02-02-2017

Deliverable DSA1.3:
Pilot on attribute provider framework

Deliverable DSA1.3

Contractual Date:	31-12-2016
Actual Date:	02-02-2017
Grant Agreement No.:	653965
Work Package:	SA1
Task Item:	TSA1.2
Lead Partner:	EGI.eu
Document Code:	DSA1.3
Authors:	Peter Solagna (EGI.eu), Alessandro Paolini (EGI.eu), Mario Reale (GARR), Nicolas Liampotis (GRNET), Michal Prochazka (CESNET)

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 contains the most relevant information about two demonstrators that have been implemented in the AARC project to pilot attribute aggregation and attribute management solutions.
The goal of the demonstrators is to show with a practical implementation how group membership attributes or other attributes from multiple sources can be used in a federated environment to regulate access to services.
The goal of the document is to collect the most relevant information of the demonstrator, in the form of a table with links to the relevant AARC resources.

Table of Contents

Executive Summary

This document provides a high-level overview of the demonstrators implemented in the task "Pilots of an attribute management framework", which is part of the Pilots work package (SA1.2) of the AARC project. The goal of this task is to deploy demonstrators and pilots to showcase solutions for attribute management and consumption in a federated environment typically in the context of a research- or e-infrastructure.

The use case implemented by the pilots is the following: enable federated access to distributed service providers, with the assumption that identity providers (IdPs), service providers (SP) and attribute authorities (AA) may be operated by separate entities. The use case does not have a single community as a reference, but is a strong use case for e-infrastructures such as EGI and EUDAT, and for research infrastructures supporting multiple communities. This use case has been extrapolated from the requirements recorded in the DJRA1.1.

As part of the work three different demonstrators have been implemented.

Attribute management to access federated services: Implements workflows to enable attribute aggregation from multiple trusted sources and attribute provisioning to the SP. The goal is to allow research communities to independently organise and assign entitlements and authorisation attributes to the members of their community, and allow the service providers to consume attributes from both IdPs and communities in a transparent way. The pilot has been successfully implemented using a SimpleSAMLphp instance as an attribute aggregator, Perun and COmanage for the attribute provisioning, and a test SAML2 IdP. All these components have been deployed in the AARC testbed and integrated to build the pilot.

Social identities and attribute management: The key topic for this pilot is to integrate multiple authentication technologies, such as OIDC and SAML2, in the attributes provisioning framework developed in the previous demonstrator. The pilot has been successfully implemented, demonstrating how service providers can consume authentication information from social IdPs - based on OIDC and OAuth2 - and authorisation information from community-managed attribute authorities – based on SAML2 - without the need of specific additional developments on the SP side. In other words, a SAML-based service provider can consume authentication information from social media IdPs based on OIDC.

