Authentication and Authorisation for Research and Collaboration

Pilots on the Integrated R&E AAI

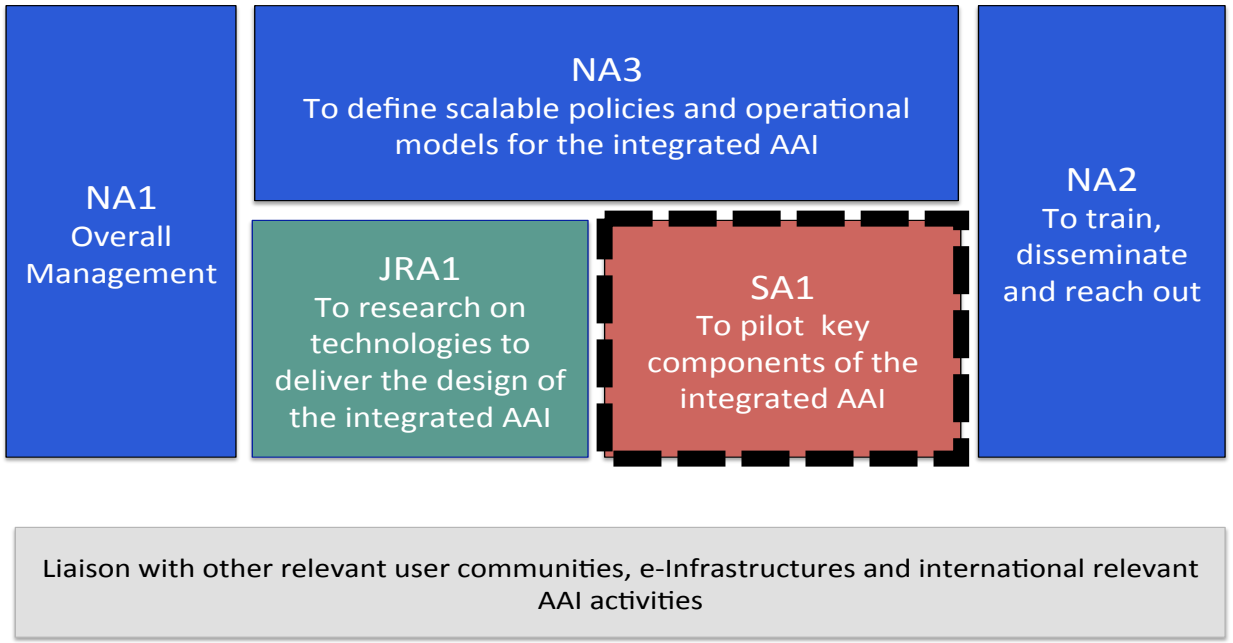
An overview of the “SA1” activities

Paul van Dijk, Activity Lead Pilots (SA1)

SURF NET

AARC Kick-Off Meeting
June 2015

AARC Work Packages



Current AAI landscape

Nat'l AuthN ✔ *.....many successful national implementations*

"Guest" access ✗/✔ *.....some ad-hoc solutions, not standardized, LoA??*

Int'l AuthN ✗/✔ *.....framework available but needs optimization*

Attribute management for AuthZ ✗/✔ *.....available in some communities, others just started*

Non-web SSO ✗ *.....a huge challenge, royal route or workarounds??*

However, many components available to improve current practice

status *– need overview, architecture and PoC/Pilots/Demo's of components to determine: for which use case?, compatible with?, maturity?, suitability? When do components fit together, when not?*

Goals/Approaches Pilots (SA1)

- Demonstrate that the solutions identified and proposed by JRA1 and NA3 are effective in addressing the requirements of the communities
- Proof of concepts will involve services from the main e-infrastructures in Europe
- Show to what extent different technologies used by the e-infrastructures and service providers are compatible and interchangeable
- (Re-)using not building

Task1: Pilots of solutions for “guest” users

Lead: GARR - Mario Reale, Barbara Monticini, Lalla Montovani

- Lower barriers for entry of organisations not already participating in identity federations
- Showcase viable solutions whether commercially available or R&E community supported for guest access to shared resources
- Showcase ways to support scalable LoA for guest users
- Showcase AAI Approaches for research libraries

