



30-04-2017

Deliverable DNA1.2: Annual Report

Deliverable DNA3.3

Contractual Date:	30-04-2017
Actual Date:	16-06-2017
Grant Agreement No.:	653965
Work Package:	NA1
Lead Partner:	GÉANT
Document Code:	DNA1.2
Authors:	L. Florio (GÉANT), L. Durnford (GÉANT)

© GÉANT on behalf of the AARC project.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document provides an overview on the AARC achievements after two year of project.



Table of Contents

Executive Summary	3
1 Introduction	6
2 AARC Targeted Communities	8
3 Main Achievements	9
3.1 Overall management	9
3.2 Training, outreach and dissemination	10
Training	13
3.3 Architecture	15
3.4 Policy	17
3.5 Pilots	19
Conclusions	23
References	24



Table of Figures

Figure 1: AARC Timeline and key results	6
Figure 2: AARC work packages	8
Figure 3: AARC interaction with other initiatives	9
Figure 4: AARC Strategy in a nutshell	10
Figure 5: The NA2 approach [x]	10
Figure 6: FIM for Libraries [FIM4Libraries]	11
Figure 7: Benefits for SPs to join eduGAIN [eduGAIN for SPs]	11
Figure 8: Recommendations for federations operators to better support SPs [6Steps]	11
Figure 9: Summary of AARC results [AARCResults]	11
Figure 10: What is AARC? [VIDEO]	12
Figure 11: AARC postcard	12
Figure 12: Requirements at the start of AARC	15
Figure 13: Requirements at the end of AARC. In blue, are the requirements which have been addressed in AARC-BPA-2017.	15
Figure 14: AARC Blueprint Architecture 2017	16
Figure 15: Relation between the AARC blueprint architecture, eduGAIN and the GÉANT network.	17
Figure 16: Sirtfi key aspects	18
Figure 17: Making AARC results sustainable	19
Figure 18: Sirtfi key aspects	19
Figure 19: AARC Pilots leaflet	20
Figure 20: IGTF-to-eduGAIN Pilot	21
Figure 21: RCAuth Pilot	21
Figure 22: Library Pilots leaflet	22
Figure 23: EUDAT-EGI Pilot	22

Executive Summary

The Authentication and Authorisation for Research and Collaboration project, AARC, worked to define a trust framework that champions federated access, removes the need for multiple accounts, improves user experience and preserves security and privacy.

The project ran between May 2015 and April 2017 and gathered 20 partners, among NRENs, e-infrastructures, research service providers and libraries.

AARC work was driven by the principles to support collaboration across institutional borders required by large-scale research initiatives, and to promote the use of federated access for research infrastructures, e-infrastructures and libraries.

The table below shows AARC's objectives and its achievements.

AARC Objectives	Achievements
To deliver a cross-discipline AAI framework built on federated access and the relevant set of policies to support scientific collaboration and to secure access to shared resources. The integrated AAI is referred to as the AARC blueprint architecture.	<p>Two incremental iterations of the AARC Blueprint Architecture.</p> <p>Three main policy frameworks:</p> <ul style="list-style-type: none"> • Sirtfi, (security incident framework, in collaboration with REFEDS) • Snctfi (to define security policies for the IdP-SP proxy proposed by the AARC blueprint architecture) • baseline and differentiated assurance profiles <p>Furthermore:</p> <ul style="list-style-type: none"> • recommendations on handling personal data for accounting purposes, • recommendations to build sustainable services.
To pilot critical components of the blueprint architecture, and of the AARC proposed policy frameworks that meet the AARC communities' needs and address operational and security aspects.	<p>AARC produced in total 18 pilots; 2 of these are now production services:</p> <ol style="list-style-type: none"> 1. IGTF-to-eduGAIN is now operated by GRNET 2. RCAuth (also called CILogon-like) is operated by Nikhef, but plans are for EGI, EUDAT and GÉANT to jointly operate it in the EOSC.

<p>To offer tailored training to increase the uptake of federated access (in terms of more users that can access services as well as by enabling federated access for services used by the AARC-targeted communities).</p>	<p>AARC delivered:</p> <ul style="list-style-type: none"> • Federation 101 module • 3 training for SPs • a plug-fest training for developers • train-the-trainer training on attribute release • two value propositions training for libraries • A number of different webinars
<p>To validate the results of both the research and service activities by promoting them among libraries, research and e-infrastructure communities (some of them working in the AARC project).</p>	<p>AARC produced the library toolkit, the infrastructure toolkit, webinars and different types of leaflets.</p>
<p>To increase the uptake of federated access within different research communities.</p>	<p>AARC promoted the adoption of federated access among the libraries, supported the adoption of federated access in EGI, worked with NRENs partners in AARC to migrate two pilots into production (IGTF-to-eduGAIN and RCAuth) which effectively means that more researchers can use federated access.</p>

The picture below depicts the AARC timeline with the key achievements, available also online at: <https://aarc-project.eu/roadmap/>

