Authentication and Authorisation for Research and Collaboration

AARC Blueprint Architecture Reloaded

The evolution of authentication and authorization for research collaboration

Nicolas Liampotis, GRNET

David Hübner, DAASI

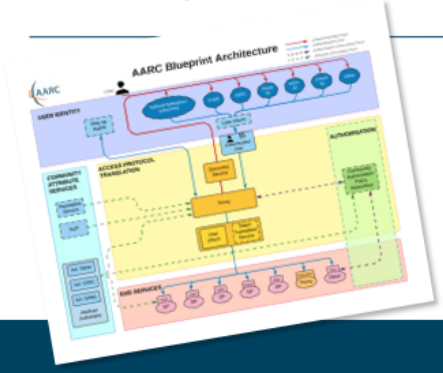
AARC2 BPA Infoshare

18 Apr, 2019

Agenda

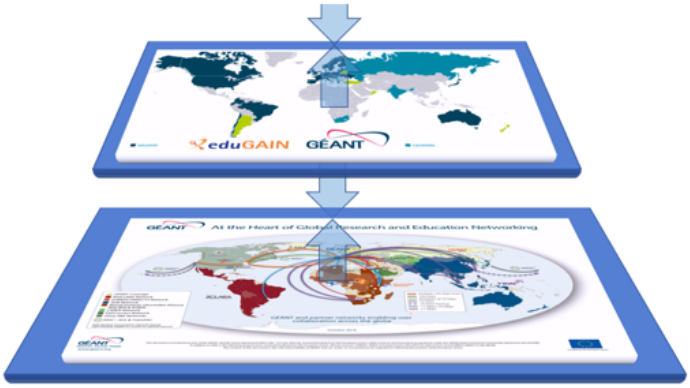
- Introduction to the AARC Blueprint Architecture
- 'Community-first' approach
- Authorisation models
- Summary & further information
- Q&A

