AARC Authentication and Authorisation for Research and Collaboration

Pilots for guest identities (Task1)

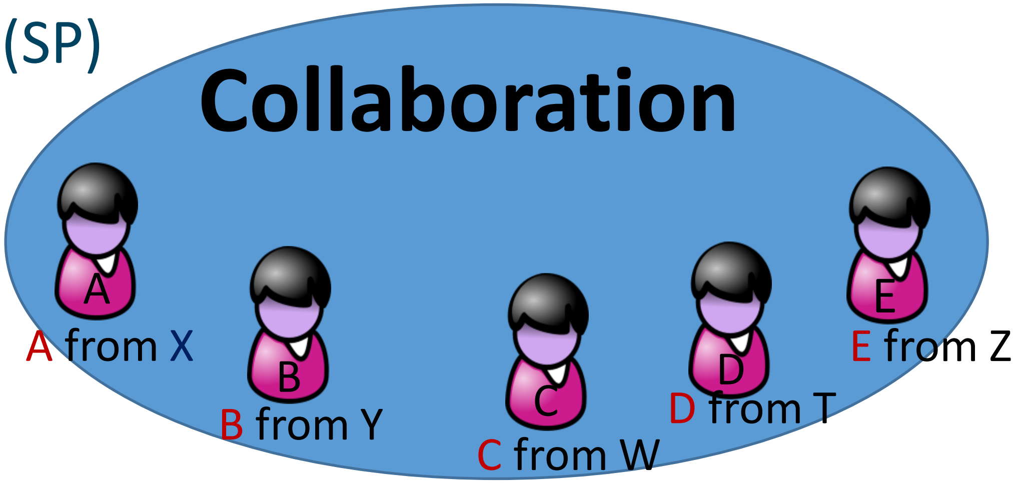
How do we provide “assured” access for non-academic users or academic users from *«?»*

- Mario Reale
- Barbara Monticini
- Lalla Mantovani

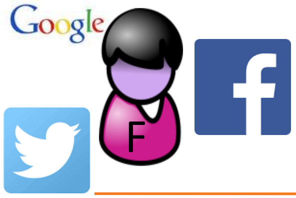
GARR

Guest Users

- A collaboration needs a Service (SP)
- The collaboration is made by users **A,B,..E** belonging to Home Organizations **X,Y...Z**
- SP knows organizations:
  - **X, Y, W**
- SP doesn't know organizations:
  - **T, Z**



→ **D** and **E** are **guest users** for the SP



→ *Additional option:*

If user **F** has a Social-Network ID or a Gov-ID , could she/he also be a **guest user** ?

Why do guest users exist?   Issues and Solutions

Issue	Solution
Orgs T and Z don’t have their IdP since their HOs cannot afford it	1. Users register to a **Guest IdP**, known by the SP 2. Org subscribe an IdP as a Service (**IdP-in-the-Cloud**)
Orgs T and Z do have their IdP, but it is not registered in the National Federation, or the National Federation doesn’t exist	IdP registers itself in a **catch-all Federation** that is joint to eduGAIN or a New National Federation is set up
Orgs T and Z do have their IdP, registered in the National Federation, but the National Federation has not joined eduGAIN	National Federation joins eduGAIN
Orgs T and Z do have their IdP, registered in the National Federation, the National Federation has joined eduGAIN, but IdP didn’t opt-in to eduGAIN	National Federation change its policy from opt-in to opt-out

What do identified solutions imply ?

Solution	What needs to be addressed
Users register to a **Guest IdP**, known by the SP	• **Guest IdP needs to be registered in eduGAIN** • **Guest IdP needs to be managed in an accepable way (LoA)**
Org subscribe an IdP as a Service (**IdP-in-the-Cloud**)	**Cloud IdP needs to be a widely adoptable model**
IdP registers itself in a **catch-all Federation** that is joint to eduGAIN	• **Need the catch-all federation joint to eduGAIN** • **catch-all federation need to be managed in an accepable way (LoA)**
National Federation joins eduGAIN	**Long elapsing time**
National Federation change its policy from opt-in to opt-out for IdPs	**Long elapsing time**