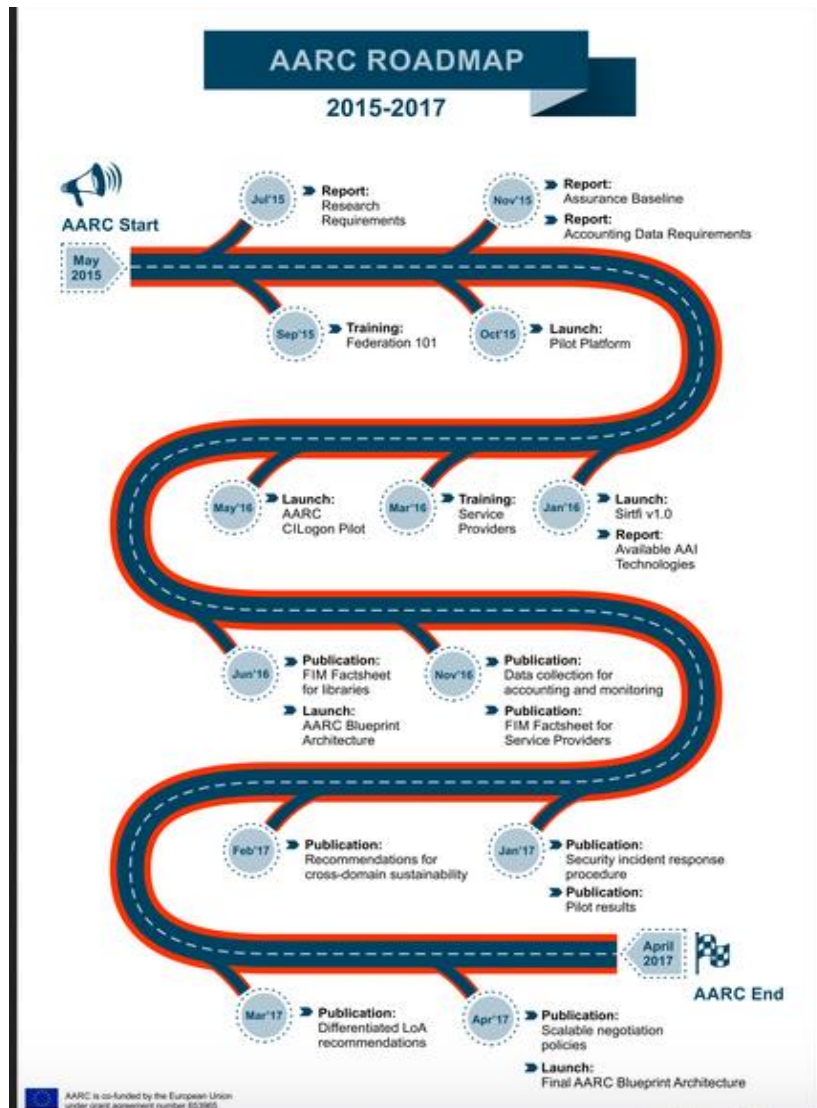


Figure 1: AARC Timeline and key results

1 Introduction

The Authentication and Authorisation for Research and Collaboration (AARC) project, gathered 20 partners covering different communities, with GÉANT acting as project lead, including:

- Nine NRENs with significant expertise in operating identity federations and all participating in eduGAIN (CESNET, CSC, DFN, GARR, GRNET, Jisc, PSNC, RENATER, and SURFnet).
- e-Infrastructures service partners, including EGI.eu, FOM-NIKHEF, CERN, STFC, KIT, Jülich and SURFsara.
- Libraries, represented by LIBER and their partner MZK.
- One SME (DAASI).



The AARC project worked to define a trust framework to champion federated access across e-infrastructures, research infrastructures and libraries. Via this framework, AARC seeks to facilitate interoperability and shared service delivery across existing and future R&E authentication and authorisation infrastructures and more in general research collaborations.

The project was organised in five work packages:

- **Management (NA1):** This work package was in charge of providing all the necessary tools, processes and procedures to ensure a smooth operation of the project. This work package monitored finances, defined the AARC strategy [[STRATEGY](#)], engaged with the EC and liaised with other projects and relevant global initiatives. NA1 also offered support for mailing lists, wikis, website, and so on.
- **Training and Outreach (NA2):** This work package was in charge of the dissemination, training and outreach for the knowledge and expertise of the AARC project. The work package provided support to the other work packages to better articulate key messages and promote their achievements. A key part of this work package covered the delivery of trainings. At the start of the project it was agreed that the training modules should focus on promoting the value of federated access (for libraries and research and e-infrastructures) as well as on supporting research and e-infrastructures to deploy federated access.
- **Architecture (JRA1):** The aim of this work package was to investigate the obstacles that prevent users, educators and researchers from using their credentials to access services. The list of research requirements drawn from the FIM4R paper [[FIM4R](#)] and TERENA AAAI study [[TERENA AAAI](#)] were revisited and complemented with the library requirements [[DJRA1.1](#)]; this list became the starting point for the architecture work. The output of this work package resulted in the blueprint of an integrated framework, the AARC blueprint architecture [[BLUEPRINT](#)], to function as a template for research and e-infrastructures that need to deploy an AAI.
- **Policy and best practices (NA3):** The aim of the policies work package was to define the necessary policies and best practices to address specific requirements collected in JRA1, and operational and security aspects to complement the technical research work carried out in JRA1. The output of this work package resulted in a number of recommendations on different topics and addressed primarily research and e-infrastructures.
- **Pilots (SA1):** The aim of the pilots work package was to demonstrate that both AARC policies and the AARC blueprint architecture could be deployed. Existing AAI components were tested to assess to what extent they meet functional and technical requirements and 'readiness' levels.

The research and e-infrastructure requirements were the main drivers; the architecture and policy work packages worked to address them. The policy work package looked also at the policy and security aspects related to the deployment of the AARC blueprint. The pilots were meant to test existing AAI components but also the 'deployability' of the proposed solutions. The training and outreach made AARC results visible and supported their adoption. The image below shows how the various work packages worked together.

The next chapters will present the key results for each work package.



Figure 2: AARC work packages

2 AARC Targeted Communities

AARC engaged with different groups directly or via common partners. AARC targeted the following communities:

- Research collaborations / research infrastructures: the two terms are used to indicate the large-scale research collaborations regardless of their legal status. Examples of these communities are Elixir, WLCG, DARIAH, life science projects and others.
- e-infrastructures: This group encompasses GÉANT, EGI, EUDAT and PRACE.
- Libraries: engagement with this community was brokered via LIBER, MZK and nationally via SURFnet, GARR and GRNET. AARC also engaged with OpenAIRE [[OpenAIRE](#)] to promote relevant results.
- Federation operators: although this group was not the main target for AARC, it was important to establish a communication channel between the federation operators (and eduGAIN) and the work done in AARC, as some of the AARC recommendations would have an impact on the federation operators. These discussions took place in REFEDS [[REFEDS](#)] and helped to balance needs and constraints.

Research and e-infrastructures provided requirements to steer the AARC work and it is expected that they will deploy AARC key results, based on the AARC recommendations.

Furthermore, AARC also engaged with and leveraged the well-established processes of other existing international groups such as REFEDS (the forum of the R&E federation operators), [WISE](#) (Wise Information Security for collaborating E-infrastructures), FIM4R (Federated Identity Management for Research Collaborations) and IGTF (Interoperable Global Trust Federation). The diagram below shows the relationships among these groups.