AARC Blueprint Architecture Reloaded

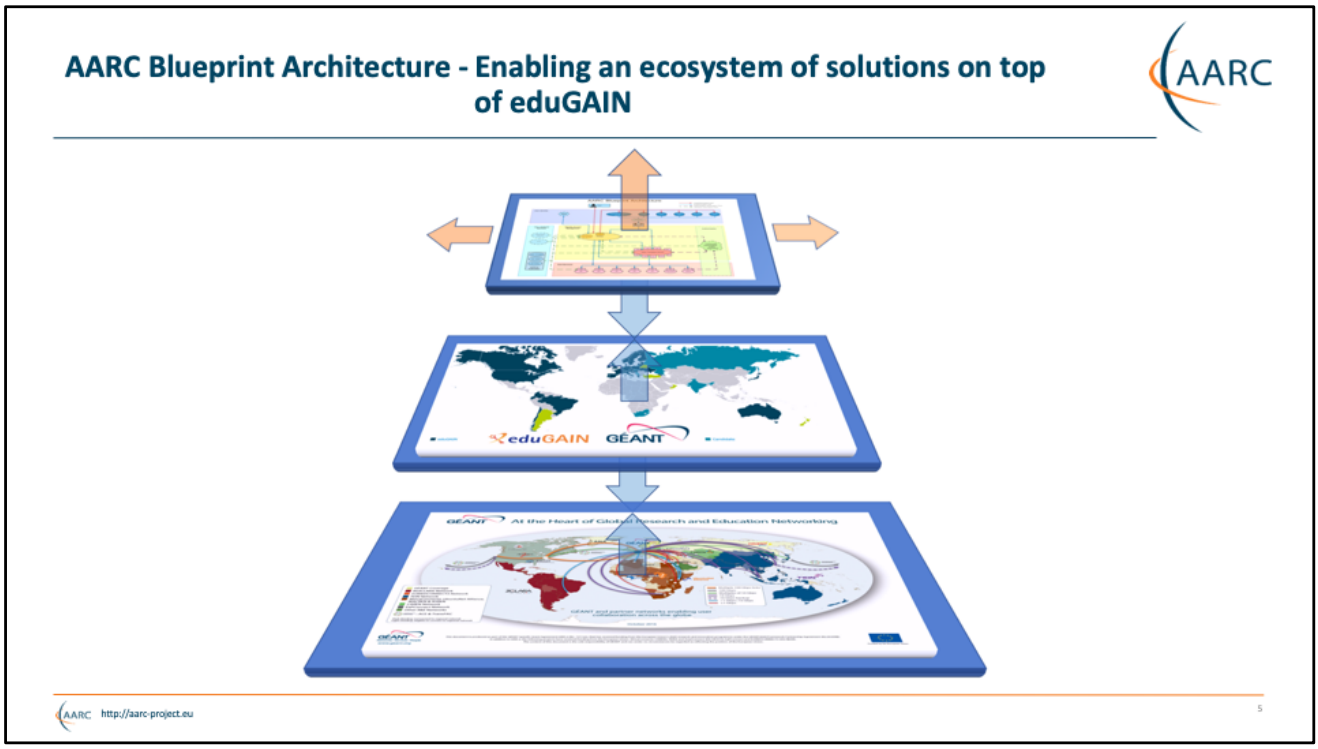


Introduction to the AARC Blueprint Architecture

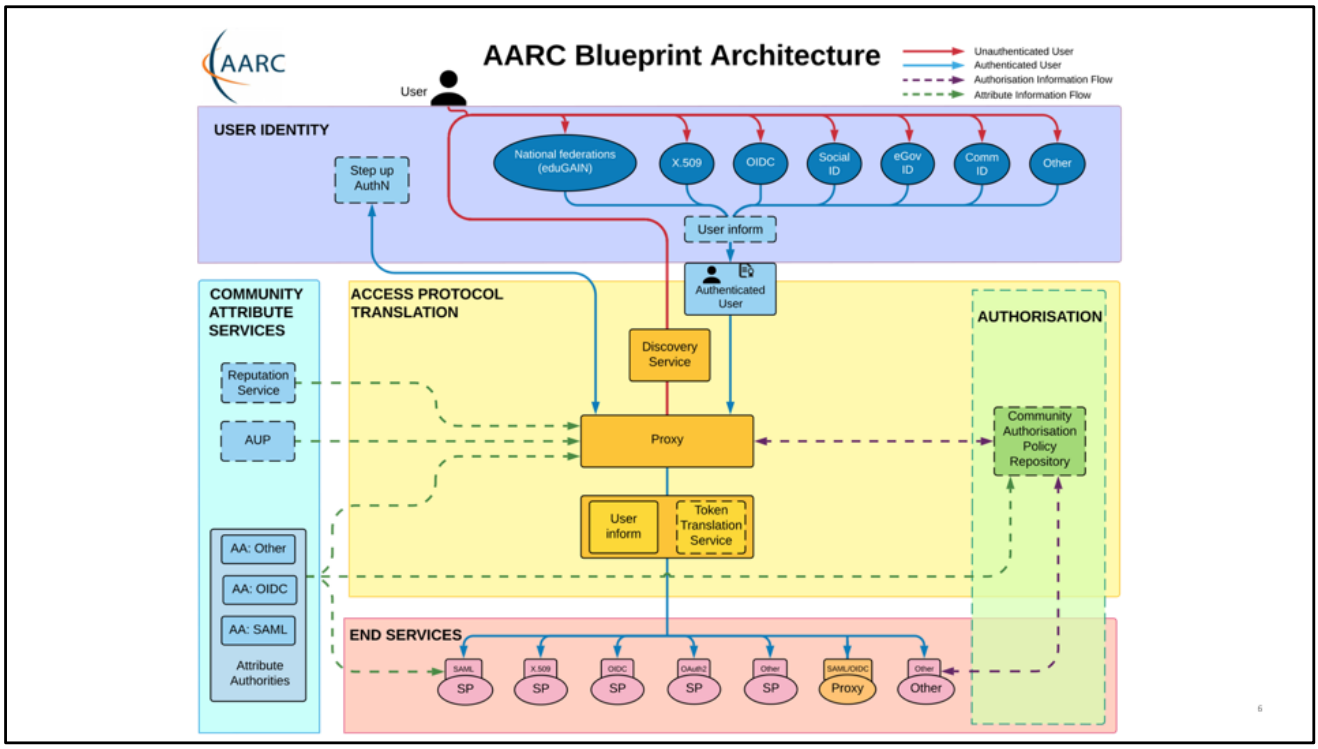
AARC Blueprint Architecture - Enabling an ecosystem of solutions on top of eduGAIN



- Researchers need to access and share resources in order to collaborate together
- Individual researchers can already use their institutional account, thanks to eduGAIN, to access thousands of resources available to their own organisation.
- But members of research collaborations need to manage, access and share resources based on their roles in these collaborations.
- To support this, research collaborations need an authentication and authorization infrastructure that allows researchers to easily access all the online resources they need.
- AARC devised an approach to building such an infrastructure: the ‘AARC Blueprint Architecture’.



- The AARC Blueprint Architecture (BPA) defines the key components for building an infrastructure in a scalable and secure way. These building blocks can be mixed and matched according to needs. This flexibility gives software architects and technical decision makers a head start in building a customised solution for their research collaboration
- eduGAIN and the national R&E identity federations enable the federation of identities and service globally. AARC is leveraging eduGAIN as the foundation for federated identities and adds the dimension of the research collaborations.
- The relationship between the users' home institutions and service providers, which is typically found in the national identity federations and eduGAIN, now becomes a relationship between a research community, the users' home institutions and service providers.
- The AARC BPA builds on top of eduGAIN and adds the functionality required to support common use cases within research collaborations, such as access to non-web services and access to resources based on community membership.