Task2: Pilots of an attribute management framework

Lead: EGI - Peter Solagna

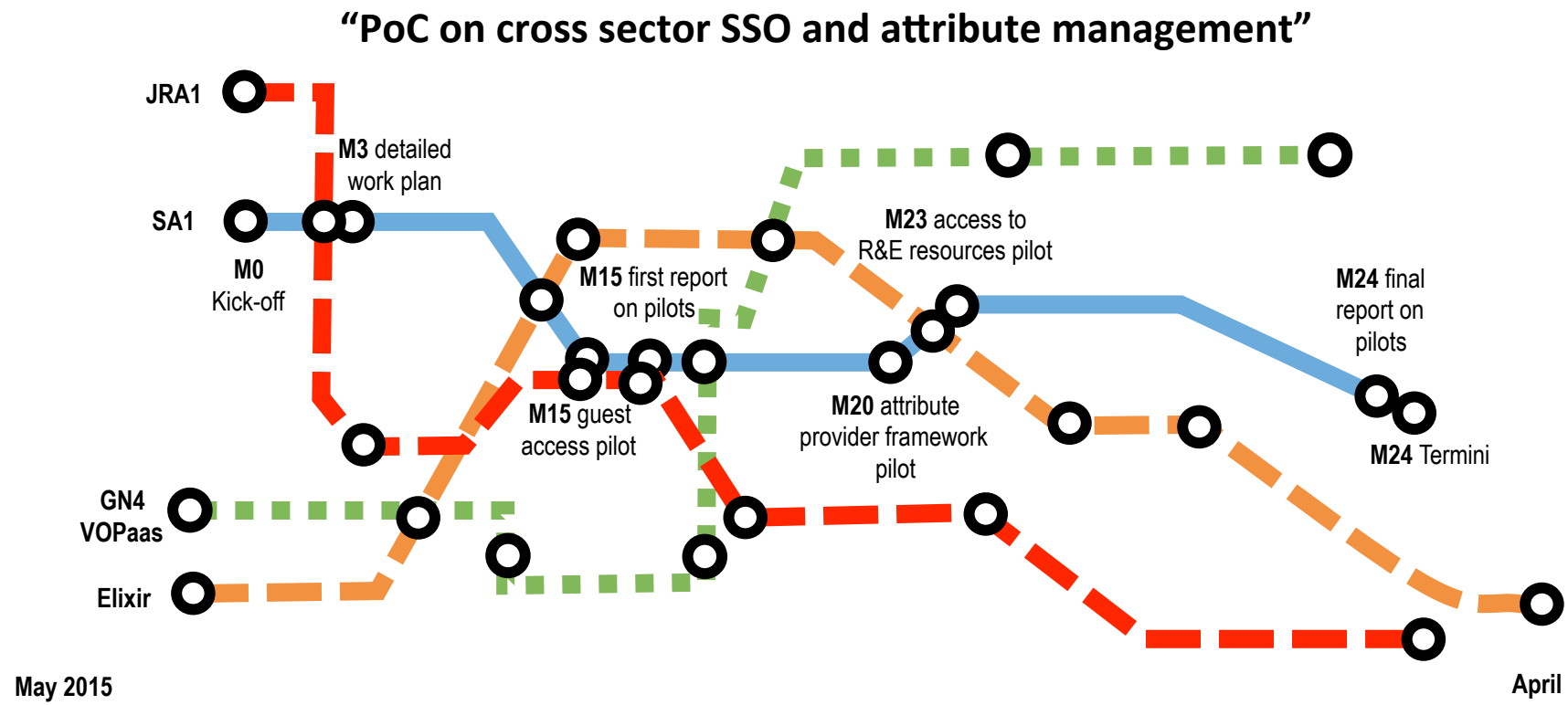
- Attribute management: identify tools and services that better support the registration and management of attributes by the research communities
- Attribute aggregation: multiple scenarios for attribute aggregation are expected to result from the attribute framework definition
- Attribute based authorisation: service providers will base authorisation on a combination of IdP and community provided attributes

Task3: Pilot to improve access to R&E relevant resources and services

Lead: PSNC - Maciej Brzeźniak, Michal Jankowski

- To provide AAI mechanisms to access (non-web) resources relevant for the R&E communities
- To pilot mechanisms identified in JRA1 to integrate services that are not yet accessible via the federated framework
- To pilot SSO access for commercial (cloud) services for research communities and consider both technical/architectural solutions (in collaboration with JRA1) and legal and policy aspects (in collaboration with NA3)

Time line, pre-set mile stones, and deliverables – The AARC-Pilots Metro Map



Agenda – Planning the work ahead...

