



Authentication and Authorisation for Research and Collaboration

NA2 Overview

(AARC2.AHM)³

Andrea Biancini

NA2 WP leader

Reti SpA

Reti

Business & IT Consulting

AARC2 Third all-hands meeting, Αθήνα

April, 13th 2018

Outreach & Communication

Communication and Outreach – past year

Updates – 1/5



✓ News – 14 blogs

- User stories
- FIM4R
- Sirtfi
- AEGIS
- Training
- Project meetings



See all [AARC news blogs](https://aarc-project.eu)

Communication and Outreach – past year

Updates – 2/5



✓ CONNECT articles

- Edition 28 – March 2018
 - eduGAIN & AARC
 - pilots
- Edition 27 – Di4R edition
 - Christos AEGIS interview



See current and past editions of **CONNECT**



Communication and Outreach

Updates – 3/5



✓ Partner outputs

- EGI newsletter article upcoming on AEGIS
- GARR article incl. LIGO & CTA user stories



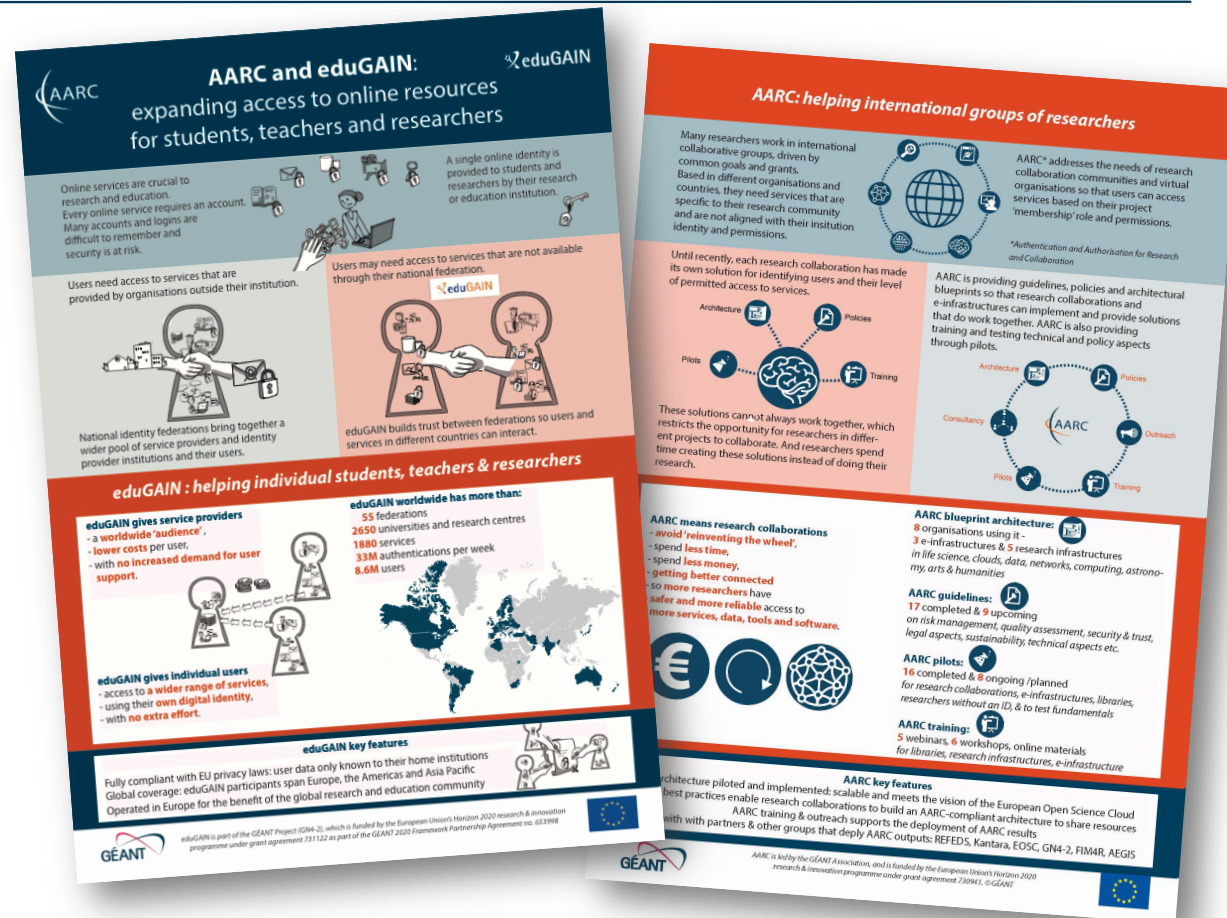
Communication and Outreach – past year

Updates – 4/5



✓ EC material

- Initial leaflet eduGAIN & AARC
- Definitive version imminent



Communication and Outreach – past year

Updates – 5/5



- ✓ Social Media
- ✓ All news posted on our 3 channels
- ✓ Engagement low
 - Twitter – 115 followers
 - 7 here at the meeting...
 - Facebook – 52 followers
 - LinkedIn – 6 followers

Show of hands!

Communication and Outreach

Ongoing / in planning



✓ NEW!:

- New section of website & pdf
- Case studies / user stories
 - Quotes / testimonials
- Promote via news etc.
- Cross-link with relevant project activity pages
- Restructure top-level landing pages

Cherenkov Telescope Array

The *Cherenkov Telescope Array (CTA)* will be the major global observatory for very high-energy gamma-ray astronomy over the next decade and beyond. CTA will be operated as an open, proposal-driven observatory, with all data available on a public archive after a predefined proprietary period.

CTA is a collaboration between 1350 scientists and engineers from 32 countries, set up with the mission to direct CTA's science goals and array design. When in production, CTA will collect the data scientists need to understand the role of high-energy particles in the most violent phenomena of the Universe and to search for annihilating dark matter particles.

The AAI challenge

Preparing the IT infrastructure necessary to process, distribute, analyse and store the Petabytes of data expected annually from the CTA is a huge challenge. Getting an Authentication and Authorisation Infrastructure (AAI) in place to serve thousands of scientists is not simple either.

