

Authentication and Authorisation for Research and Collaboration

AARC2 Project: The end but not quite....

Licia Florio

AARC2 Project Coordinator,

GÉANT

AARC2 REFEDS 2019 TNC19, Tallin Goal

Identity Federations /eduGAIN

eScience collaborations

In.

٠

APR

What we knew



Advancing Technologies and Federating Communities

A Study on Authentication and Authorisation Platforms For Scientific Resources in Europe

FINAL REPORT A study prepared for the European Commission DG Communications Networks, Content & Technology

Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lefts subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity Indentition offless economic advantages, its well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the pattern must have a sense of mutual trust.

A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organizational and taxional boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & homanities, high-energy physics, atmospherie science, homformatics and fusion energy, have come logenber to discuss how to address these issues with the objective to define a common policy and trust financework for Identity Management haved on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key states of the readmap and a set of recommendations intended to ensure its implementation.

Keywords

federated identity management, security, authentication, authorization, collaboration, community

Introduction

CERN CERN

Federated identity management (FIM) is an arrangement that cas be made among multiple organisations that less subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost asvings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in research collaborations. All these identities and services need to be able work together without the users' being obliged to remember a growing number of accounts and passwords. As the user communities served by these organizations are growing they are also becoming younger and this younger generation has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This "Facebook" generation [1] has triggered a change in the attitude towards IT tools. One expects to be able to share data, software, results, thoughts and emotions with whom they choose, when they choose. The boundaries between work and social life are less sharp, and it is expected that tools blend into this environment seamlessly. The interaction with commercial services such as the social networks must not imply that the users and research communities relinquish control over access to resources and security policies. The frequency of use will vary between the different users. Some will use these new tools continuously each day while others will log in a few times per year. This implies that operation has to be very intuitive, preferentially in a style known from common commercial devices and applications (PCs, smart phones, tablets etc).

Access services based on role(s)

ReduGAIN

One **persistent** Identifier across community's services

Easy way to connect to eduGAIN

AARC

Partners



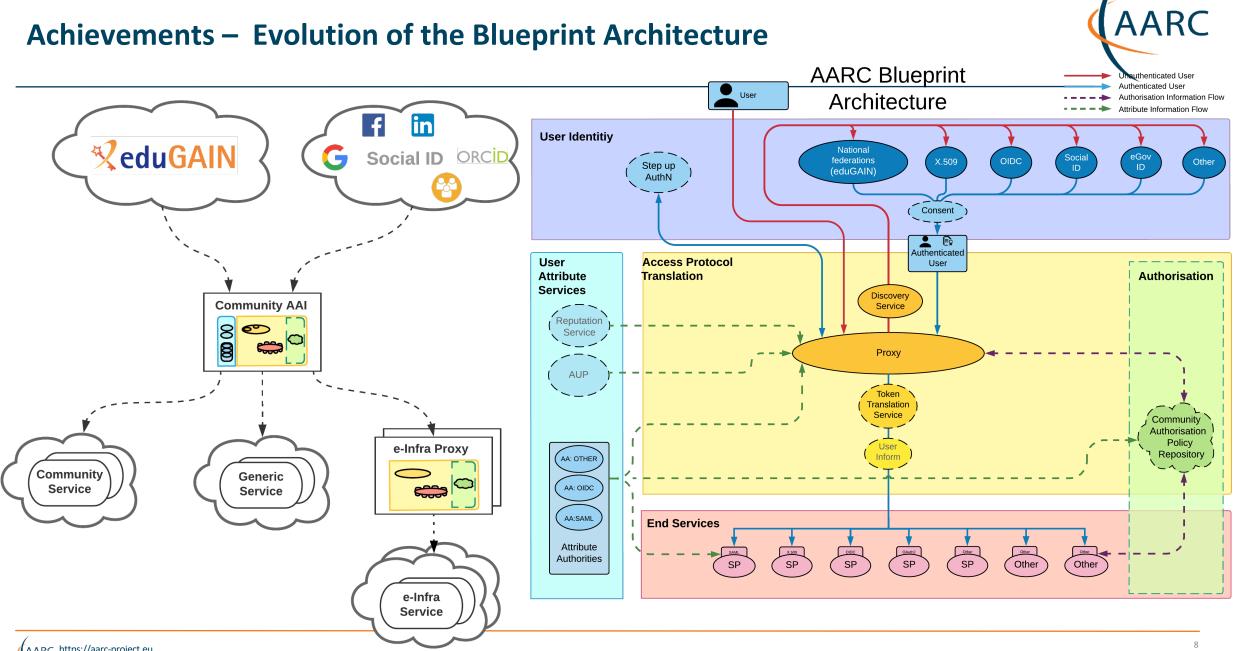


AARC https://aarc-project.eu



Key Result: AARC BPA





AARC https://aarc-project.eu

Key Result: Pilots' Lessons Learned

9 Pilots/Consultancy



Training

- FIM aspects
- Enabling SPs in OIDC and SAML
- BPA & SaToSa
- Sirtfi and PDK





AARC Continues

AARC Project

AARC Community

Are we done with T&I? -

Tomorrow 16:00 @Woodblock Room

Thank you Any Questions?

Licia.Florio@geant.org



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).