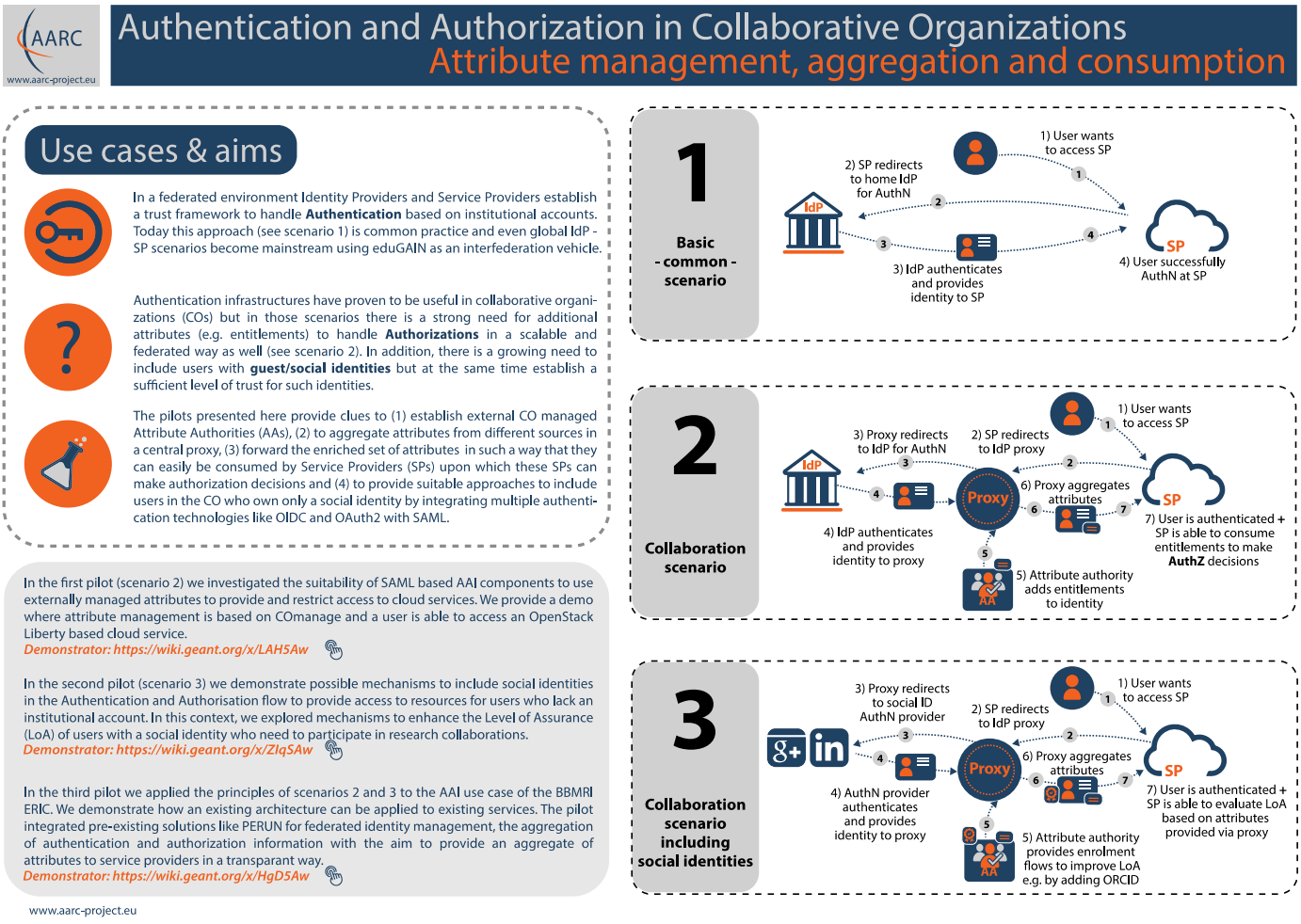
Attribute provisioning to the BBMRI services: The key topic for this pilot is to enable attribute provisioning in existing services by integrating a third-party service, with minimal or zero developments required at the service provider level. The pilot demonstrates that attributes provided by community specific sources (BBMRI Directory) and authentication information provided by federated identity providers, can be aggregated and forwarded to community services (in this implementation the BBMRI Negotiator). The result is an authentication and authorisation framework with multiple parties involved, re-use of existing tools and minimal integration work.

All three pilots successfully demonstrated the technical feasibility to implement workflows to support the use case.

A successful real-life deployment requires a trust model, supported by a policy workflow, in place between the entities (identity providers, attribute providers, proxy operators and service providers) involved in the use

case. This topic has not been investigated directly in these pilots since it is being elaborated in other work packages, such as NA3.

The team has also produced a flyer to describe and promote the pilots. The flyer can be downloaded from the AARC website: https://aarc-project.eu/documents/deliverables/



1 Summary tables

The following tables summarise the main information about the pilots and the links to the extensive documentation on the AARC project wiki.

1.1 Attribute aggregation

Task 2, Pilot 1	**Attribute management with COmanage to access a federated cloud service**
Focus	Investigate and pilot the ability of SAML-based AAI components to use externally managed attributes to provide and restrict access to cloud services.
Approach / AARC-identified solution	The use of COmanage for managing users' attributes, as an external attribute authority, allows services to manage authorisation. Such services can be entirely managed by the research community itself, independent of service providers or identity providers. The use of an attribute aggregator simplifies the configuration at both the service provider and the attribute authority level. Acting as an IdP proxy, the attribute aggregator is the only entity that needs to be configured in the service provider for authentication and authorisation data provisioning. Similarly, an attribute authority does not need to configure multiple IdPs or service providers but only the proxy.
Components piloted	OpenStack Liberty as SP with Shibboleth v3 (federated authentication configuration is described in the wiki); COmanage as attribute authority; SimpleSAMLphp as an IdP proxy/attribute aggregator.
Benefits for research communities / e-infrastructures	• No need to configure local accounts on the accessed service: ephemeral users are used. • Authorisation is based on mapping users to the proper groups, depending on the attributes released by the attribute authorities. • The affiliation to research collaborations is easily managed. • IdP Proxy simplifies the configuration at SP and attribute authority level. • The attribute aggregator allows central definition of authoritative sources of authorisation information.
Detailed technical description	AARC wiki
Documentation of components	OpenStack COmanage Registry (version 1.0.4)
Software source(s)	SimpleSAMLphp (version 1.14.5) for the IdP/SP proxy Shibboleth (Service Provider version 2.5.3)
Lead	EGI and GRNET
Status	Concluded