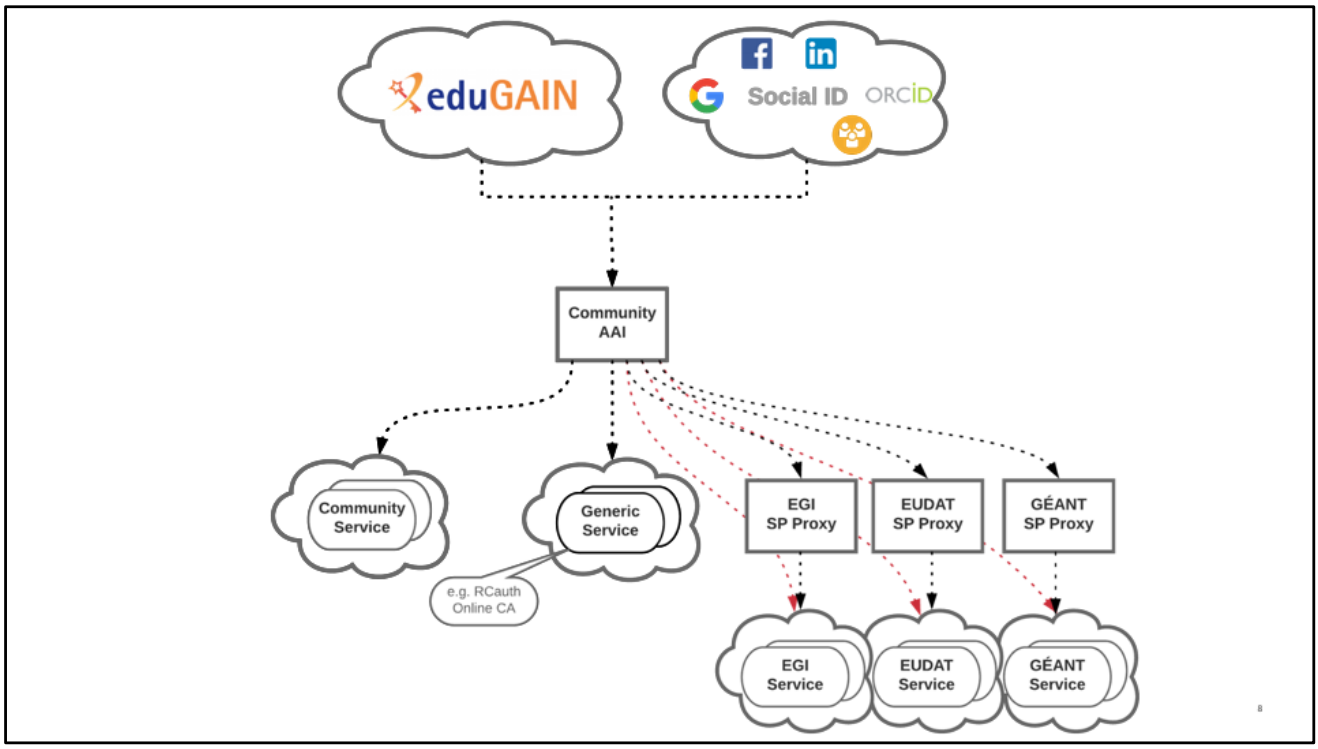


- The AARC BPA champions a proxy architecture in which services in a research collaboration can connect to a single point, i.e. the proxy
- The proxy itself takes the responsibility for providing the connection to the identity federations in eduGAIN
- This reduces the need for each service having to separately connect to a federation/eduGAIN).
- The first version of the AARC BPA was published in the Summer of 2016.
- The current AARC BPA provides a more detailed layered architecture, while retaining full backwards compatibility.
- Five component layers have been identified based on their functional role:
    - **User Identity:** services which provide electronic identities that can be used by users participating in International Research Collaborations.
    - **Community Attribute Services:** components related to managing and providing information (attributes) about users, such as community group memberships and roles, on top of the information that might be provided directly by the identity providers from the User Identity Layer.
    - **Access Protocol Translation:** defines an administrative, policy and technical boundary between the internal/external services and resources.
    - **Authorisation:** contains elements to control the different ways users can access services and resources.

- **End-services:** where the external services interact with the other elements of the AAI.