The current CTA AAI implementation provisions more than 1000 consortium SAML identities and is releasing a persistent and non-reassignable ID as defined by CTA user requirements. The authorisation is performed through a dedicated Attribute Authority which grants the definition, management and provisioning of roles based on groups and subgroups.

Working with AARC

The CTA team set up a pilot to improve their service using elements of *AARC's Blueprint Architecture*.

The pilot will expand the AAI capabilities to secure the CTA resources and digital assets through role-based authorization allowing federated authentication based on the centralised SAML service and on eduGAIN. The first release is planned for the Summer of 2018.

Why AARC?

For the CTA team, working with the AARC project means that they don't have to invent an AAI service from scratch. They can save time building a custom system based on best practices and tried and tested solutions.



"The AARC Blueprint Architecture represents the possibility for us to speak with other technological partners using a common language describing AAI and its complex world."

Alexandro Costa, National Institute of Astrophysics (INAF) and CTA.

CORBEL – biomedical Research Infrastructures

CORBEL is a collective of thirteen research infrastructures (RIs), working together to create a platform for harmonized user access to biological and medical technologies, samples and data services required by cutting-edge biomedical research.

The data and computational tools offered by the individual research infrastructures are indispensable to the scientists that used them. Collectively, through CORBEL, these services will have a larger impact across the entire range of life-science disciplines: from discoveries in the lab to personalized treatments.

The AAI challenge

Key to the success of the CORBEL platform is a sustainable and robust Authentication and Authorisation Infrastructure (AAI). The AAI is crucial to manage the access of hundreds of users from many institutions spread across different countries to the services and data provided by the platform. On top of that, because CORBEL operates with medical and privacy-sensitive data, the AAI will need to support mechanisms to manage permission of access to different groups.