1.2 Social identities and attribute aggregation

Task 2, Pilot 2	**Social identities and attribute aggregation**
Focus	This pilot aims to demonstrate possible mechanisms for including diverse authentication technologies (for example social identities based on OIDC and SAML IdPs) in the authentication and authorisation process for providing federated access to resources within a given research collaboration, exploiting mechanisms to enhance the LoA of the users.
Approach / AARC-identified solution	The use of an IdP proxy, as already demonstrated in the first pilot, simplifies the authentication and authorisation workflows. In particular, the IdP proxy can act as a translator from social identity technologies (OIDC, OAuth2) to the SAML technology, which is more common in a research environment.
Components piloted	OpenStack Liberty as SP with Shibboleth v3 and SimpleSAMLphp; COmanage as attribute aggregator; IdP/SP proxy supporting SimpleSAMLphp, OpenID Connect and OAuth2 and enabling logins through Facebook, Google, LinkedIn, and ORCID.
Benefits for research communities and e-infrastructures	• No need for individual researchers to be affiliated with any of the traditional home organisations. • Support for users whose identity providers are not part of any of the eduGAIN-participating federations. • Mixed technologies (OIDC for the IdP, and SAML for the community attributes) can be consumed by service providers without the need for local developments.
Detailed technical description	AARC wiki
Documentation of components	OpenStack COmanage Registry (version 1.0.4)
Software source(s)	SimpleSAMLphp (version 1.14.5) for the IdP/SP proxy Shibboleth (Service Provider version 2.5.3) Memcached (version 1.4.21) PostgreSQL (9.4)
Lead	EGI/GARR/GRNET
Status	Concluded

1.3 Attribute aggregation for the BBMRI community

Task 2, Pilot 3	**BBMRI**
Focus	This pilot demonstrates the use of federated attribute provisioning to distributed services that are federated in a research infrastructure. As a technical implementation the pilot used Perun, which is among the AAI solutions promoted by GN4 project eduTEAMS. The AAI infrastructure follows the AARC blueprint architecture. The goal of the pilot is to demonstrate that the AAI tools can be re-used and simply deployed in a different research infrastructure to implement similar use cases.
Approach / AARC-identified solution	One of the requirements was to do the attribute aggregation from different sources and to provide user/group management. But also, the Perun solution, which was developed for the research infrastructures, supports almost all the requirements of the BBMRI community. Also, the attribute aggregation solution can be provided by a third party as a service to the community.
Components piloted	Perun identity and access management system; BBMRI Negotiator as consumer of attributes; BBMRI Directory as provider of attributes; The applications used standardised interfaces OIDC and REST.
Gain for end-users / administrators	• Re-use existing solutions for attribute aggregation. • In this case, user registration is part of the attribute aggregation service. Users can log in with their institutional accounts. • The solution can be a complete solution for user and group management, based on standard protocols that can be already supported by several service providers. • Integrated connection to eduGAIN, therefore users can use their existing federated identity to access BBMRI resources.
Detailed technical description	AARC wiki
Documentation of components	Perun (https://perun.cesnet.cz)
Software source(s)	Perun (https://github.com/CESNET/Perun) Shibboleth Service Provider (version 2.6.0) (https://shibboleth.net) PostgreSQL (9.4) OpenLDAP (2.4)
Lead	CESNET
Status	Concluded

2 Conclusions

The work of these demonstrators is very relevant to test the management and consumption of attribute aggregators in a federated environment typically in the context of a research- or e-infrastructure.

The results of the pilots will inform recommendations that will be included as part of the final version of the blueprint architecture.