Introduction to Advanced AAI Components
Training from AARC
Agenda

1. Discovery Service
2. The Attribute Release Problem
3. Federating Through a Proxy
4. How to deal with Social Identities
5. Account Linking
6. Step-up Authentication
7. Token Translation Services
8. Introduction to Authorization
Section 1: Discovery Service
The Authentication Flow

• How is it possible to choose which IdP to contact at (2)?
• Is it possible to use identities from social providers (Facebook, Google)?
• Can we access to the same application with different identities?
• How can the application improve security in identification at (4)?
Section 1: Discovery Service
How to choose the IdP to connect with

- To choose which IdP to use for authentication, a **Discovery Service** is used.

- The Discovery Service usually shows the user a list of known **IdPs** and the user can **choose** one of those to be used for authentication.

- In the diagram an example of the interactions for a user to select the IdP used for authenticating.
Section 1: Discovery Service

Two kinds of DS

In general terms we have two different kinds of Discovery Services:

1. the **Discovery Service Centralized**: is a single discovery service used by all applications in a federation to choose between all the IdPs of that federation.

2. the **Discovery Service Embedded**: is a discovery service which is implemented inside the Service Provider and so is specific for the application he’s associated with.
Section 1: Discovery Service
Discovery Service Centralized

It is usually implemented by the federation operator and serves all applications in the federation.

• Pros:
  • the service is maintained and updated by third parties
  • the hardware platform to provide the service is dedicated and managed by third parties

• Cons:
  • it is not possibile to customize user experience for the DS, in fact it shows the same UX for all application in the federation
  • it can create more confusion to users: there is a new redirect that can confuse users
  • it creates a dependency on third party services (if the DS is not reachable, the application cannot be accessed)
Section 1: Discovery Service
Discovery Service Embedded

It is usually implemented by the application provider and serves only that specific application.

• Pros:
  • simplifies user experience since it can be integrated in the application
  • permits to limit the list of IdP to only the ones relevant to that specific application

• Cons:
  • the DS must be maintained and managed by the operators of the application
Section 2: The Attribute Release Problem

A SP needs to receive the users’ attributes from the IdPs to be able to recognize and allow access to the protected resources.

However, an IdP may want to be as cautious as possible in providing user attributes to SPs for privacy and regulatory constraints.

**Problem:** The SP that is not able to provide reassurance of his adherence to privacy policies may not receive the necessary user attributes to allow access on the protected resource, so users will get errors after their correct authentication.
Section 2: The Attribute Release Problem

Entity Category solution

**Entity Categories** group federation entities that share common criteria. The intent is that all entities in a given entity category are obliged to conform to the characteristics set out in the definition of that category.

Entity Categories were conceived as a way to **facilitate IdP decisions to release a defined set of attributes to SPs** without the need for detailed local review for each SP. The decision by the IdP would instead be based on the criteria detailed in each SP entity category specification. Categories were also conceived for IdPs to indicate support for the SP categories; SPs would use this information to tailor discovery and other aspects of the user experience.

Categories in use:

1. **Research and Scholarship (R&S):** For Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part.

2. **GEANT Data protection Code of Conduct (DP_CoCo):** For Service Providers that meet the requirements of the EU Data Protection Directive in federated identity management. **CoCo V2** (with modifications for the GDPR) is under development and will have a much higher status under GDPR.
Section 2: The Attribute Release Problem
Entity Category support in eduGAIN

2616

eduGAIN Identity Providers

January 2018
Section 2: The Attribute Release Problem

Other solutions

Other than relying on Entity Categories there are other approaches:

- **User-Consent**
  The rationale is to only release attributes if the user explicitly gives his or her consent. However, this does not fix all problems and is problematic under the GDPR (since consent must be given freely)

- **Contracts between IdP and SP**
Section 3: Federating Through a Proxy

- To simplify configurations on the SP side, a proxy between SPs and IdPs may come to help.

- Proxy can help:
  - in account linking
  - with social logins
  - in attribute aggregation
  - implementing a DS
  - with consent
Section 3: Federating Through a Proxy
How the AARC BPA leverages a Proxy

• This approach is the foundation for the “Proxy” component in the AARC Blueprint Architecture (BPA)

• It defines an administrative, policy and technical boundary between the internal services and resources of an infrastructure or community with external user identities
Section 4: How to deal with Social Identities

What are Social Identities?

Many users, nowadays, use regularly the identity from social medias (Facebook, Google, LinkedIn) to access services on the Internet.

For this reason, also in federated access for research, many Identity providers are increasingly using to leverage such IDs for user identification.

Many Discovery Services list social medias within the available identity providers to be used for authentication.
Section 4: How to deal with Social Identities

Attention points

- When permitting social identities to access our services, a **strong attention** must be put on **authorization** (users of social medias outnumber largely the users of R&E).

- Social identities must be considered of a very **low Level of Assurance** (Google or Facebook never does significant vetting).

- When using social identities, “new” problems must be kept in mind: for instance nothing ensures the fact that social providers may **re-assign user IDs** to new users.