AARC Blueprint Architecture Reloaded

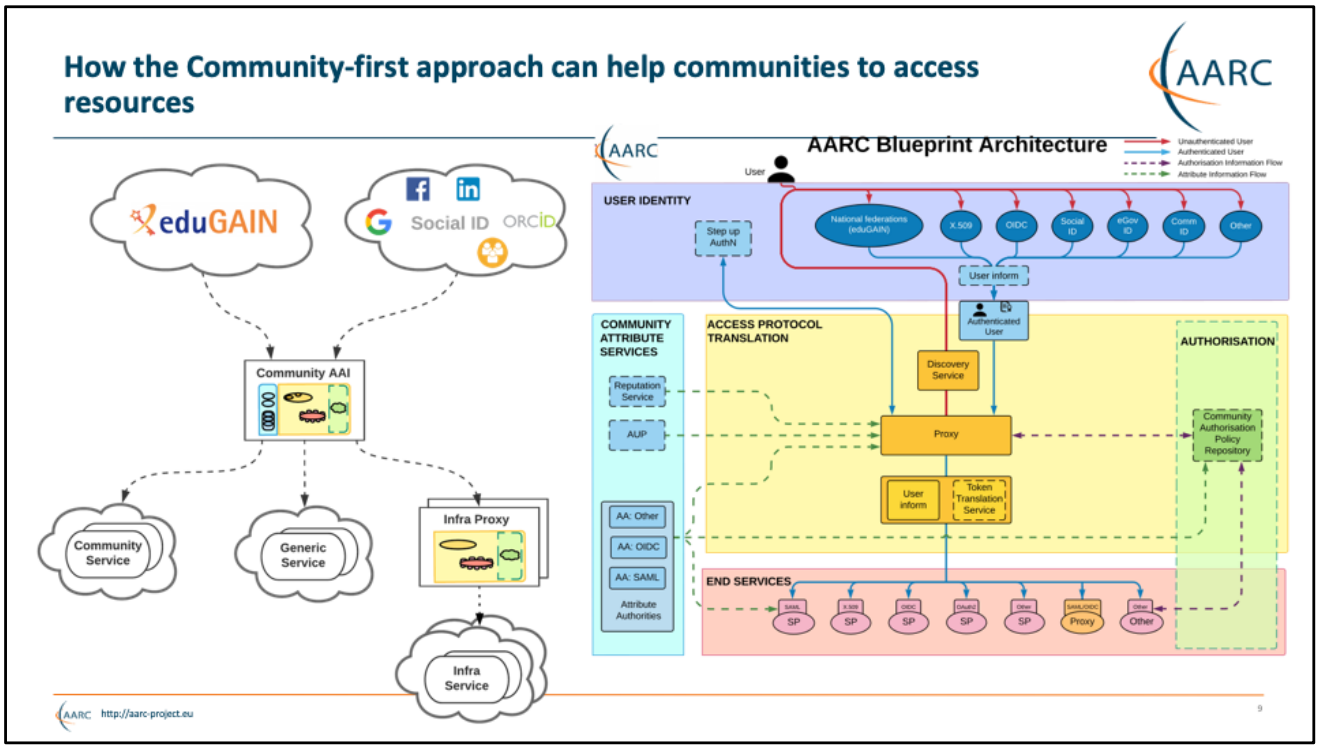
Community-first approach



- The “community-first” approach to the AARC BPA aims at streamlining how researchers can access services/resources via their Community AAI using their institutional credentials from the National Identity Federations in eduGAIN, but also from other sources as needed/allowed by the community, such as social media or other community-managed identity providers.
- The Community AAI is therefore responsible for dealing with the complexity of using different identity providers with the required **community services**. Furthermore, the Community AAI enables the addition of attributes to the federated identity that in turn can enable service providers to control access to their resources, which can range from typical web services to data repositories, scientific instruments etc.
- These community-specific services only need to connect to a single identity provider, i.e. their Community AAI IdP Proxy.
- Apart from the community-specific services, there are **generic services**, such as the RCauth.eu Online CA, which serve the needs of several communities and are thus connected to more than one Community AAIs.
- It should be emphasised that community services often require access to various generic services and resources offered by the e-Infrastructures. Access to these (generic) **e-Infrastructure services** is typically mediated through a dedicated e-infrastructure proxy. So while e-Infrastructure Proxies can be connected to

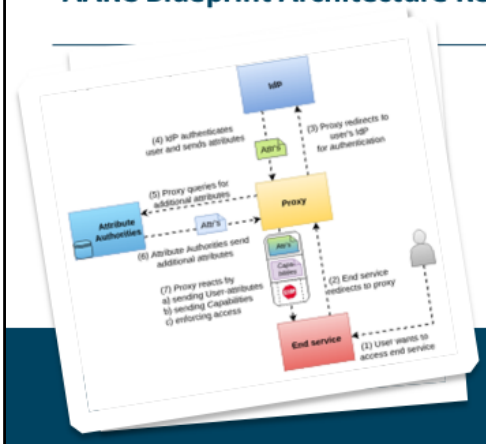
different Community AAIs, the e-Infrastructure services are connected to a single e-infrastructure SP proxy

- Benefits of community-first approach:
  - Researchers sign in using their institutional (eduGAIN), social or community-managed IdP via their Research Community AAI
  - Community-specific services are connected to a single Community AAI
    - Note: Generic services (e.g. RCauth.eu Online CA) need to be connected to more than one Community AAI
  - e-Infra services are connected to a single e-infra SP proxy service gateway, e.g. B2ACCESS, EGI Check-in, Identity Hub, etc

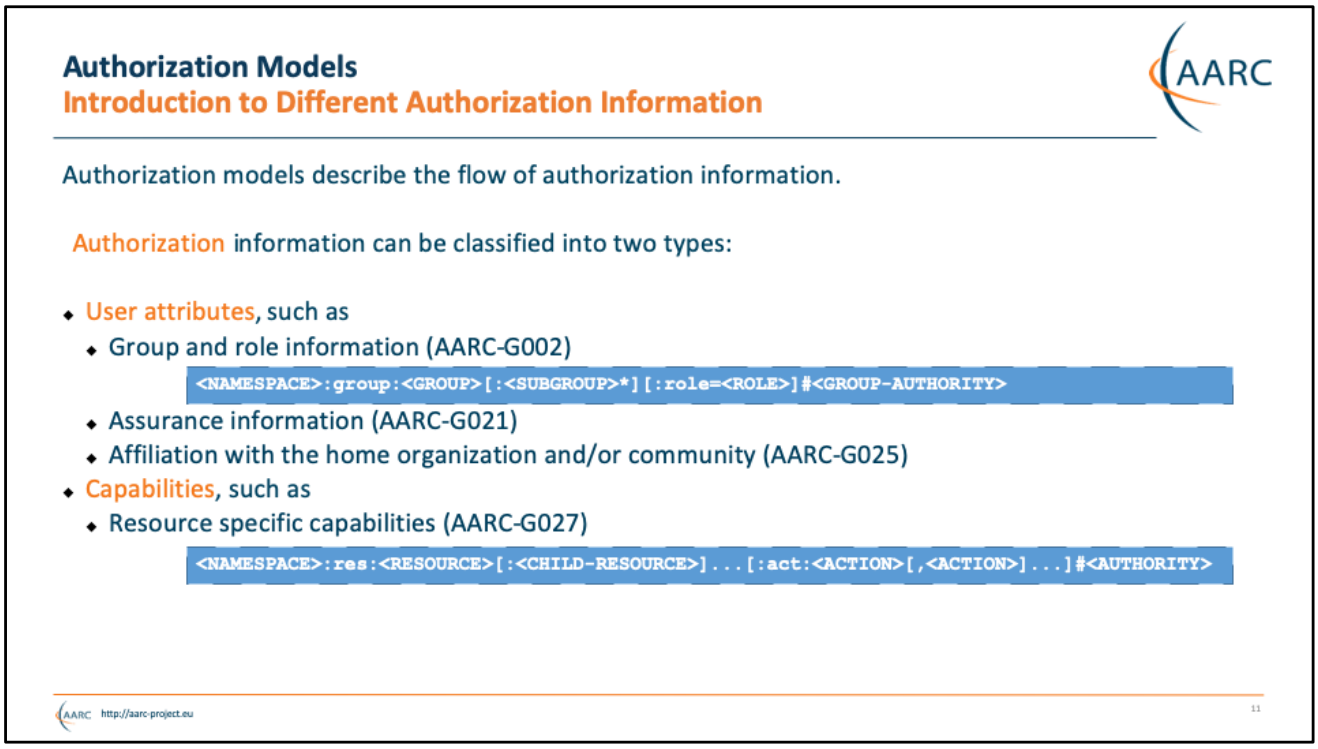


- The Identity Providers (eduGAIN, Social media, etc) depicted in the community-first approach diagram can be directly mapped to the User Identity Layer of the AARC BPA
- The Community AAI which enables the use and management of community identities for access to resources comprises three (3) AARC BPA component layers: the Access Protocol Translation, the Community Attributes Services, and the Authorisation
- The community-specific services, the generic services and the general-purpose infrastructure services can be mapped to the End Services Layer.
    - Note: The infrastructure proxy is an AAI service of an e-Infrastructure that enables access to resources offered by Service Providers connected to that infrastructure. This AAI service does not provide its own community membership management, but instead relies on the information received from the Community AAIs for that. Specifically, the e-Infrastructure Proxy comprises two (2) AARC BPA component layers: the Access Protocol Translation and the Authorisation

AARC Blueprint Architecture Reloaded



Authorization models



For that, we've analyzed existing authorization use-cases in various communities and identified three common authorization models.