SA1 Task 1 Goal

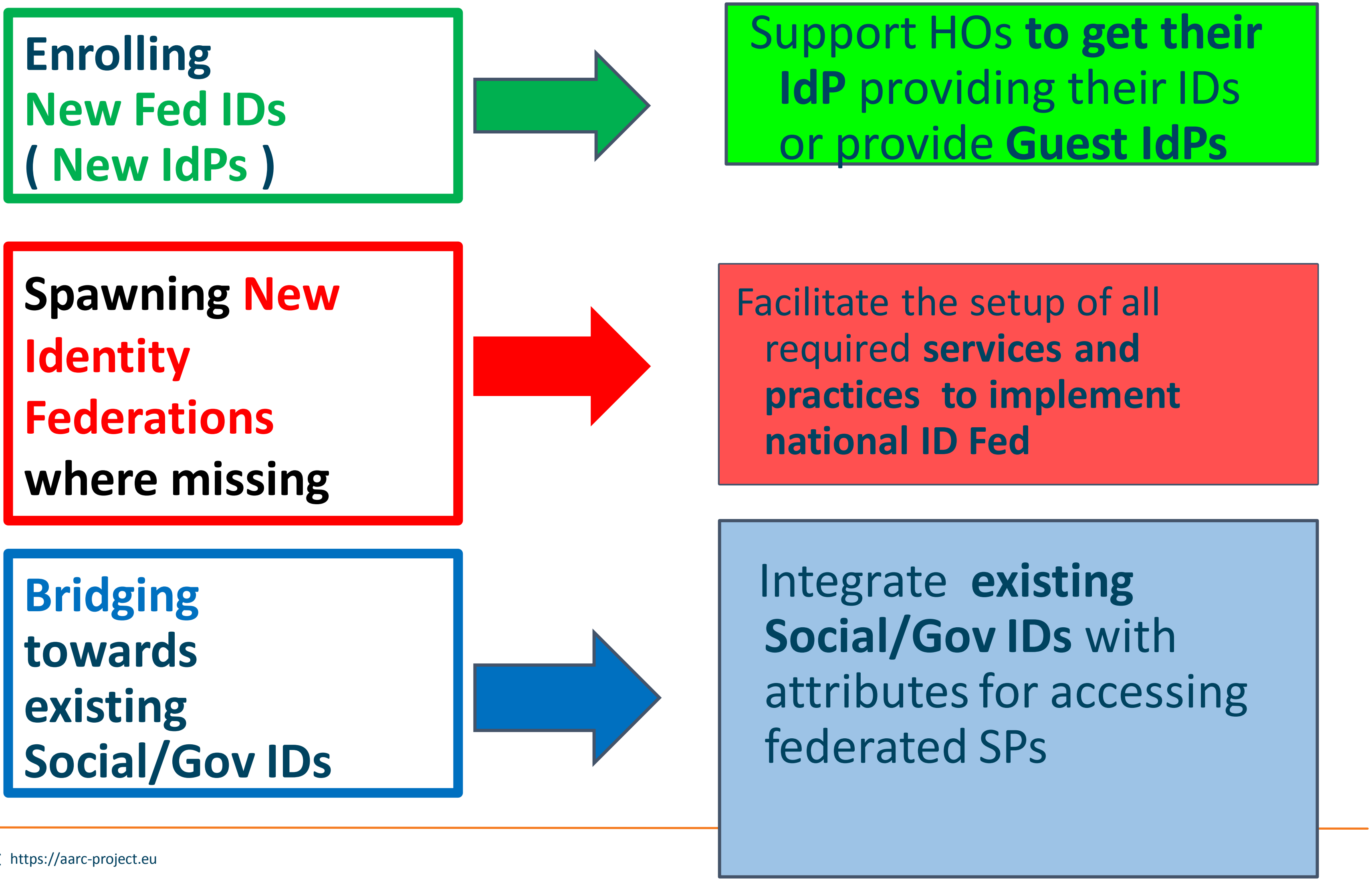
- **Implement pilots** on **supporting guest identities** according to the recommended solutions by JRA1-NA3
  - And prove their feasibility, involving user communities

Project Objectives on guest identities

- **Lower the entrance barriers** for organizations to adopt federated AAI
  - by providing them with solutions to get their IdP
  - and have it federated

- To **identify relevant use cases** within selected user communities for applying solutions and prove their effectiveness

Possible strategies to manage guest users



Enrolling New Fed IDs (New IdPs)

Support HOs **to get their IdP** providing their IDs or provide **Guest IdPs**

Spawning New Identity Federations where missing

Facilitate the setup of all required **services and practices to implement national ID Fed**

Bridging towards existing Social/Gov IDs

Integrate **existing Social/Gov IDs** with attributes for accessing federated SPs