- In summary infrastructures can decide to **leverage social identities** (which are easy to set-up and use) but should use additional **complementary controls** to ensure adherence to standards and regulations.
Section 5: Account Linking

- In our communities, it happens that **users move from one institution to another** or many users may have different identities. In these cases, it is however desirable for users to be able to do account linking.

- **Account Linking** is the process to link user accounts from various identity providers, allowing a user to authenticate from any of their accounts and still be recognized by your service and associated with the same user profile.

- With account linking:
  - Users that changed home organization, can login with their new credentials reconnecting with their existing profile.
  - Users that have multiple identities on different IdPs can login with any identity provider without creating a separate profile for each.
  - Registered users can use a new social login but continue using their existing profile.
Section 5: Account Linking
A practical way to do it

• Account Linking is usually performed by releasing, after authentication, a unique ID which is able to identify the users even if authenticating with different IdPs (i.e. a community identifier or common identifier)

• As for general attribute aggregation, two approaches are possible:

  • Push
    Applied to account linking, the proxy deals with linking different accounts (i.e. identifiers released by IdPs used for authentication) and pushed the community identifier to the SPs. This is the approach used in proxied environments and usually simplifies things for SPs!

  • Pull
    Applied to account linking, a SP receives the identifier from the IdP used for authentication and then requests the community identifier from an attribute authority. No proxy is involved.
Section 6: Step-up Authentication

• With step-up authentication, applications that allow access to different types of resources can require users to authenticate with a stronger authentication mechanism to access sensitive resources.

• For example, an Intranet application requires users to authenticate with their username and password to access customer data. However, a request for access to employee data (which may contain sensitive salary information) triggers a stronger authentication mechanism like multifactor authentication (MFA).
Section 6: Step-up Authentication
Multi Factor Authentication

• To enforce user identification, a multi factor authentication mechanism can be implemented.

• Examples of MFA are:
  • RSA keys
  • Software generated tokens
  • OTP passwords sent on the phone
  • Yubikeys
  • ....
Section 6: Step-up Authentication
How this is done in a proxied environment

- When deploying a proxied environment (e.g. AARC BPA) the proxy is responsible to fulfill any given requirements

- Option 1: leverage a dedicated step-up service (cf. account linking)

- Option 2 (might be preferred): use MFA from the home IdP if possible
• In federated environments, it may happen that there are **technological incompatibilities** between the source of the user identity (e.g. IdP) and the service that user would like to access.
  • For example, grid environments use X.509 certificates for the authentication and authorization of users, while current R&E Identity Federations are based on SAML2.0.
  • Furthermore, commercial entities (e.g. social networks, cloud solutions) are increasingly relying on OIDC.

• In order to increase the adoption of federated identities there is a need to provide mechanisms that enable the **translation between different protocols or technologies**. The term “Token Translation Services” (TTS) is a broad term used to denote such mechanisms.
Section 7: Token Translation Services
Embedded token translation operation

• Some services are created in a way that translate user attributes or tokens without the user action, or they are implemented in a way that user is not even aware of it.
• This type of operation happens on the service provider.
• User access the service in a continuous manner, without the need to change its user agent.
  • An example could be that user does not have to authenticate through browser, and then use the generated credentials for a non-web access.
• A token translation operation can still be considered “embedded” in a situation where initial registration for the service is a separate action from subsequent utilization of service.
Section 7: Token Translation Services
Standalone token translation service

• This type of operation requires an **explicit action from the user**.
• Token translation functions as a **“bridge” between user authentication and authorisation, and final generated credential**.
• TTS takes user’s information (e.g. name, mail, LoA, etc.) to generate/provision a credential later utilised to access/use a desired service.
  • If the token translation or generation happens in a browser, for example, user may access the portal where it selects which types of tokens should be generated, depending on the desired service. In this example these tokens may later be used for a non-web access.
• These TTSs are usually deployed in two ways:
  • as a service specific instance or
  • as a centralized/shared service.
Section 8: Introduction to Authorization
Federations today

• Currently, the goals of an Identity Federation are:
  • give a delegated mechanism to manage user identification among different entities and within different subjects;
  • provide a set of attributes to an authenticated users to be used by the final application.

• We decided to extend the success of current identity federation to the field of user authorization.
Section 8: Introduction to Authorization

How to reach that goal?

- Traditionally, identity federations have solved the authorization problems with two opposite approaches:
  - SP managed authorization
  - IdP managed authorization

- A different approach may be followed (leveraging Attributes Authorities and implementing tools like Grouper) where authorization is delegated to a specific system designed for that purpose.
Section 8: Introduction to Authorization

Authorization interaction diagram

At **login time** user groups are retrieved from the **Attribute Authority**.

SP, after authentication, from the **authorization server**.

In a proxied architecture it can be the **proxy to perform such operation**, simplifying the configuration of SPs.
What we have learnt

★ Discovery service
★ How is it possible to simplify attribute release within AAs built with SAML
★ What is a Proxy and which advantages it brings to federations
★ How to integrate social identities in a secure way
★ What is account linking and when it is used
★ What is step-up authentication
★ How Token Translation Services work to simplify user experience
★ What additional challenges Authorization include and how to solve them
Thank you
Any Questions?

https://aarc-project.eu

© ESGMT 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 (AARC).