4th June

Time	Activity
09:00-10:30	**Planning the work ahead: working sessions**2. AARC architecture and pilots: finding dependencies and synergies, *Christos Kanellopoulos* and *Paul Van Dijk*3. Training and Outreach session, *Alessandra Scicchitano*

Participation of partners per pilot task (tbd)

	"guest" users (task1)	attribute management (task2)	access to (non-web resources) (task3)	person-months Involved	comments
SN				23	
PSNC			**LEAD**	12	
EGI		**LEAD**		11	
GARR	**LEAD**			6	
FOM/NIKHEF				10	
CESNET				8	
GRNET				8	
KIT				8	
DAASI				7	
CSC				4	
Moravian Libary				1	

Thank you

Any Questions?

paul.vandijk@surfnet.nl

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. 653965 (AARC).

Authentication and Authorisation for Research and Collaboration

Pilots for guest identities (Task1)

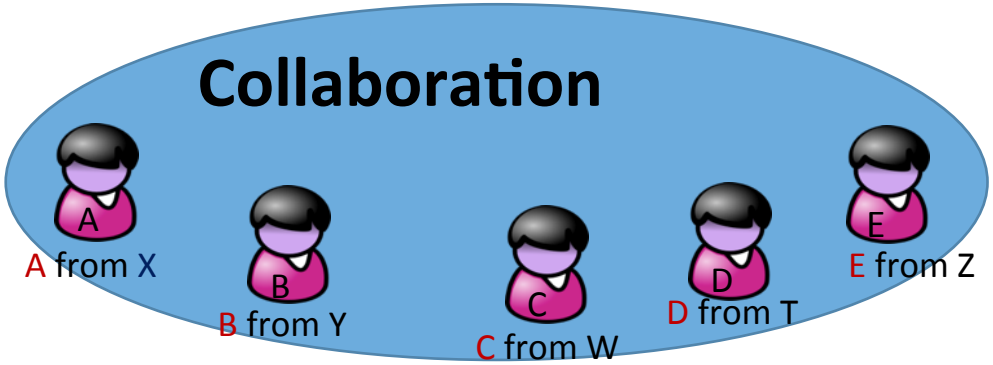
How do we provide "assured" access for non-academic users or academic users from *«?»*