Working with AARC

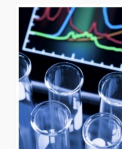
The main focus of CORBEL is science, not building AAI solutions, so the project opened a call for an AAI Architecture that would answer their requirements.

The EGI Federation, EUDAT and GÉANT, joined forces to propose an AAI solution based on the *AARC Blueprint Architecture* and on AARC's *Guidelines and Policies*. This AAI solution is now being piloted in the context of the AARC project.

AARC Pilot

The pilot started in December 2017 and is being rolled out in three stages:

During **Phase 1** the team bootstrapped the AAI solution by putting components together and defining the user registration process, attributes required by service providers and the authorisation flow. This has ended in January 2018.



Communication and Outreach

Ongoing / in planning



✓ NEW!:

- Newsletter for final year
 - Promoting AARC case studies, pilots, guidelines, blogs, policies, architecture updates etc.
 - Also circulate content from relevant communities
 - 7 editions: May, July, September, November, January, March, April/May
 - Send to AARC2 mailing list **AND** a new opt-in list

- Possible longevity beyond AARC?

Name ideas?

Communication and Outreach

Ongoing / in planning



✓ Other current activities:

- Blog news articles
- CONNECT mag articles editions 29, 30
- Social media dissemination
- Review & update of materials online
- CEF / FIM4R communications
- AEGIS briefings & news
- EU materials
- Promote guidelines, training, outputs of pilots & architectures
- Preparations for EC Y1 review

Communication and Outreach

Ongoing / in planning



[@AARCproject](#)



[@AARC Project](#)



[AARC Project](#)

Next: **we need your inputs!**

- Partner outputs – [give us your PR colleague contacts](#)
- News – [let us know](#) if there's anything to report
- User stories / testimonials etc. – [help us get them!](#)
- Get sign-ups for newsletter – **share the subscription link (coming soon)**
- **Share, follow, like & tag** us on social media!