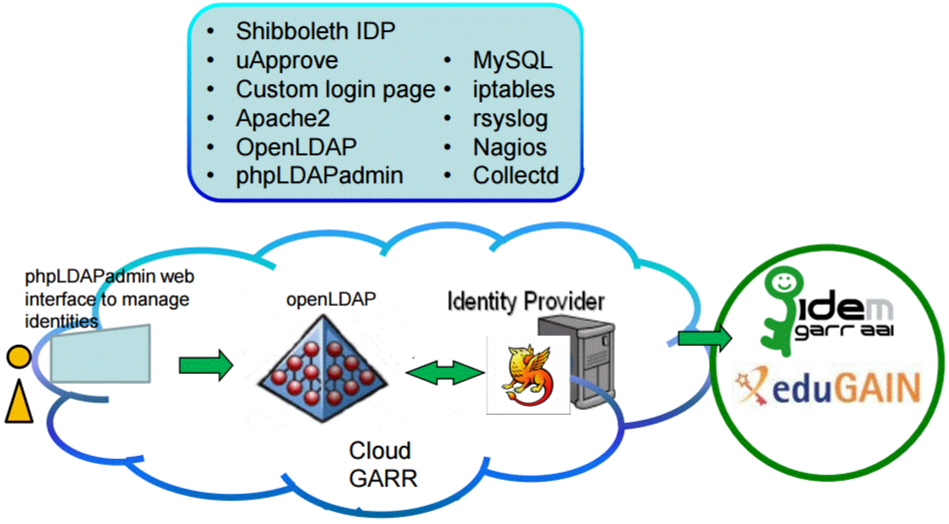
Identified paths to support guests

- **Provide an IdP** on the Cloud for organizations unable to set it up on their own (Cloud IdP)
    - Needs the IdP to be part of an existing Federation
        - or part of an “Homeless” Federation/Interfederation
- **Provide a Guest IdP** for users of specific communities (e.g. ERIC)
    - Needs the IdP to be part of an existing Federation
        - or part of an “Homeless” Federation/Interfederation

- **Promote new,** missing **national ID Federations**
    - IDFed-a-a-S
- Implement a **bridge towards trusted social network or governmental identities**
    - Entitlement ? Integrate ID with misssing authorizing attributes ?
    - Need to have reference, linked Attribute Authorities (eg.ERIC) to enhance LoA
    - How do we (R&E) want to deal with Social-IDs and Gov-IDs ?

New Fed-IDs: Cloud-based IdP (IdP-a-a-S)

- Cloud IdP hosted by National ID Fed managing remote HO identities
  - **GARR** currently hosting ~ 20 IdPs belonging to IDEM (National ID-Fed)
- Deployment and Configuration based on automated procedures and tools (Puppet)
- Can this approach **be made more general/widely adoptable** ?



- Shibboleth IDP
- uApprove
- Custom login page
- Apache2
- OpenLDAP
- phpLDAPadmin
- MySQL
- iptables
- rsyslog
- Nagios
- Collectd

New Fed-IDs: Guest IdP

- An IdP could be set up for guests of specific user communities

- Issues to be addressed:
  - Level of Assurance: how to enhance it   (NA3)
  - Link to Attribute Authorities
  - Management of Guest ID
    - Legal entity in charge ?

New Fed-IDs: Catch-all federation ?

- A Catch-all federation joined to eduGAIN could provide a home to IdP without a reference National Federation Identity
  - How to set it up ?
  - How to manage it
    - eduGAIN could manage it where Nat Id Fed do not yet exist

New Federations : Federation-a-a-S

- There are on-going activities in GN4 on this topic
  - We should liaise with them

Bridging towards Social and Gov-IDs

- Activities on going in AARC JRA1 and GN4
  - OAuth2 vs SAML2 bridge
  - + AA managed by ERICs

Target communities to be involved in pilots

- Public Libraries in the R&E domain
  - dealing with online publishers / editors

- Social Science and Humanities / Cultural Heritage

- Health Science

Libraries

- **Additional components** are involved in the process of accessing online full-text resources
  - Structured query tools, DOI, URL-resolver
    - Pilot should be set up **with hands-on these tools**

- **IP-based AuthN** still plays a relevant role in many cases
  - A roadmap for moving towards federated AuthN has to be established

- SA1 task1 will liaise with JRA1, NA3 and other project partners to design a specific use case

Health-Science and Cultural Heritage communities

- Cloud-IdP approach to be further pursued and extended
- New possible interested institutions will be sought for
- How to extend this model and make it scalable and sustainable ?
  - So that many federations could adopt it

Steps ahead

- **Liaise with JRA1 and NA3** to design pilot architectures
- Organize Working group to design a **specific pilot involving Libraries**
- Design a strategy for Gov and Social ID and how to bridge them into the Federated model   (JRA1, NA3)
- Hardware resources available from GARR to implement pilot services (DELL Blade servers attached to FC-Storage)
- **Contributions from other partners** are welcome !