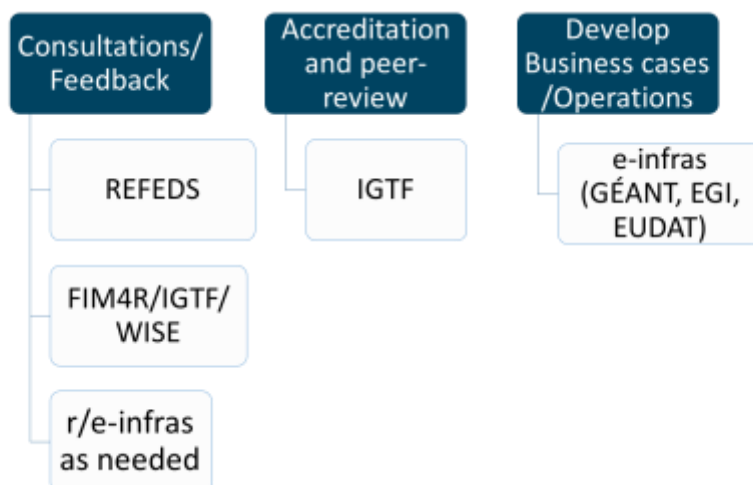


Figure 3: AARC interaction with other initiatives

3 Main Achievements

3.1 Overall management

The management activity ensured that AARC project participants could successfully carry out the work they committed to. Beside managing the website, wiki and mailing lists, NA1 organised and coordinated four AARC all-hands meetings, two AARC project reviews, and managed the liaisons between AARC, the EC and other EC-funded projects. NA1 also organised periodic calls with the AARC project management team composed of the work package leaders, as well as with the AARC project board composed of 1 representative for the libraries (LIBER), 2 NRENs representatives, 1 research infrastructure representative (Elixir) and 1 e-infrastructure representative (EGI).

Towards the end of the first year of the project, the management work package (in collaboration with the other work packages) produced the AARC strategy. This document reflects the technical annex, but is much more concise and highlights the key areas that AARC wanted to improve. The image below shows the key aspects.

Improve adoption of FIM – Promote FIM key aspects, increase number IdPs by leveraging providers outside the academic boundaries and deliver training modules.

Address eScience requirements – Deliver a blueprint architecture (on top of eduGAIN) to plug in solutions that meet eScience requirements.

Offer support for global policies – Work on and sponsor the development of key policy frameworks that aim to add additional ‘flavours’ to eduGAIN.

Make results sustainable – Pilot results in production environments and ensure that pilots operations and, security and policy frameworks rest with r/e-infrastructures.

Figure 4: AARC Strategy in a nutshell

NA1 also managed the AARC Infoshare [INFOSHARE], periodic webinars to share updates across the project and beyond. A total of 5 infoshares were delivered.

NA1 also handled the exploitation strategy, in collaboration with NA2; the dissemination and exploitation deliverable [DNA1.3] reports on these aspects. AARC has worked on all tasks as planned and in most cases, outperformed.

3.2 Training, outreach and dissemination

The main objective of the dissemination, outreach, and training activity was to create a network of contacts that goes beyond the AARC project partners and involves as many research communities and libraries as possible, to inform them about the project results and to ensure that results are deployed. The outreach and dissemination team supported the other work packages to better articulate their key achievements.



Figure 5: The NA2 approach [x]

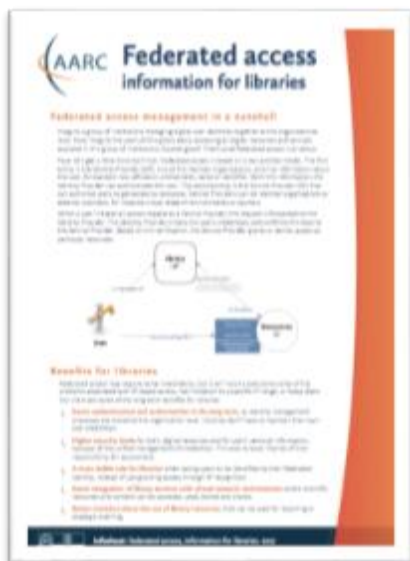


Figure 6: FIM for Libraries
[FIM4Libraries]

Figure 7: Benefits for SPs to join eduGAIN [eduGAIN for SPs]



Figure 8: Recommendations for federations operators to better support SPs [6Steps]

Figure 9: Summary of AARC results [AARCResults]



Figure 10: What is AARC? [VIDEO]



Figure 11: AARC postcard

AARC outreach and dissemination was done mostly via presentations, ad-hoc meetings with interested parties, website, blogs and participants' social media. NA2 shaped the content for the libraries toolkit [LibraryToolkit], infrastructure toolkit [InfrastructureToolkit] and FAQ [LibraryFAQ]; helped produce materials for the other work-packages, and produced a short video about AARC [video], as indicated in pictures below.

The **library toolkit** is meant for libraries and library service providers and offers information about federated access, its benefits, an FAQ section, a training module for service providers, a roleplay, and lists the AARC pilots carried out to promote federated access. See more at: <https://aarc-project.eu/libraries/>.

The **infrastructure toolkit** contains information on the AARC blueprint architecture and how to implement it, the policy frameworks AARC has defined, training for SPs, value proposition leaflet and other relevant information. See more at: <https://aarc-project.eu/infrastructures/>.

Seventeen blogs by 12 project participants were published about work done within year two of the AARC project or related developments, and were disseminated across participant newsletters and social media channels, supported by NA2.

4 May 2017 - AARC's CILogon pilot helps users to use resources from different infrastructures - <https://aarc-project.eu/aarcs-cilogon-pilot-helps-users-to-use-resources-from-different-infrastructures/>

1 May 2017 - AARC gets ready to kick-off a new cycle - <https://aarc-project.eu/aarc-gets-ready-to-kick-off-a-new-cycle/>

27 Apr 2017 - AARC training for biological data infrastructure gets positive results - <https://aarc-project.eu/aarc-training-for-biological-data-infrastructure-gets-positive-results/>

20 Apr 2017 - AARC plugfest: bundling expertise, bridging e-infrastructures, having fun - <https://aarc-project.eu/aarc-plugfest-bundling-expertise-bridging-e-infrastructures-having-fun/>