Training

The cookbook for Service Providers

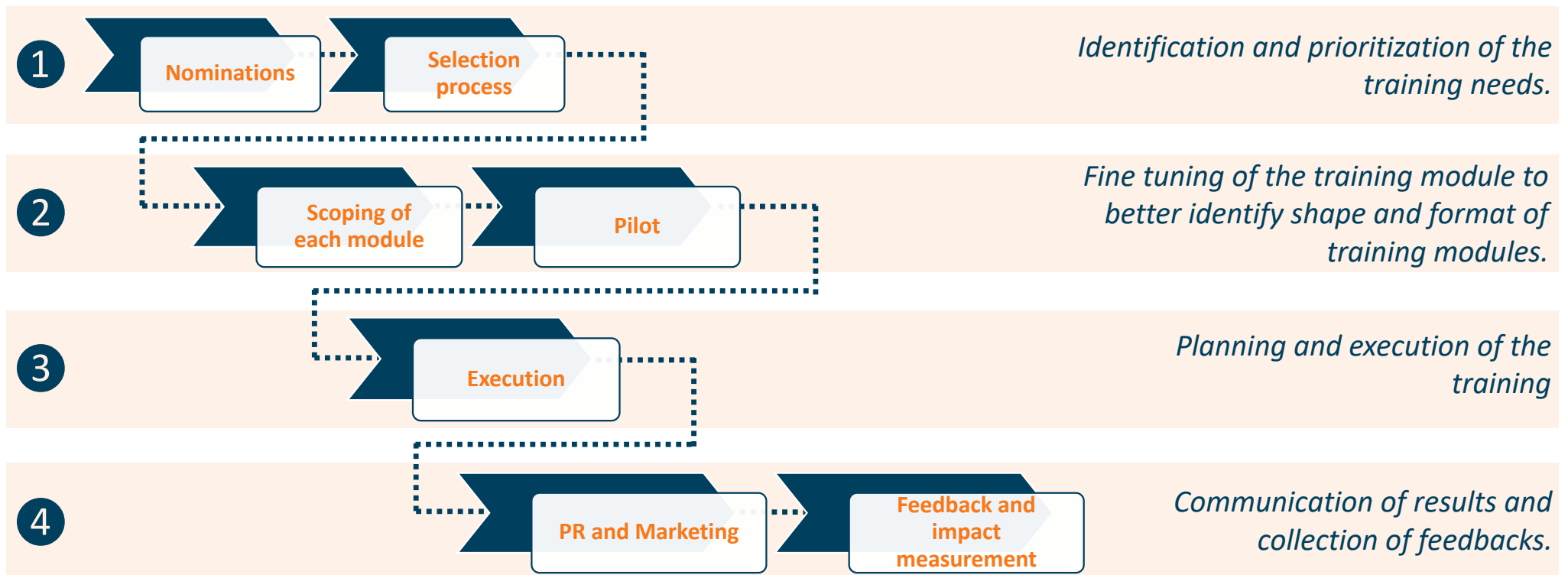
The NA2T2 team composition



Training Module	People		
Task Leadership	Mario Reale	(GARR)	
Participants	Andrea Biancini	(RETI)	      
	David Hübner	(DAASI)	
	Marco Malavolti	(GARR)	
	Irina Mikhailava	(GÉANT)	
	Uros Stevanovic	(KIT)	
	Hannah Short	(CERN)	

The AARC2 training process

High level description of the process phases



Feedbacks obtained

Topics with higher preferences



Topic	Preferences	
Introduction - Basic info on FIM - For everybody interested	2	
Scenarios - how to connect to IdPs - How to leverage external identities - For SPs dev/ops	4	EPOS (03.2018)
SP-focused advanced scenarios - Advanced use of FIM (i.e. non-web, OIDC, centralised authZ, etc) - For SPs dev/ops	9	mid 2018
AARC BPA - Blueprint architecture basic info - Mapping use-cases to blueprint architecture - For r/e-infras	2	
Technical components - How to implement technical components of the BPA - For r/e-infra and SPs dev/ops	6	
Policy - Basic info on how to implement policies for international collaborations - Specific info GDPR, Sirtfi, Snctfi	9	ASAP

Training for EPOS – 1/3

Introduction to FIM, AAI and OIDC



1. What do we want to achieve? (course learning goals)

Introduction to AAI concepts and federated access to share a common model of knowledge and to move AAI infrastructures forward for the EPOS community.

2. For who this course is?

Different AAI stakeholders from EPOS community (expected around 15 participants).

3. What the format should be (f2f, online, etc)?

Face to face training during the annual EPOS meeting in Lisbon on March 12-14, 2018.

4. What are the manageable chunks of the course? (course main arguments)

- *which are the major scenario service providers have when dealing with identities (internal authentication, external authentication, federated access)*
- *what kind of functionalities an AAI can provide to research infrastructures*
- *what work AARC has done (blueprint architecture, pilots, etc)*