These models descibe the flow of authorization information in infrastructures, which are based on the AARC BPA.

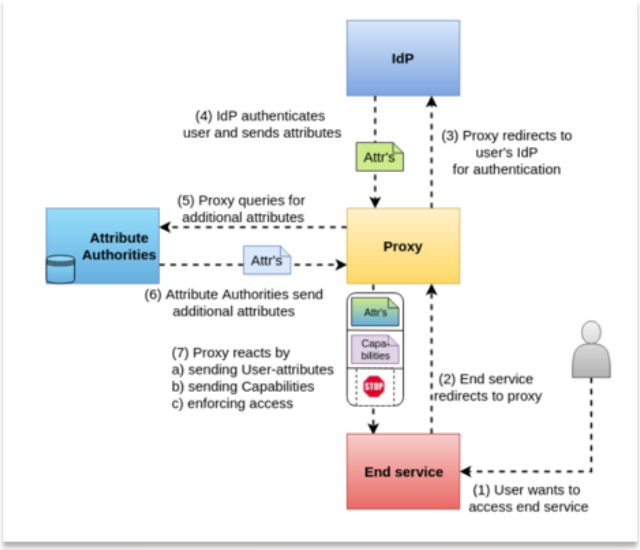
We use two categories of authorization information:

The first category is called user attributes and contains information about the user aggregated from different sources.
This information does not directly express an authorization decision, but rather is information, that can be used, either by the proxy or by end services, to make such decisions.
One type of user attributes is group and role information, for which a schema was specified back in AARC1, that follows the syntax illusstrated in the first blue box. Other types of user attributes are assurance or affiliation information.

The other category is Capabilities, which can be used to express access rights to a specific resource or child resource. Similarly to AARC-G002 we‘ve created a guidelines document on how to express this kind of information using the entitlement attribute. (second blue box)

Authorization Models
Three Authorization Models

1. Centralized Policy Information Point
2. Centralized Policy Management and Decision Making
3. Centralized Policy Management and Decision Making and Enforcement



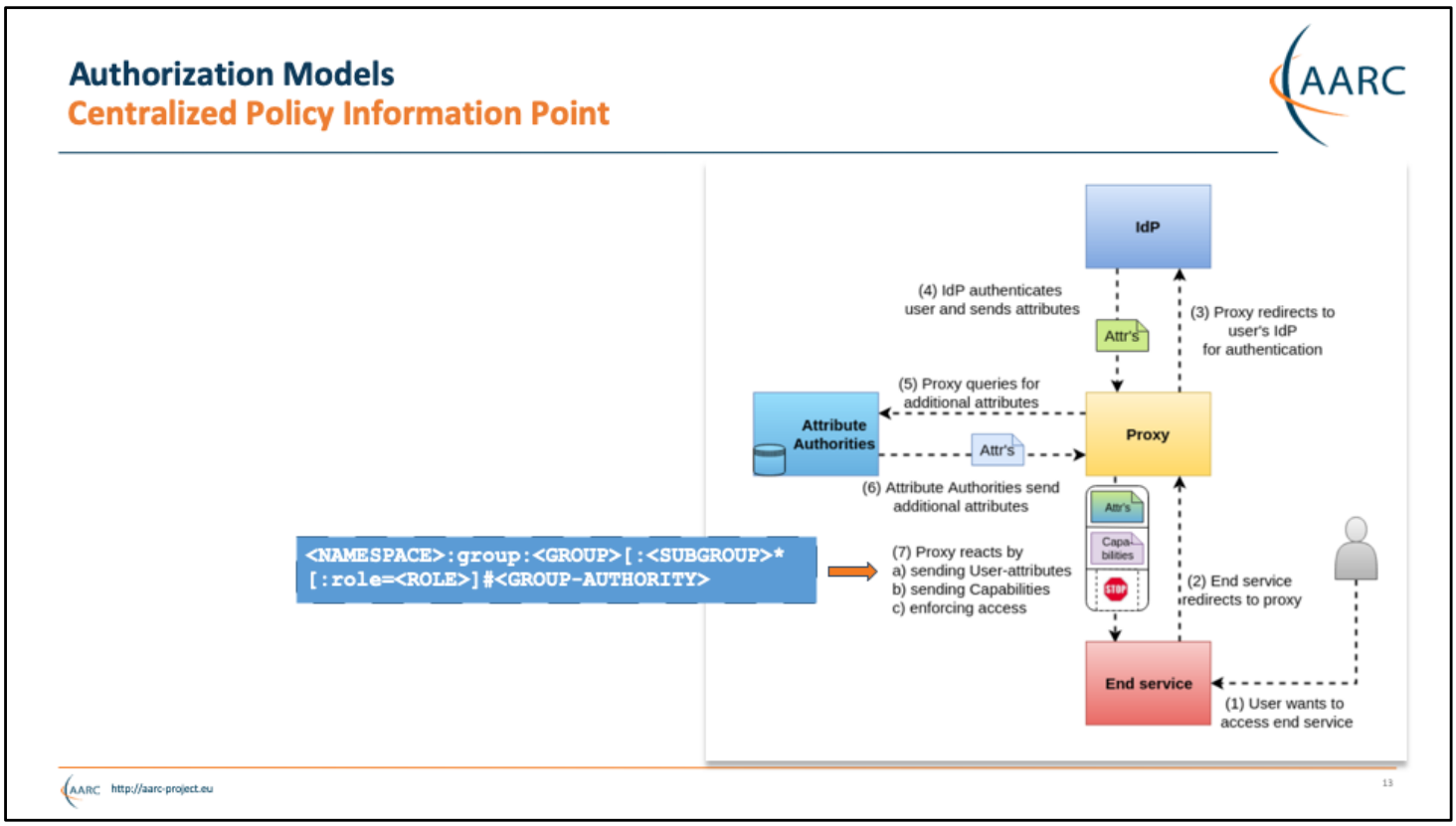
The diagram shows the general flow of a user through BPA-based infrastructure, who wants to access a resource or end service (red box).