21 Mar 2017 – Welcome to IAM Online! - <https://aarc-project.eu/welcome-to-iam-online/>



- 17 Feb 2017 - The challenges of accessing non-web based shared resources - <https://aarc-project.eu/the-challenges-of-accessing-non-web-based-shared-resources/>
- 17 Feb 2017 - Architecture guidelines and recommendations open for comments - <https://aarc-project.eu/architecture-guidelines-recommendations-for-comments/>
- 15 Dec 2016 - AARC reviews progress and strategy at CERN meeting - <https://aarc-project.eu/aarc-progress-strategy-cern/>
- 29 Nov 2016 - AARC advises HNSciCloud at Project Design Phase Kickoff - <https://aarc-project.eu/aarc-advises-hnscicloud-at-project-design-phase-kickoff/>
- 13 Oct 2016 - A hitchhiker's guides to the AAI galaxy - <https://aarc-project.eu/a-hitchhikers-guides-to-the-aa-galaxy/>
- 26 Sep 2016 - AARC pilot platform approaching take off - <https://aarc-project.eu/aarc-pilot-platform-approaching-take-off/>
- 21 Sep 2016 - Federate to Win! An AARC Workshop at the LIBER Annual Conference 2016 - <https://aarc-project.eu/federate-to-win-an-aarc-workshop-at-the-liber-annual-conference-2016/>
- 26 Jul 2016 - AARC steps into its second year with praise for achievements already made - <https://aarc-project.eu/aarc-steps-into-2nd-year/>
- 16 Jun 2016 - AARC draft Blueprint Architecture available for comments - <https://aarc-project.eu/aarc-draft-blueprint-architecture-available-for-comments/>
- 1 Jun 2016 - Digital certificates behind the scenes: the AARC CILogon pilot - <https://aarc-project.eu/digital-certificates-behind-the-scenes-the-aarc-cilogon-pilot/>
- 27 May 2016 - AARC project workshop at TNC16 - <https://aarc-project.eu/aarc-project-at-tnc16/>
- 18 May 2016 - Evolution, not revolution in Tübingen in June 1 and 2 - <https://aarc-project.eu/evolution-not-revolution-in-tubingen-in-june-1-and-2/>
- 4 May 2016 - Making federated security a priority with Sirtfi - <https://aarc-project.eu/making-federated-security-a-priority-with-sirtfi/>

Two editions of GÉANT's CONNECT magazine carried double-page spreads about AARC:

- Issue 25 p 30-31 – AARC is dead – long live AARC! <https://aarc-project.eu/aarcs-cilogon-pilot-helps-users-to-use-resources-from-different-infrastructures/>
- Issue 23 p 28-29 – AARC on target to deliver on its strategic potential - <https://issuu.com/geantpublish/docs/connect23>

Training

Training has been a critical aspect of the AARC work. Whenever possible AARC used existing materials, previously provided by NRENs and other projects.

AARC has delivered different type of training modules, some via webinars, some in the form of face-to-face meetings, plug fests and some train the trainers. AARC has also built a Moodle-based eLearning platform to increase ease of access and geographical outreach of the training materials as well as to create a single training resource to draw training materials together and provide longevity beyond the lifespan of the project. Some of the content is being adjusted to make it more modular and more interactive.

At the start of the project, AARC put together an information package to explain what federated access is, its benefits (for libraries, for service providers and for infrastructures) and how to enable it. This package evolved and became Federation 101.

Training modules Delivered	Targeted Group
Federation 101 [Fed101] – Basic material to explain what federated is, its added value and to implement it for services, libraries and research/e-infrastructures.	Aimed at decision makers, libraries, research and e-infrastructures.
Training Module for SPs [TRAININGSP] - to support service providers to enable federated access	Aimed at service providers (SPs) in research collaborations. AARC delivered training for Elixir (two events) and DARIAH.
Train-the-trainers – to build know-how. This model was used for the Training Module for IdP which focused on Attribute release [ATTRELEASE]	Attribute release module: aimed at the federation operators to implement tools and offer support for their identity providers in the attribute release process. The module was presented at TNC16 (see also DNA2.4) and further improved.
Training workshop Federate to Win! [LibraryTraining]	Basic training aimed at libraries. Training events were arranged during the LIBER conference.
Internal Training: <ul style="list-style-type: none"> - Lego Training: to define a common vision on AARC and identify dependencies and workflows within AARC work packages. The training was delivered using the Lego serious playing methodology. - AARC Plug fest: to get familiar with the pilot platform, group management tool and address cross-infrastructure integration pilots. [PLUGFEST] - Blogging training: tips and tricks on writing more effective blog posts. 	Aimed at project partners
Webinars: <ul style="list-style-type: none"> - Basic Training on the AARC Blueprint Architecture [InfoshareBlueprint] - Recommendations to resource providers and user 	Aimed at research infrastructures, e-infrastructures and AARC partners, already familiar with federated technologies that plan to adopt AARC architecture and policies.

<p>communities to collect, provide access to, and publish any (personal) data related to the accounting, monitoring and logging (based on DNA3.5) [InfosharePersonalData]</p> <ul style="list-style-type: none"> - Moonshot Primer: To learn about Moonshot technology and it is currently used to provide federated access to non-web resources. [InfoshareMoonshot] 	
--	--

Table 1: AARC training modules

3.3 Architecture

The goal of this work package was to deliver the design of an integrated AAI framework, by enhancing eduGAIN by adding additional ‘layers’ to support use-cases that span beyond today’s capabilities. eduGAIN was the solid foundation upon which AARC work was built.

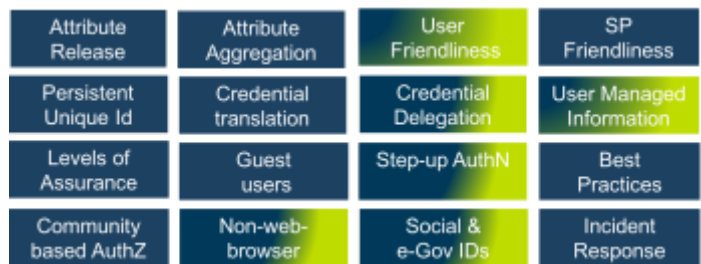
This work package investigated research communities’ requirements, ways to do account linking, revisited available solutions for non-web federated access, explored scalable approaches for attribute aggregation and provided recommendations to research and e-infrastructures on how to use guest identities.

The pictures below show the list of research communities’ requirements that AARC gathered at the start of the project.



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

Figure 12: Requirements at the start of AARC



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

Figure 13: Requirements at the end of AARC. In blue, are the requirements which have been addressed in AARC-BPA-2017.

The requirements and the interviews with different research and e-infrastructures led the team to define a AARC blueprint architecture [[BLUEPRINT](#)], which has been one of the main achievements of AARC. The pictures below show the different layers in the architecture and how it relates to eduGAIN.