- Mario Reale
- Barbara Monticini
- Lalla Mantovani

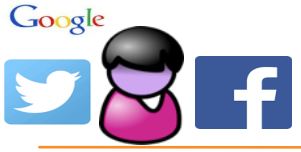
GARR

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

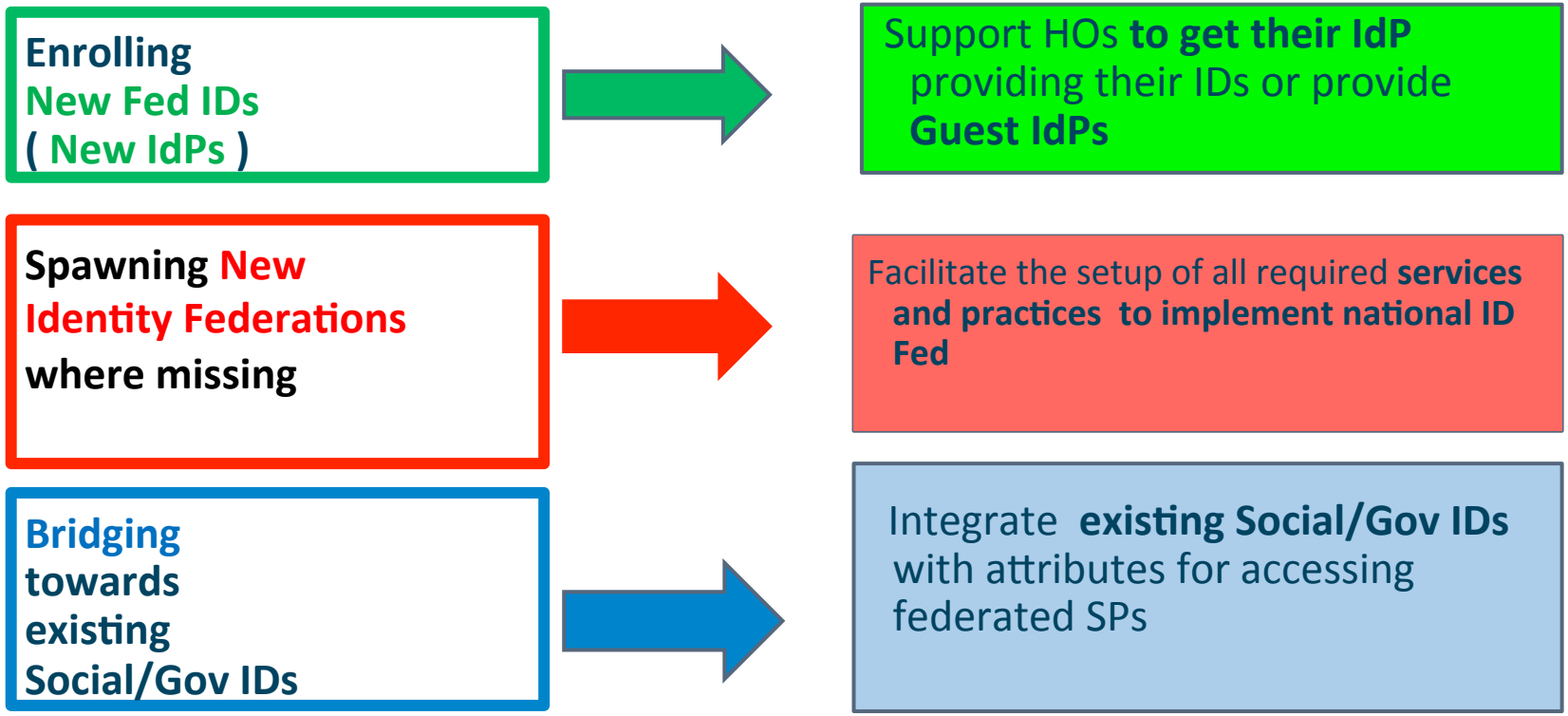
- **Implement pilots** on **supporting guest identities** according to the recommended solutions by JRA1-NA3
  - And prove their feasibility, involving user communities

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



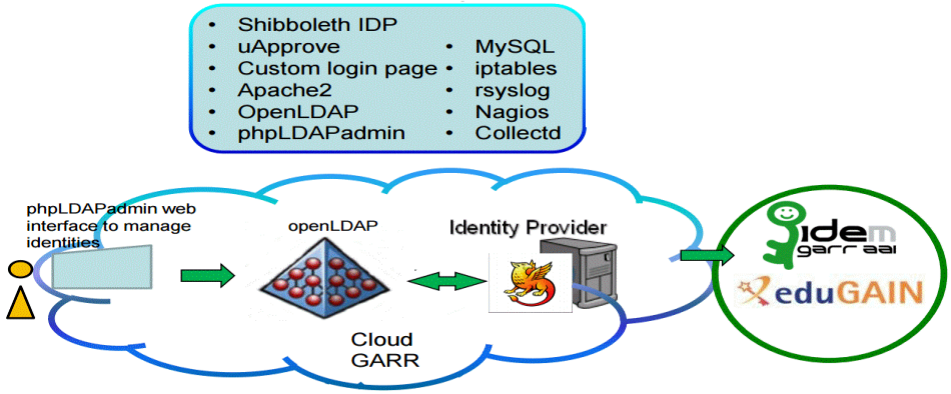
Identified paths to support guests

- **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** ?



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 !

Authentication and Authorisation for Research and Collaboration

Attribute Management (Task2)

Managing attributes, tooling, approaches...