The user is then redirected through the proxy to an IdP used for authentication. Note that this step can also involve for example an additional proxy in line with the community-first approach.

After authentication, the proxy receives various information, some of those attributes qualify as authorization information. The proxy can also aggregate such attributes for other sources, e.g. an attribute authority within the infrastructure.

The three different authorization models vary on how this authorization information is conveyed back to the end service.

(step 7)



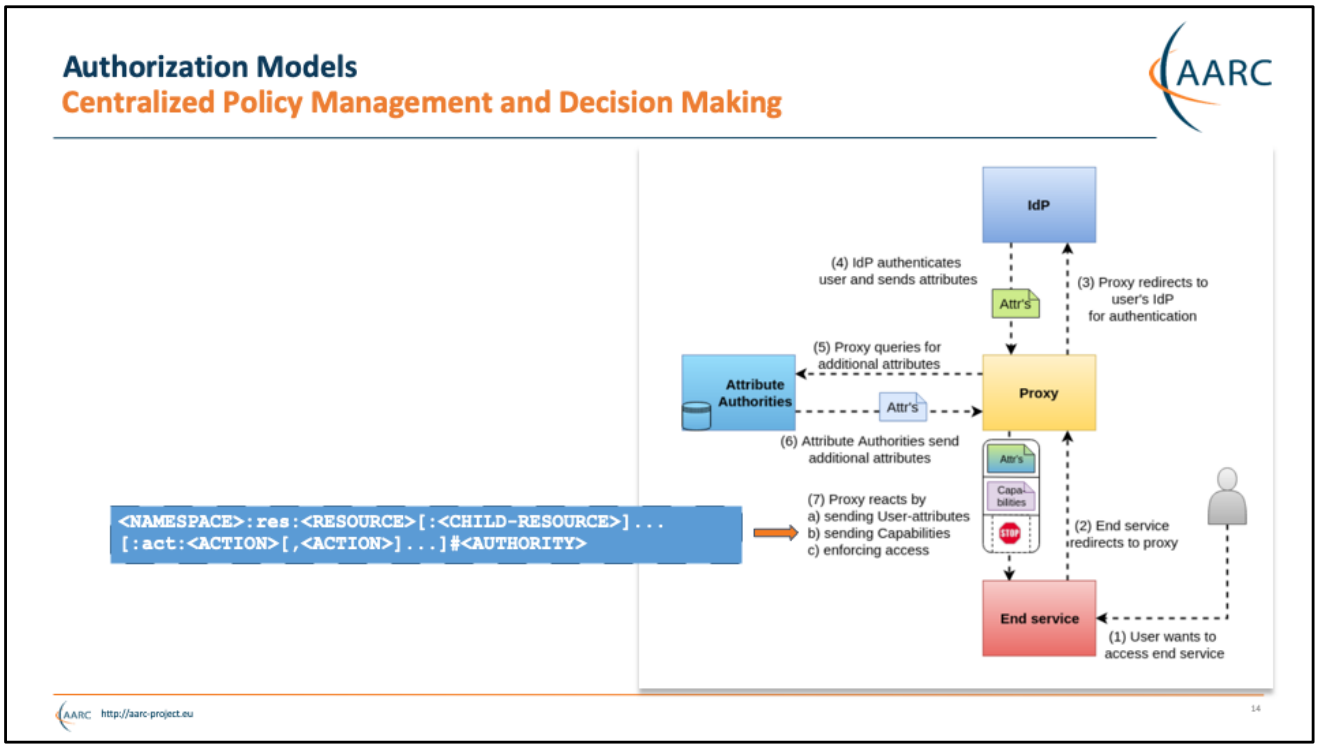
The first model is called “Centralized Policy Information Point”

Here, authorization information, in the form of user attributes, such as group and role information, is aggregated by the proxy and then conveyed to the end service.

The end service is responsible for interpreting this information correctly and taking the correct access decision.

The advantage of this model is that all information is available at the end service, which can do fine grained access managament.