Training for EPOS – 2/3

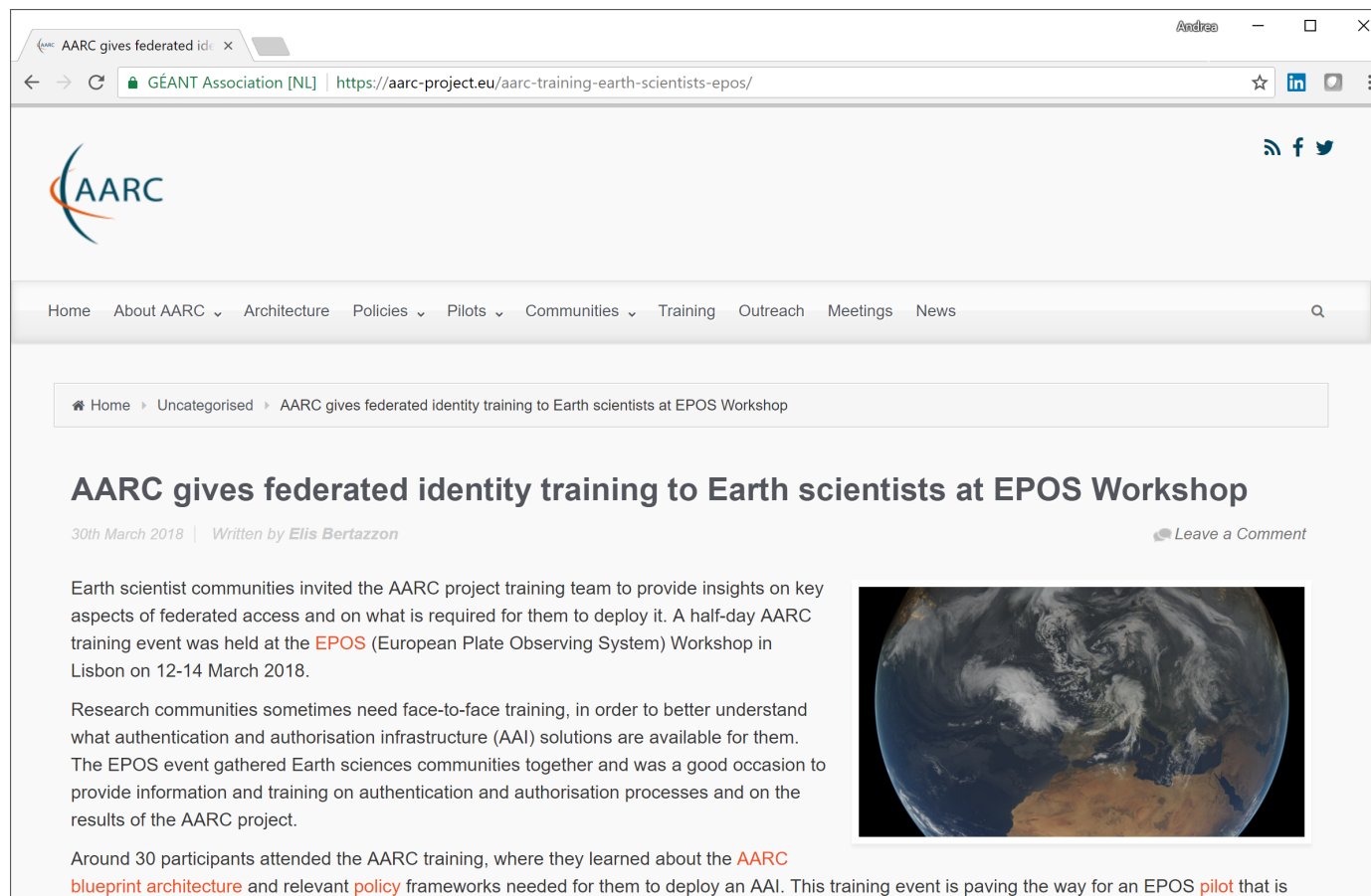
Introduction to FIM, AAI and OIDC



AARC		Training for EPOS	
		Agenda	
14 March 2018 - Morning:			
Course introduction			
• Course objectives and agenda			
• Introduction of the participants			9:00 - 9:30
AAI overview			
• Authentication and authorization processes			
• Externalizing authentication (LDAP)			
• Federated authentication (SAML and OIDC)			9:30 - 10:30
• Federations in R&D			
• The inter-federation: eduGAIN			
How to start federating			
• What is an SP, what is an IdP			
• Trust between SPs and IdPs			
• How to deal with authentication			
• How to deal with authorization			10:30 - 11:00
Break			
Setting up authentication with OpenID Connect			11:00 - 11:15
• Introduction about OpenID connect			
• Description of the OIDC authentication flows			11:15 - 12:15
• Authorization code flow			
• Example with Python			
• Implicit flow			
• Example with Python			
AARC BPA and project experiences			
• Goals of the BPA			
• The resulting diagram			12:15 - 12:45
• Example from other communities: the LS pilot			
Q&A, discussion and closing			
Lunch			12:45 - 13:00
Open Session			13:00 - 14:00
			14:00 - 15:00