- Peter Solagna – EGI.eu
- peter.solagna@egi.eu

Authorization through attribute management

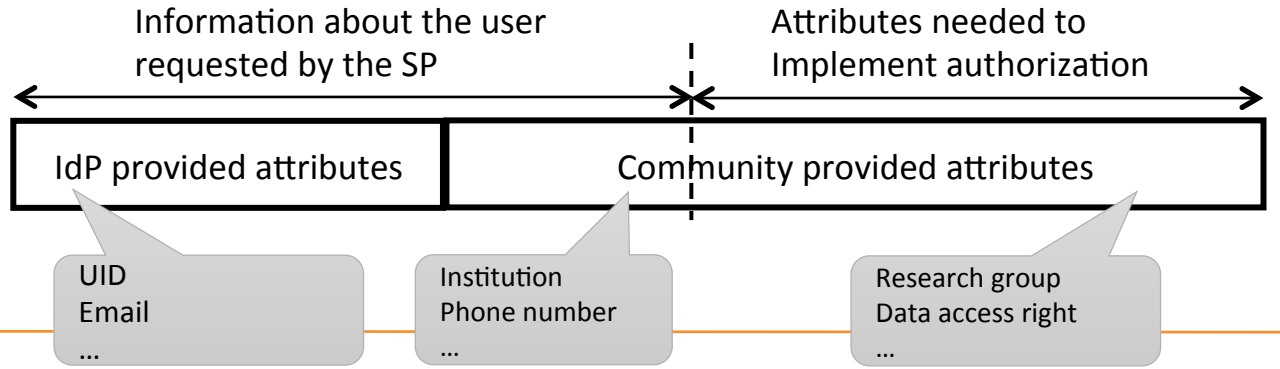
- In federated/distributed service provisioning AuthN and AuthZ information cannot be configured at service level for every service
  - Service providers need attributes associated to users' identities to information to implement authorization in the services
- Attributes should be managed by the research communities as much as possible
  - The community knows who a user is, and what he/she is allowed to do
  - Service providers often do not know the internal organization of a community
- An example of collaborative - attribute-based – authorization is already successfully implemented in EGI using X509 credentials
  - There are many other solutions based on other technologies

Role of attributes management in enabling access to services

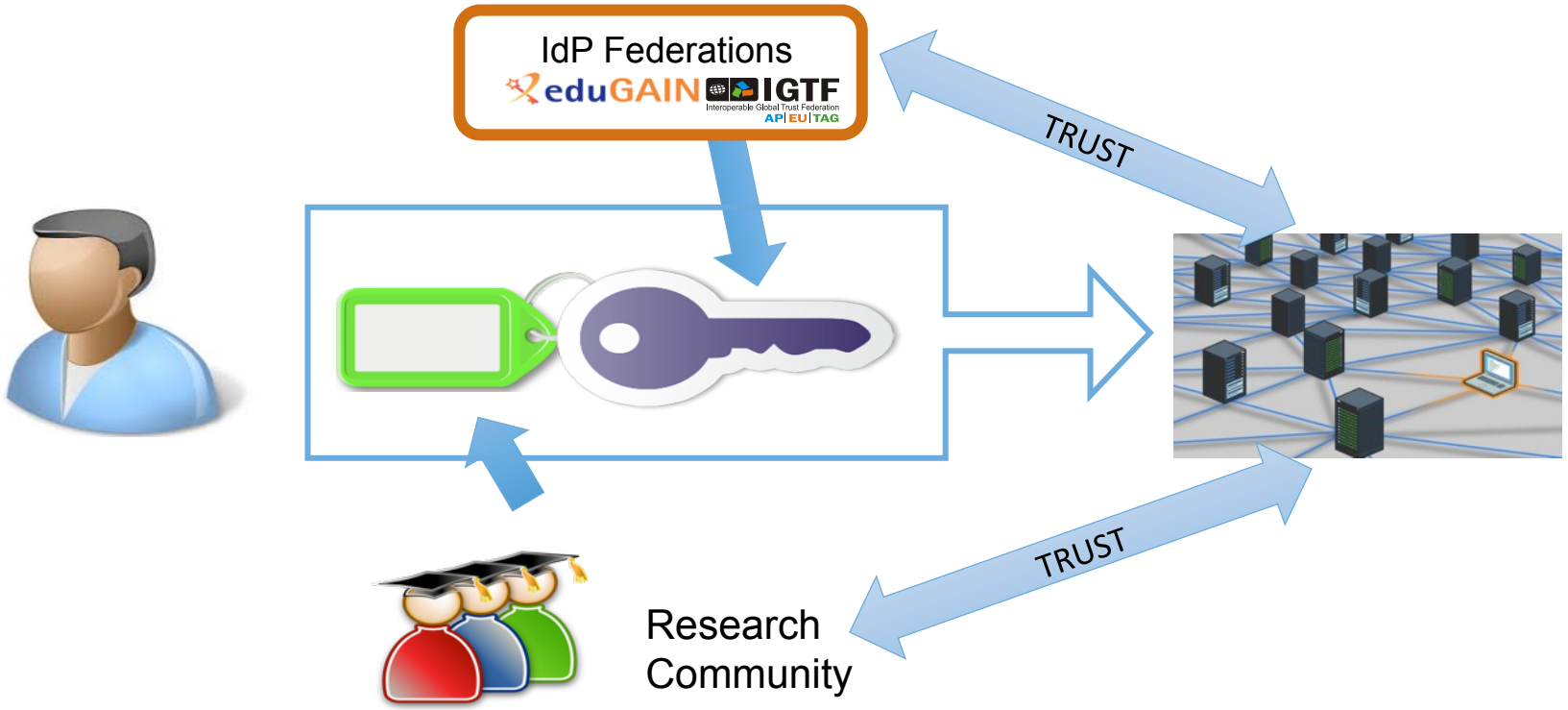
Community-managed attributes are important in accessing the services at two levels:

- Integrating the attributes provided by the IdP, providing information that are not released but are necessary to access the services.
  - This is important in every use case, from large organizations to individual users who need to get access to e-infrastructures/ federated service providers
  - When service providers need attributes not provided by the IdP (e.g. affiliation, or phone number) users must provide them

- Providing the attributes that qualify the user's capabilities within the organization and the actions that the user is authorized to perform on the services
  - User communities have the control on the actions that users can perform
  - Users groups, user capabilities can change without the need to directly interact with service providers



Collaborative authorization in federated services



Attribute Management

- Attribute management solutions although not commonly used are increasing in popularity, particularly within research infrastructures who are in an advanced development status
- Still the use of third-party attribute providers for user authentication and authorization is not widely enabled among service providers
- Pilot activities:
  - Attributes management services
  - Attribute aggregators
  - Services capable to consume attributes to implement authorization
  - Test in simple use case scenarios and real users workflows
    - Some preliminary work: https://wiki.egi.eu/wiki/AAI_pilot
- Attribute providers to evaluate:
  - VOMS
  - HEXAA
  - UNITY
  - PERUN
  - REMS
  - …

Attribute Management pilots timeline

- Generic testing of attribute providers for user authorization (June-August)
- Analysis of the use cases/requirements and deployment of related pilots (September-December)
- Extension of the pilots with the results of the JRA1 architecture suggestions (November- …)
- Attribute management pilots must be integrated with the other pilots to implement a coherent architecture

Authentication and Authorisation for Research and Collaboration

Task 3: Access to resources
Non-web & Commercial services

- Maciej Brzeźniak
- Michal Jankowski
- - PSNC -

Aims of the task

- To provide AAI mechanisms to access (non-web) resources relevant for the R&E communities (i.e. FIM4R)
- To pilot mechanisms identified in JRA1 to integrated services that are not yet accessible via the federated framework.
- To pilot SSO access for commercial (cloud) services for research community and consider both technical/architectural solutions (in collaboration with JRA1) and legal and policy and legal aspects (in collaboration with NA3). This work will build on the results of the service activity “Support to cloud” that is part of the the GN3plus.

AAI mechanisms to access (non-web) resources - problems to solve

- Dislike web-based services federated access to non-web ones is not common
- Mechanisms like redirection or client-side scripting are not present
- The existing software (e.g. ssh clients and servers) is not ready
  - building the software from scratch is not feasible
  - most solutions need modification both client and server side
- Service-specific requirements may exist

AAI requirements for non-web services

- Possibly no intrusion in existing software, especially on client side
  - maintainability
  - no need to change used so far client software
- The user uses credentials from his home organization
- Provisioning or deprovisioning of local user context
- Security
  - not worse than in non-federated environment
  - trust relationship
- Reasonable performance

Example services to be integrated

- Access to storage services through SSH

in Poland we run large backup/archive service PLATON-U4 for now accessible by SSH + X.509 authentication, which is not very elastic; we believe trial to federate the access through existing non-Web SSO solutions will provide interesting real-life challenge

- Access to virtual machines

there is an service where auth/authn is based on some enrollment process supported by a home-grown solution

- Access to sync&share services

e.g. based on Seafile, ownCloud etc.

Considered technologies

- FACIUS
  - “An easy to deploy SAML-based approach to federate non-web based services”
- LDAP Facade
  - Appears to be a local LDAP directory
  - SAML-based service provider component
- Moonshot
  - EAP/RADIUS authentication
  - SAML-based authorization
  - GSS-API application integration
- CI-Logon
- …

Thank you

Any Questions?

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. 653965 (AARC).