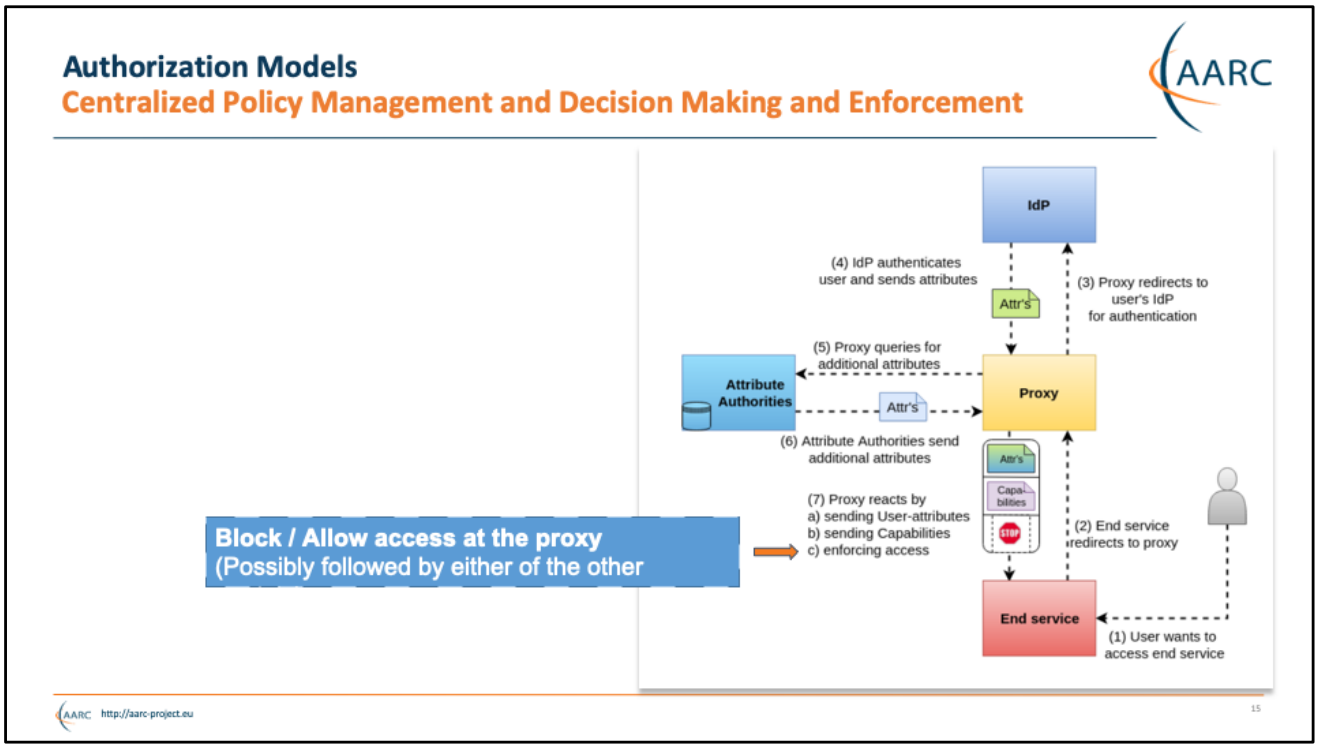
However, it requires that the end service is able to understand the information and another issue might be scalability, since an updated authorization policy needs to be implemented in all end services.



The second model is called “Centralized Policy Management and Decision Making”.

Here, the proxy takes the aggregated authorization information and re-expresses it as capabilities. Only these capabilities, or access decisions, are sent to the end services.

These capabilities allow certain actions to be performed on a specific resource. Therefore the logic of interpreting the user-attribute authorization is located in the proxy, instead of the end service, which generally simplifies the process for the end services.



The last model is called “Centralized Policy Management and Decision Making and Enforcement”
It also allows the proxy to completely block access to the end service, therefore enforcing the access decision.

This can be useful when certain services are not capable to enforce either of the previous two models themselves or to enforce certain decision on a central level, such as black- or whitelists.

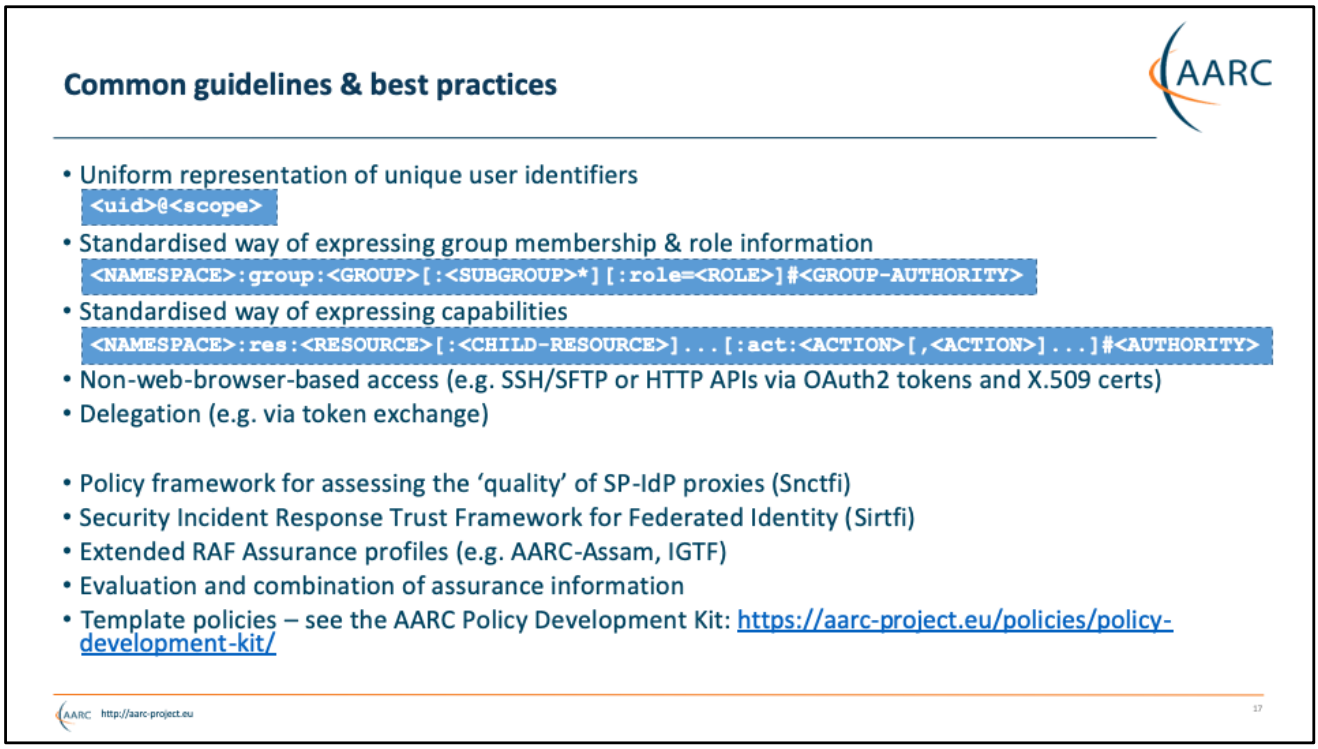
In this model the proxy has the most responsibilities, since it also needs to understand the exact authorization policy of the end services.