Nine additional guidelines to cover different aspects were produced:

- [[AARC-JRA1.4A](#)] Guidelines on expressing group membership and role information
- [[AARC-JRA1.4B](#)] Guidelines on attribute aggregation
- [[AARC-JRA1.4C](#)] Guidelines on token translation services
- [[AARC-JRA1.4D](#)] Guidelines on credential delegation
- [[AARC-JRA1.4E](#)] Best practices for managing authorisation

- [\[AARC-JRA1.4F\] Guidelines on non-browser access](#)
- [\[AARC-JRA1.4G\] Guidelines for implementing SAML authentication proxies for social media identity providers](#)
- [\[AARC-JRA1.4H\] Account linking and LoA elevation use cases and common practises for international research collaboration](#)
- [\[AARC-JRA1.4I\] Best practices and recommendations for attribute translation from federated authentication to X.509 credentials](#)

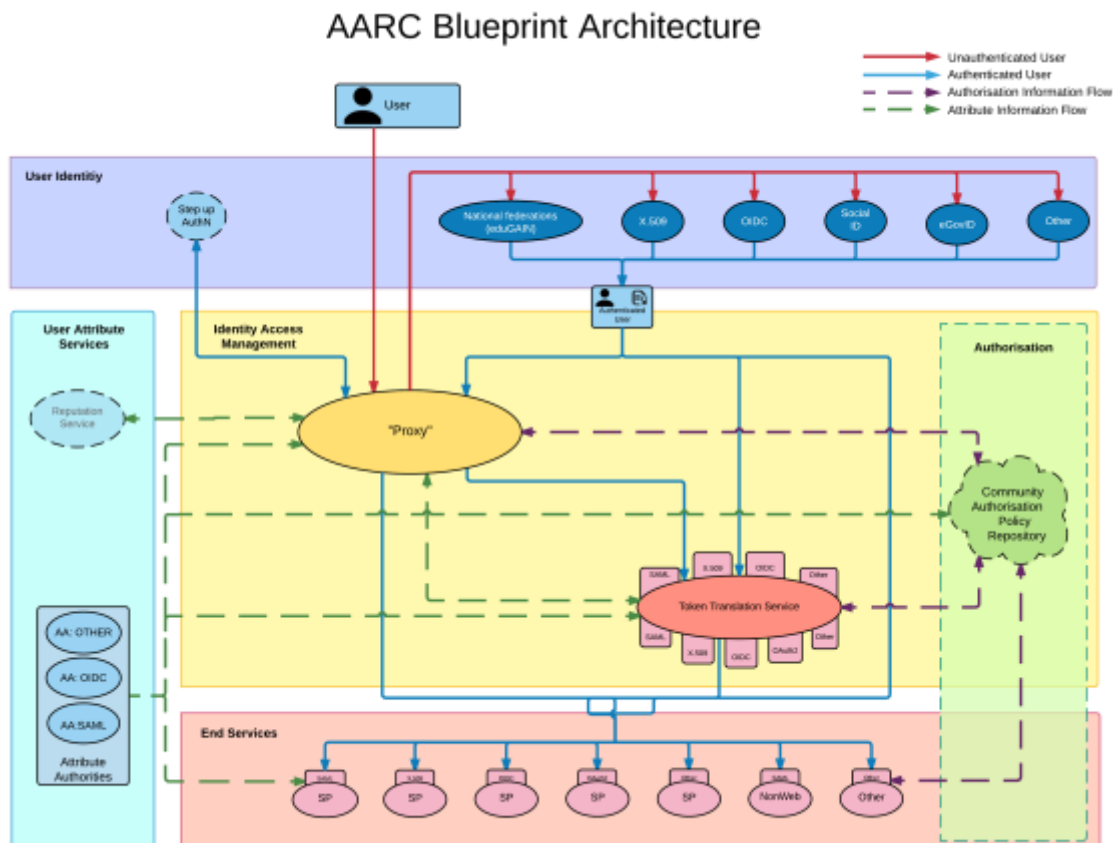


Figure 14: AARC Blueprint Architecture 2017



Figure 15 Relation between the AARC blueprint architecture, eduGAIN and the GÉANT network.

3.4 Policy

The high-level objectives for the policy work package were:

- Provide an assurance profile (LoA) framework meeting the requirements of the resource providers (RIs and EIs) that is feasible to achieve by the identity providers in eduGAIN;
- Identify a (distributed) approach to handling security incidents in a federated environment;
- Investigate sustainable service delivery aspects – recommendations and sustainability models;
- Specify scalable policy negotiation mechanisms between identity providers, attribute providers and service providers to facilitate access to resource providers;
- Develop guidelines to facilitate the exchange of accounting and usage data.

The table below shows the results in the assurance area.

Baseline Assurance
 1.known individual
 2.Persistent identifiers
 3.Documented vetting
 4.Password authenticator
 5.Fresh status attribute
 6.Self-assessment

A document to address 'low risk use cases' – See the relevant deliverable [\[MNA3.1\]](#).



A REFEDS Assurance Working Group was created to define a differentiated assurance Framework. This approach benefits from the REFEDS well defined process, and from the wider discussion between research/e-infrastructures and federation operators. See more at the REFEDS Assurance Framework [RAF]

The work package also contributed effort to lead the Sirtfi working group, which was created under REFEDS just before the AARC project started. Sirtfi defines a security incident procedure for federations. The key aspects of Sirtfi are depicted in the pictures below. Sirtfi adoption is growing fast: from its inception in February 2016, 167 IdPs in eduGAIN are Sirtfi'd today.

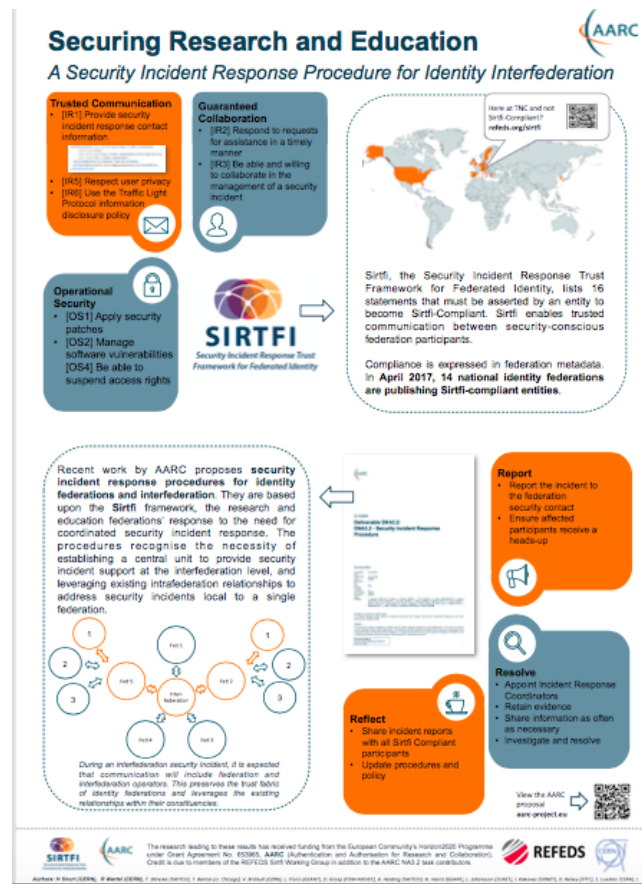
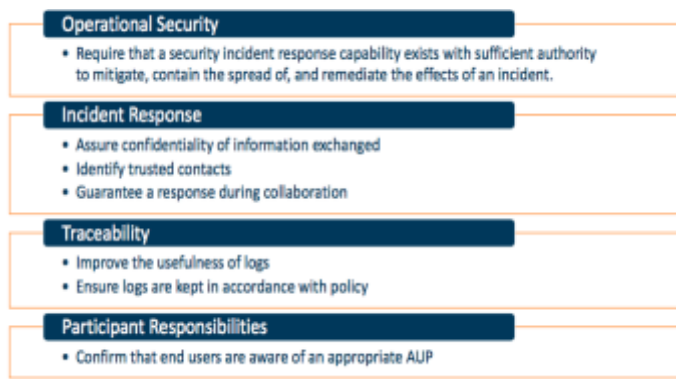