Training for EPOS – 3/3

Introduction to FIM, AAI and OI DC

A screenshot of a web browser displaying an article on the AARC website. The browser's address bar shows the URL 'https://aarc-project.eu/aarc-training-earth-scientists-epos/'. The website header features the AARC logo and a navigation menu with links: Home, About AARC, Architecture, Policies, Pilots, Communities, Training, Outreach, Meetings, and News. A breadcrumb trail reads 'Home > Uncategorized > AARC gives federated identity training to Earth scientists at EPOS Workshop'. The article title is 'AARC gives federated identity training to Earth scientists at EPOS Workshop', dated '30th March 2018' and written by 'Elis Bertazzon'. The text describes a half-day training event at the EPOS (European Plate Observing System) Workshop in Lisbon, March 12-14, 2018. It mentions that Earth scientist communities invited the AARC project training team to provide insights on federated access and deployment requirements. The event gathered Earth sciences communities for face-to-face training on authentication and authorisation infrastructure (AAI) solutions. Around 30 participants attended, learning about the AARC blueprint architecture and relevant policy frameworks needed for deploying an AAI, paving the way for an EPOS pilot. An image of Earth from space is shown on the right side of the article.

Home > Uncategorized > AARC gives federated identity training to Earth scientists at EPOS Workshop

AARC gives federated identity training to Earth scientists at EPOS Workshop

30th March 2018 | Written by *Elis Bertazzon* [Leave a Comment](#)

Earth scientist communities invited the AARC project training team to provide insights on key aspects of federated access and on what is required for them to deploy it. A half-day AARC training event was held at the **EPOS** (European Plate Observing System) Workshop in Lisbon on 12-14 March 2018.

Research communities sometimes need face-to-face training, in order to better understand what authentication and authorisation infrastructure (AAI) solutions are available for them. The EPOS event gathered Earth sciences communities together and was a good occasion to provide information and training on authentication and authorisation processes and on the results of the AARC project.

Around 30 participants attended the AARC training, where they learned about the **AARC blueprint architecture** and relevant **policy** frameworks needed for them to deploy an AAI. This training event is paving the way for an EPOS **pilot** that is

Training for LifeScience – 1/2

Introduction to FIM, AAI and AARC pilot



1. What do we want to achieve? (course learning goals)

Introduction to AAI concepts and federated access to share a common model of knowledge and to move AAI infrastructures forward for LifeScience communities.

2. For who this course is?

Different AAI stakeholders from LifeScience communities (expected around 15 participants).

3. What the format should be (f2f, online, etc)?

Face to face training during the BMS AAI meeting in München on April 23-24, 2018.

4. What are the manageable chunks of the course? (course main arguments)

- *which are the major scenario service providers have when dealing with identities (internal authentication, external authentication, federated access)*
- *what kind of functionalities an AAI can provide to research infrastructures*
- *what work AARC has done (blueprint architecture, pilots, etc)*
- *introduction to the AARC2 Life Science pilot (requirements specification, results so far)*
- *"bring your own service" discuss next steps on a service proposed by a community*