Finally, note that this model explicitly allows to be followed by

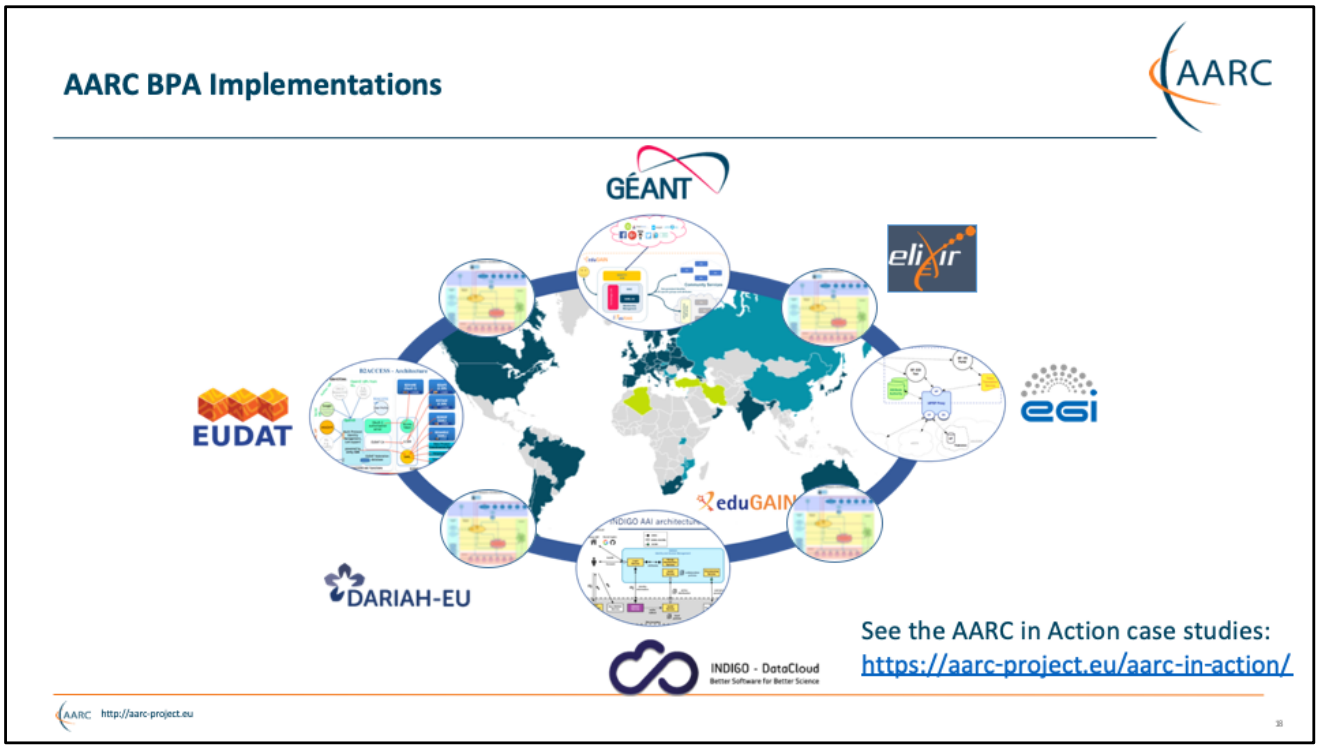
either of the other two models, in case access is allowed.

AARC Blueprint Architecture Reloaded

Summary & further information



Along with the reference architecture, the AARC BPA comes with a set of technical guidelines



- Four years after the AARC initiative started, we are witnessing wide adoption of the AARC BPA as the reference model for building AAIs for research collaboration in Europe and beyond.
- Examples include:
    - DARIAH - Digital Research Infrastructure for Arts and Humanities
    - EGI
    - ELIXIR
    - EUDAT
    - GÉANT
    - Life Sciences - A cluster of 13 research communities from the Life Sciences domain
    - LIGO (The Laser Interferometer Gravitational-Wave Observatory),
- In parallel, there is a number of pilots carried out in the context of AARC2 where more research collaborations, such as WLCG (Worldwide Large Hadron Collider Computing Grid), CTA (Cherenkov Telescope Array) and EPOS (Earth Science Collaboration Clusters), are testing the implementation of AARC BPA compliant AAIs.
- See the AARC in Action collection of research collaboration case studes: https://aarc-project.eu/case-studies

The AARC project

Watch the AARC videos to find out more
https://www.youtube.com/playlist?list=PLELuOn8jN3IIbp0W-WxO6712JKGz7qK0N

Check the IamOnline YouTube channel:
https://www.youtube.com/channel/UCussxbcR_OxG1e_kRp0pjpA

Webinar on the AARC extensions to assurance is scheduled for May 13
https://eventr.geant.org/events/3121

AARC Blueprint Architecture webpage
https://aarc-project.eu/architecture

Thank you

Any Questions?

aarc-connect@lists.geant.org

http://aarc-project.eu/

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).