Figure 16: Sirtfi key aspects

The work package produced recommendations and templates to define sustainable plans for AARC results.

The picture below shows the main results in this area. The deliverable DNA3.3 [DNA3.3] lists contains all the necessary information.

Template for sustainability analysis	➔	Concrete future plans for SA1 pilot results
RCauth sustainability model	➔	Adoption as baseline service by major Research and e-Infrastructures
Recommendations for Infrastructures	➔	Better attribute release by federations and increased usability by researchers
Recommendations for federations	➔	Increased adoption of R&S and Sirtfi allows research SPs like CERN and EGI to join
Model study for guest IdPs	➔	Improve planning and expectations of 'cheap-and-cheerful' project-based IdPs

Figure 17: Making AARC results sustainable

The work package produced Snctfi (Scalable Negotiator for a Community Trust Framework in Federated Infrastructures), [SNCTFI] the framework that describes the policy aspects for the proxy component that is a key aspect in the AARC blueprint architecture. The picture below shows the key aspects of Snctfi.

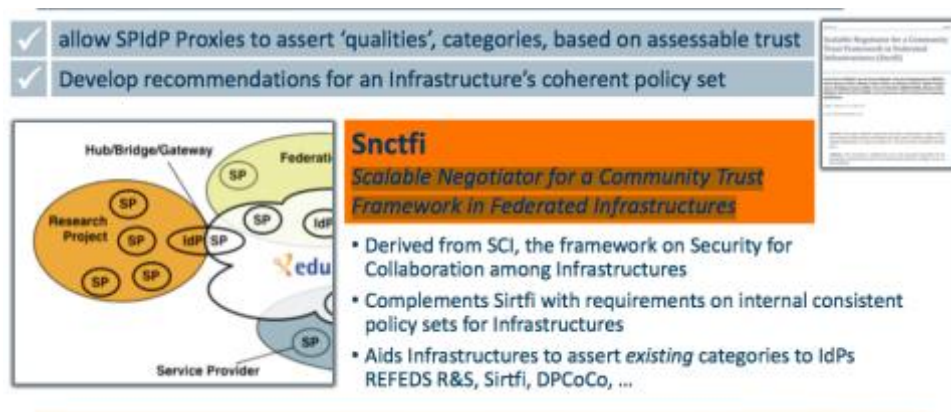


Figure 18: Snctfi key aspects

Lastly the work package also produced recommendations for research/e-infrastructures on handling personal information for accounting purposes. The results of this work is part of DNA3.5.

3.5 Pilots

AARC carried out a total of 18 pilots, that covered different aspects as depicted in fig 16. Of these, IGTF-to-eduGAIN and RCAuth are operated in production (the former by GRNET and the latter by Nikhef).

IGTF to SAML offers a guest IdP to enables researchers with an IGTF accredited digital certificate to log into services that require federated access. See fig 17 for more information. The information in the certificates are extracted and converted into a SAML assertion.



Conversely, RAuth work allows researchers to log in using their federated credentials, which are converted into a X.509 token and used to access non-web resources. See fig 18 for more information.



Pilots

Performed in AARC

To assess to what extent existing solutions meet the functional and technical (integration) requirements of research communities and e-infra-structures, we performed a large number of AAI pilots with communities:

Expanding the reach of federated access

- A proxy to centralize access management for library resources
- An EZproxy based solution to bridge SAML to IP based access for library services
- Enabling and managing access to library resources for walk-by users
- Linking ORCID persistent iD to the user's institutional account with CManage
- Mechanisms to include Social Identities in the Authentication and Authorization process when accessing shared R&E resources

Testing technical and policy components

- Managing group membership attributes or other attributes from multiple sources which can be used in a federated environment to regulate access to EGI services and a similar setup with BBMRI services
- Enable certificate based access to Elixir and EGI services with VOMS and RAuth.eu
- Reuse existing issued certificates in order to access services published to eduGAIN
- Enable access to X.509-based resources without the need for users to understand the intricacies of a Public Key Infrastructure: RAuth.eu (CILogon-like pilot)
- Enable a researcher to enrol a collaborative organization and to upload an SSH public key for access to non-web resources with CManage (CManage SSH pilot)
- Managing credentials for services that do not natively support OpenID Connect with the WaTTS token translation service: testing the SSH-plugin (WaTTS SSH-plugin)
- Using OIDC to generate a session where an RAuth Certificate is stored in WaTTS (WaTTS RAuth-plugin)
- Providing access to non-web resources via SAML and PAM with LDAPfacade

Cross infrastructure pilots

- Allowing end-users to transparently access EGI and EUDAT resources with an institutional account
- Enable automatic provisioning of accounts on EUDAT from PRACE

Enabling federated access to (commercial) 3rd party services

- Enable federated access and IdP selection to get access to the SeaFile file syncing and sharing service
- Exploring federated access to the NextCloud web-based document management service and the Collabo-
- ORCID and three e-infrastructures: EGI, EUDAT and Elixir enabled eduGAIN

All pilot descriptions, goals, documentation, sources and demos are available via the url below...



www.aarc-project.eu/pilots



AARC is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement number 653965.