Training for LifeScience – 2/2

Introduction to FIM, AAI and AARC pilot



CORBEL/AARC AAI Training	
Munich Airport Marriott Hotel, Alois Steinecker Strasse 20, Freising, 85354, Germany	
Agenda	
23 April 2018 - Day 1 - Afternoon:	12:30 - 13:00
Course introduction	
• Course objectives and agenda	
• Introduction of the participants	
• Course expectations	13:00 - 14:30
AAI overview	
• Authentication and authorization processes	
• Externalizing authentication (LDAP)	
• Federated authentication (SAML and OIDC)	
• Federations in R&E	
• The inter-federation: eduGAIN	14:30 - 16:00
How to start federating	
• What is an SP, what is an IdP	
• Trust between SPs and IdPs	
• How to deal with authentication	
• How to deal with authorization	
• The attribute release problem	16:00 - 16:15
Break	16:15 - 17:15
More advanced use-cases	
• Discovery service	
• Social identities	
• Account linking	
• Step-up authentication	
• Token Translation Services	
• Federate through a Proxy	17:15 - 17:45
Q&A and discussion	

CORBEL/AARC AAI Training	
Munich Airport Marriott Hotel, Alois Steinecker Strasse 20, Freising, 85354, Germany	
Agenda	
24 April 2018 - Day 2 - Morning:	
Day 2 Introduction	
• Quick recap of what learned in Day 1	
• Plan for Day 2	8:30 - 9:00
Examples of AAI	
• Why an AAI for community	
• eduGAIN	
• ELIXIR AAI	
• DARIAH AAI	9:00 - 10:00
AARC Project	
• AARC Introduction	
• Project's requirements	
• How eScience requirements are being addressed	10:00 - 10:30
AARC Blueprint Architecture (BPA)	
• Goals of the BPA	
• The resulting diagram	
• The main BPA components	10:30 - 11:00
Break	
The LifeScience pilot	
• Goals of the pilot	
• The pilots' main components	
• Pilot planning	11:00 - 11:15
Q&A, discussion and closing	
	11:15 - 12:00
	12:00 - 12:30

Policies starter workshop – 1/2

Introduction to the policy space

1. **What do we want to achieve? (course learning goals)**

The workshop aims to deliver an overview of policy provisions for research communities operating as a service provider proxy in an identity federation.

2. **For who this course is?**

The workshop is designed to support those making operational or management decisions for Research Communities operating as a service provider.

3. **What the format should be (f2f, online, etc)?**

Face to face training in Amsterdam on April 23, 2018.

4. **What are the manageable chunks of the course? (course main arguments)**

- *Head start on policy writing*
- *AARC's Snctfi framework with the special focus on:*
 - *Data Protection*
 - *Membership Management*
 - *Security Incident Response*
- *Expert and peer support and advice on pressing policy issues during a 'Peer2peer Forum'*

