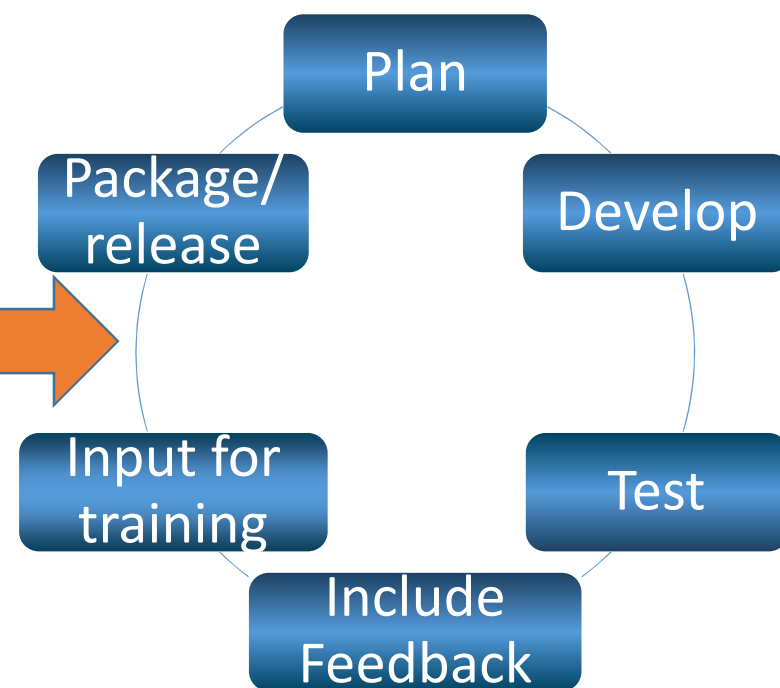
<https://goo.gl/NzQA2U>

## Draft Blue-Print Architecture



<https://goo.gl/7dZZF4>

## Pilots With Communities



[aarc-project.eu](https://aarc-project.eu)

# Thank you Any Questions?

Christos Kanellopoulos  
skanct@admin.grnet.gr



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).