Figure 19: AARC Pilots leaflet

Purpose

- Demonstrating how researchers can use X.509 certs to access eduGAIN services with substantial or higher LoA
- Not forcing them to use organization accounts

Services/Components used

- SimpleSAMLphp add-on
- WaTTS one-stop-TTS-shop
- ~Okeanos infrastructure

wiki.geant.org/x/JoEKB

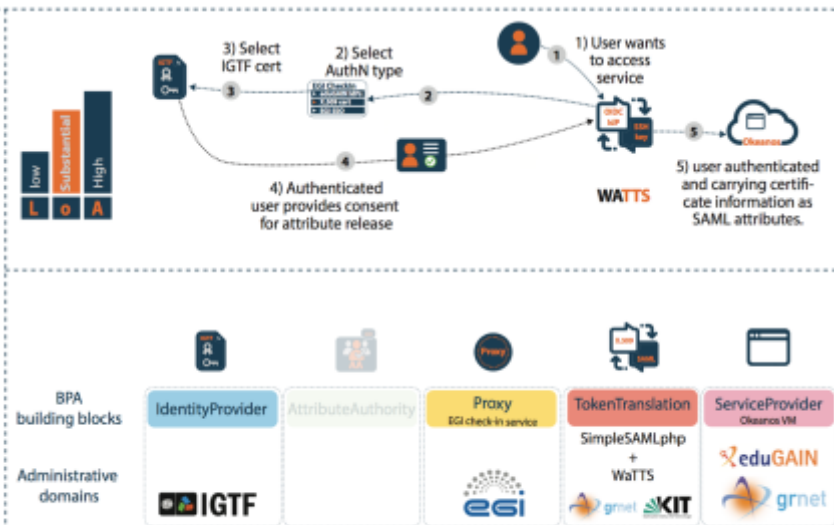


Figure 20: IGTF-to-eduGAIN Pilot

Purpose

- Enable access to certificate based services for users with an institute account, generating certs on the fly
- Bridging eduGAIN & IGTF

Services/Components used

- Cligon, adapted as RAuth
- Several master portals
- Several science gateways
- SimpleSAMLphp
- VOMS Attribute Authority
- Tested with AARC community + ...

wiki.geant.org/x/yADaAw

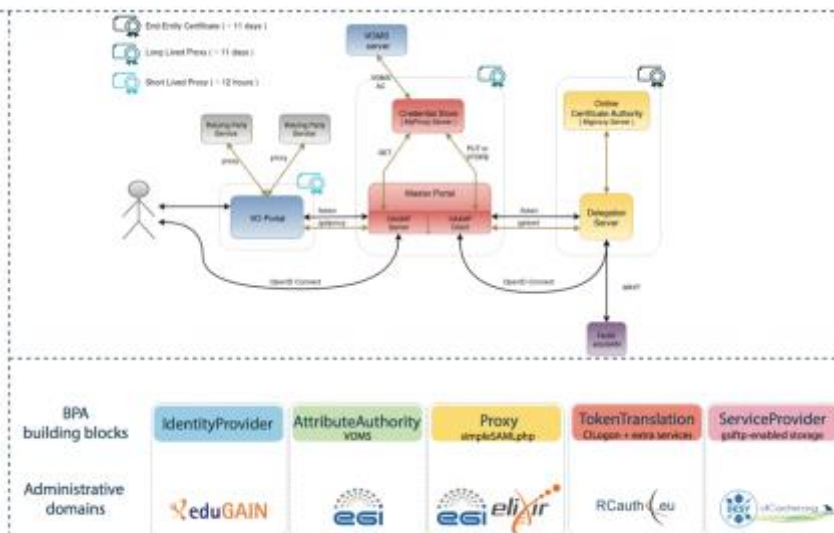


Figure 21: RAuth Pilot

AARC carried out specific pilots dedicated to libraries to show how federated access can be implemented without disrupting their existing approaches. The leaflet below shows what has been done in this area.



Federated Access To LIBRARY RESOURCES for EVERYONE

Do you grant access to your library's resources based on IP-addresses? Do you maintain the correct IP-address ranges yourself — a labour intensive and inaccurate process? Can you manage multiple identity provider - service provider connections? Are your users confronted with confusing interfaces? Can walk-in guest users access e-resources easily?

AARC has piloted the following solutions - try them!

Centrally Managed Access for Consortia

- Manage publisher contracts centrally, as a consortium.
- Save time implementing and managing: no need to establish many one-to-one trust relationships between IdPs and SPs.
- Retain control of branding and all policies.
- Produce accurate statistics quickly and easily.

Guest Access for Walk-in Users

- Allow all users, even those without institutional accounts (eg. 'walk in' guest users), to access federated e-resources.
- Configure or change settings via an intuitive web-based interface.

Federated Access to all Resources

- Deliver quick federated access to all e-resources, even those which currently only support IP-based authentication, using AARC's suggested set-up of the EZProxy software.
- Give users one consistent method of authentication to access both federated and non federated e-resources.

“ We have been running EZproxy for many years now and we also have walk-in users. By adopting these solutions, we could change our configuration and it could solve our problems. ”

-Talio Nicosi, University of Trento

www.aarc-project.eu/libraries

Figure 22: Library Pilots leaflet

AARC started also to test the interoperability between e-infrastructures. The driving use-case was to enable users from one e-infrastructures to access services in another infrastructure. This is particularly relevant also in light of the European Open Science Cloud Initiative [EOSC]. AARC carried out two pilots, one between EUDAT and EGI and another one between EUDAT and PRACE.

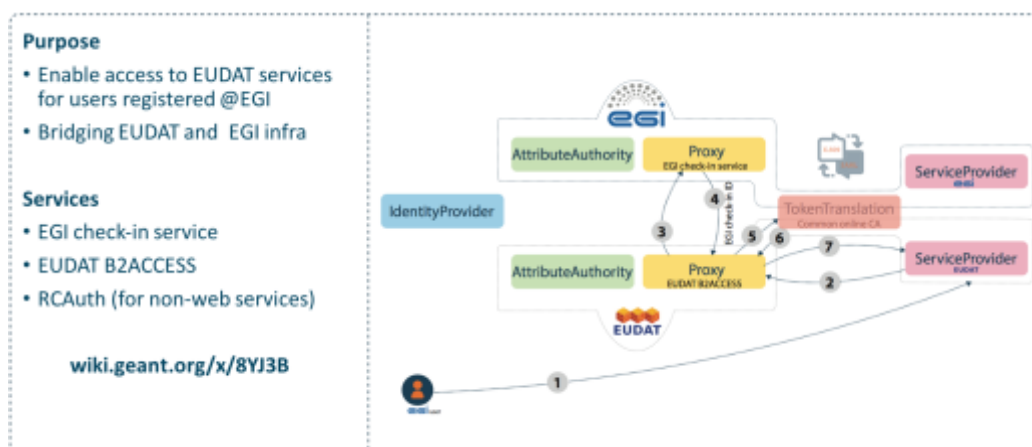


Figure 23: EUDAT-EGI Pilot



Conclusions

During the last two years, AARC has worked with the research and education community to design and promote an integrated authentication and authorisation framework that enables international research collaborations to adopt federated access solutions in an interoperable and sustainable manner.