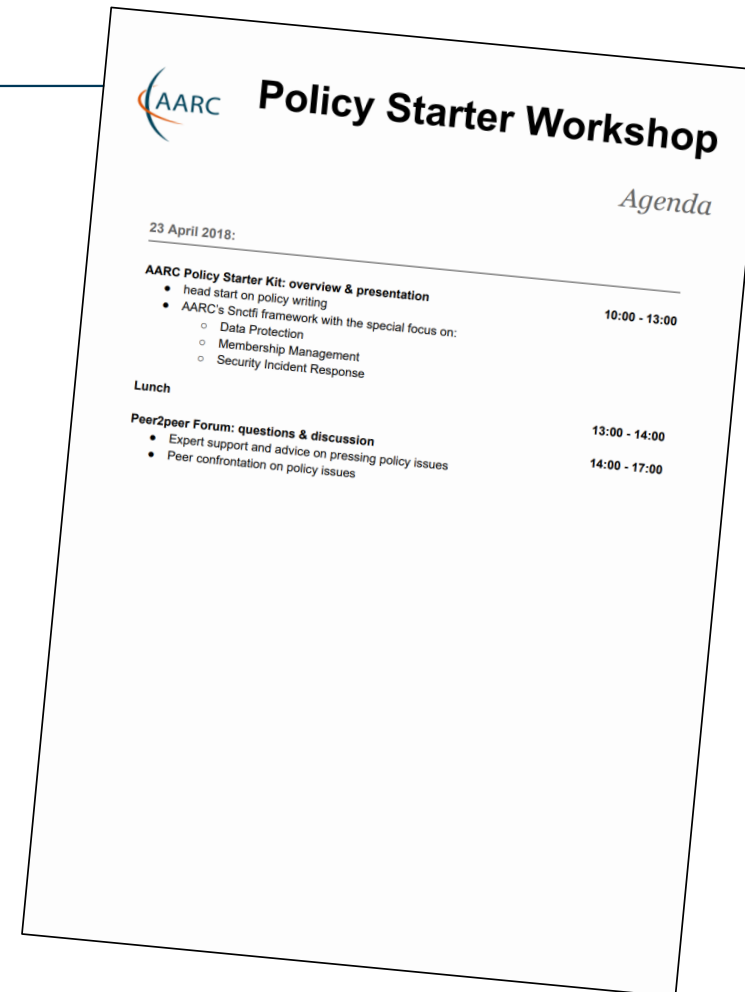
Training for LifeScience – 2/2

Introduction to FIM, AAI and AARC pilot



- ✓ *Only few subscriptions...*
- ✓ *What about it?*
- ✓ *Shall we move it later in Autumn?*

- ✓ *Maybe we could combine it with other initiatives (like the FIM4R workshop)?*



Courses organized in Y1

Training achievements



- ✓ June 27th, 2017 and July, 5th 2017 - **OIDC Primer, Rome** (*in collaboration with GARR*)
Introduction to the next generation identity management and authorisation protocols and their constituent components (OAuth2/JW*/OIDC/UMA).
<https://eventr.geant.org/events/2694> and <https://eventr.geant.org/events/2698>
- ✓ March 14th, 2018 - **Training for EPOS, Lisbon**
Introduction to AAI concepts and federated access to share a common model of knowledge and to move AAI infrastructures forward for the EPOS community.
<http://events.epos-ip.org/event/36/registrations/participants>
- ✓ April 23rd, 2018 - **Policies Starter Workshop, Amsterdam**
Overview of policy provisions for research communities operating as a service provider proxy in an identity federation.
<https://eventr.geant.org/events/2906>
- ✓ April 23rd, 2018 - **Training for LifeScience, Munich**
Introduction to AAI concepts and federated access to share a common model of knowledge and to move AAI infrastructures forward for LifeScience communities.
<http://meetings.infrafrontier.eu/meeting-tool/xhtml/corbelAAITrainingApr18.jsf>

Handbook for Service Providers

General idea and goals



- ✓ The [handbook](#) is intended to represent what AARC will leave as a legacy after project termination.

- ✓ The handbook is conceived around this principles:
 - It will end being a web-page or a wiki section
 - It will be a sort of TOC collecting all training materials developed within AARC or already available in different communities or projects
 - The handbook will structure the training materials in order to simplify the identification of the right training for interested communities

Handbook for Service Providers, status

Advanced Technical Training



✓ Setting up a Service Provider (Relying Party/OIDC Client)

First draft

✓ Recommendations for setting up a Discovery Service

First draft

✓ Analysing your authentication sources to design user-friendly authentication processes

First draft

✓ Planning which user information (attributes) your SP requires to work properly

Ongoing

✓ Best practices for managing authorization from the SP point of view

Ongoing

✓ Account linking: benefits and best practices/tips

Not Yet Started

✓ Activating and managing the step-up authentication

Not Yet Started

✓ What is an IdP/SP proxy

Not Yet Started

Handbook for Service Providers, status

Advanced training on policy



✓ Introduction	First draft
✓ Frameworks	First draft
✓ Policies	First draft
✓ Policy templates	First draft
✓ Additional policy of interest	First draft

Next Training Events

- ✓ To be determined (EISCAT3D?).
- ✓ We need to start a new nomination process and then move to selection...
- ✓ Any contribution, on the fly?

Thank you Any Questions?

andrea.biancini@reti.it



<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. 730941 (AARC2).