The AARC blueprint architecture is a main achievement; it is the result of ongoing engagement with research collaborations and e-infrastructures and enables research and e-infrastructures to use federated access and reap the full benefits of eduGAIN, while addressing higher-level trust requirements typical of some international research collaborations.

During Y2 in particular, the blueprint architecture has become a reference guide for AAI developers in research and e-infrastructures. The AARC technical recommendations and guidelines for implementers and a set of policy frameworks and sustainability models help to support the production of the AAI interoperable solutions that are being deployed by research and e-infrastructures.

Through continuous engagement with scientific communities via the training & outreach activities, but also through the focused technical piloting activities, AARC has attracted critical mass for the adoption of federated access. AARC's funding has clearly contributed to facilitating the involvement and commitment of the parties, as without AARC it would not be possible to engage with research and e-infrastructures to align architecture and policies.

The work with the libraries has been completely finalised and AARC partners keep promoting it. The Library toolkit has been very well received by the libraries and has helped to form a better idea on federated access.

The training activities have also progressed, also thanks to more results maturing elsewhere in the project. AARC video material is being moved to a Moodle platform and repackaged to make the content more interactive.

In the next two years, the second AARC project (AARC2), will pick up from the work of the first AARC project and will work closely with infrastructures and technology providers to ensure that they have available the architectural and policy building blocks that are required to implement secure, sustainable, scalable and interoperable AAI solutions for international research collaborations. AARC2 will bring even more pilot activities with many communities and infrastructures and will facilitate the production, deployment, and the sustainable operation of such solutions by the infrastructure providers for the benefit of the research collaborations.

References

- [6Steps] <https://aarc-project.eu/wp-content/uploads/2017/05/6-steps-for-SPs-1.pdf>
- [AARC-JRA1.4A] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4A.pdf>
- [AARC-JRA1.4B] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4B.pdf>
- [AARC-JRA1.4C] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4C.pdf>
- [AARC-JRA1.4D] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4D.pdf>
- [AARC-JRA1.4E] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4E.pdf>
- [AARC-JRA1.4F] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4F.pdf>
- [AARC-JRA1.4G] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4G.pdf>
- [AARC-JRA1.4H] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4H.pdf>
- [AARC-JRA1.4I] <https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4I.pdf>
- [AARCResults] <https://aarc-project.eu/wp-content/uploads/2017/04/AARC-results-overview.pdf>
- [ATTRELEASE] <https://aarc-project.eu/workpackages/training-and-outreach/training-modules/training-for-identity-providers/>
- [BLUEPRINT] <https://aarc-project.eu/blueprint-architecture/>
- [DJRA1.1] <https://aarc-project.eu/wp-content/uploads/2015/10/AARC-DJRA1.1.pdf>
- [DNA1.3] <https://aarc-project.eu/wp-content/uploads/2017/05/DNA1.3-final.pdf>
- [DNA3.1] <https://aarc-project.eu/wp-content/uploads/2017/04/DNA3.1-Differentiated-Assurance.pdf>
- [DNA3.5] [https://aarc-project.eu/wp-content/uploads/2016/12/AARC-DNA3.5 Recommendations-for-Processing-Personal-Data_2016_11_07_v4_DG.pdf](https://aarc-project.eu/wp-content/uploads/2016/12/AARC-DNA3.5_Recommendations-for-Processing-Personal-Data_2016_11_07_v4_DG.pdf)
- [eduGAIN] https://www.geant.org/Services/Trust_identity_and_security/eduGAIN
- [eduGAIN for SP] <https://aarc-project.eu/wp-content/uploads/2016/11/AARC-FIM-leaflet-whole-v1.pdf>
- [EGI] <https://www.egi.eu/>
- [EOSC] <https://eoscpilot.eu/node>
- [FIM4R] <https://indico.cern.ch/event/301888/>
- [FIM4Libraries] https://aarc-project.eu/wp-content/uploads/2017/03/Infosheet-federated-access-for-libraries_v2017.pdf
- [IGTF] <https://www.igtf.net/>
- [InfoshareBlueprint] <https://geant.box.com/s/qcsqu46cfst5rxqa5z1t6upfphf25r7k>
- [InfoshareMoonshot] https://drive.google.com/file/d/0B2_gN9krquXkQWU1c0JTUGhIUHM/view
- [InfosharePersonalData] <https://geant.box.com/s/sr25gjwsbchubnji4fxyduzljdebq9ai>
- [LEGO] <https://geant.box.com/s/sr25gjwsbchubnji4fxyduzljdebq9ai>
- [INFOSHARE] <https://aarc-project.eu/AARC-infoshare/>



[LibraryFAQ]	https://aarc-project.eu/libraries/faq/
[LibraryTraining]	https://aarc-project.eu/federate-to-win-an-aarc-workshop-at-the-liber-annual-conference-2016/
[LibraryToolkit]	https://aarc-project.eu/libraries/
[MNA3.1]	https://aarc-project.eu/wp-content/uploads/2015/11/MNA31-Minimum-LoA-level.pdf
[PLUGFEST]	https://aarc-project.eu/aarc-plugfest-bundling-expertise-bridging-e-infrastructures-having-fun/
[RCauth]	https://rcauth.eu/policy/
[RAF]	https://wiki.refeds.org/download/attachments/22544423/REFEDS-Assurance-Frameworkv1.0.pdf?version=1&modificationDate=1492686581984&api=v2
[REFEDS]	https://refeds.org
[SIRTFI]	https://refeds.org/wp-content/uploads/2016/11/Sirtfi-certification-v1.0.pdf
[SNCTFI]	https://wiki.geant.org/display/AARC/Snctfi
[STRATEGY]	https://aarc-project.eu/wp-content/uploads/2016/12/AARCStrategy.pdf
[TERENA AAAI]	https://wiki.geant.org/download/attachments/21266435/2012-AAA-Study-report-final.pdf?version=1&modificationDate=1355503760046&api=v2
[TRAININGSP]	https://aarc-project.eu/workpackages/training-and-outreach/training-modules/training-for-service-provider-operators/
[VIDEO]	https://www.youtube.com/watch?v=Xpwb6BNxNW4&list=PLELuOn8jN3Ibp0W-WxO6712JKGz7qK0N
[WISE]	https://wise-community.org