Authentication and Authorisation for Research and Collaboration

Continuing engaging with research collaborations beyond the AARC Project

Licia Florio (GÉANT),

FIM4R Meeting
New Orleans
Dec 2019

What was the AARC Project?

Partners

GÉANT

egi

JÜLICH
FORSCHUNGSZENTRUM

Science & Technology
Facilities Council

EMBL

CERN

INAF
ISTITUTO NAZIONALE
DI ASTROFISICA
NATIONAL INSTITUTE
FOR ASTROPHYSICS

BBMRI-ERIC
Biobanking and
BioMolecular resources
Research Infrastructure

SURF NET

grnet

instruct
Integrating
Biology

MORAVIAN
LIBRARY

NIKHEF

KIT

INFRAFRONTIER

EISCAT SCIENTIFIC ASSOCIATION

LIBER
LIBER

CESNET

Consortium
GARR

CYFRONET

PSNC

UC
UNIVERSIDAD
DE CANTABRIA

CARDIFF
UNIVERSITY
PRIFYSGOL
CAERDYDD

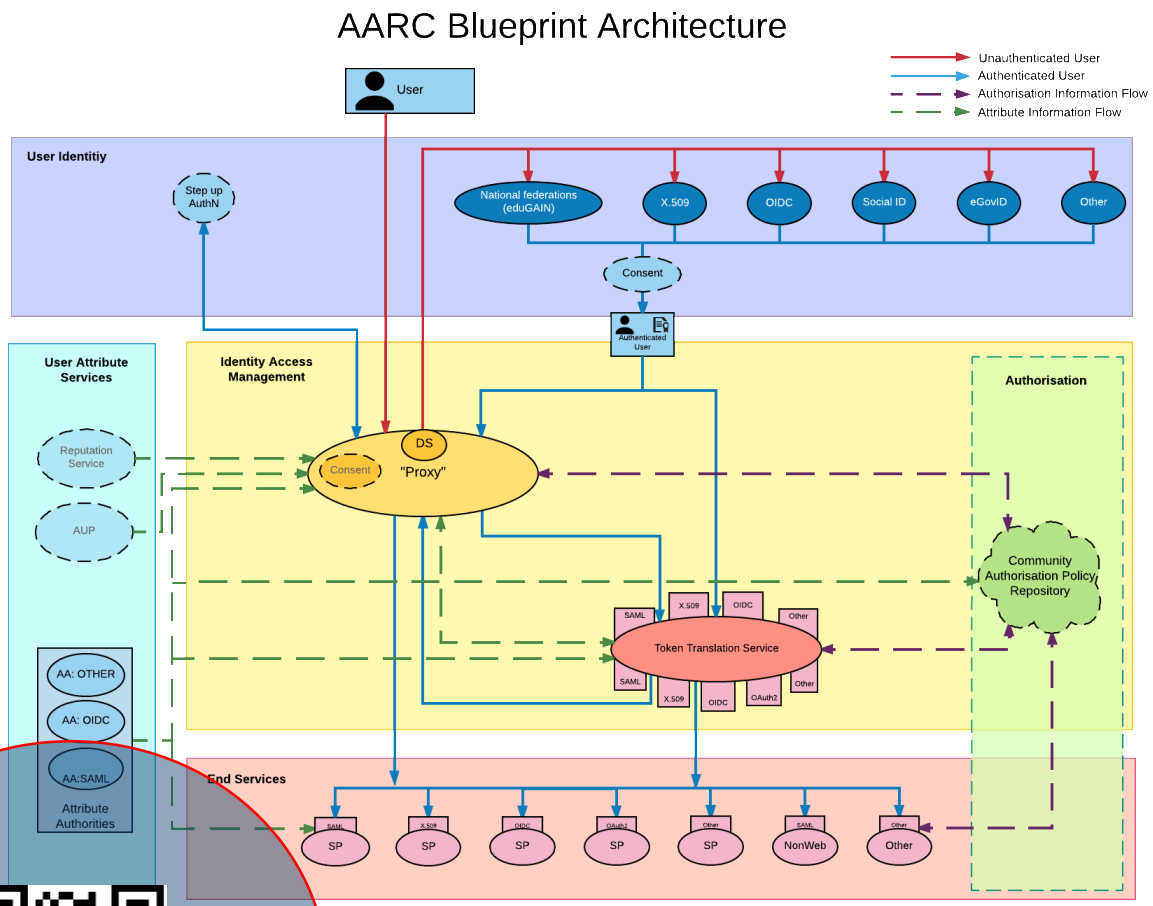
DAASI
International

Reti
Business & IT Consulting

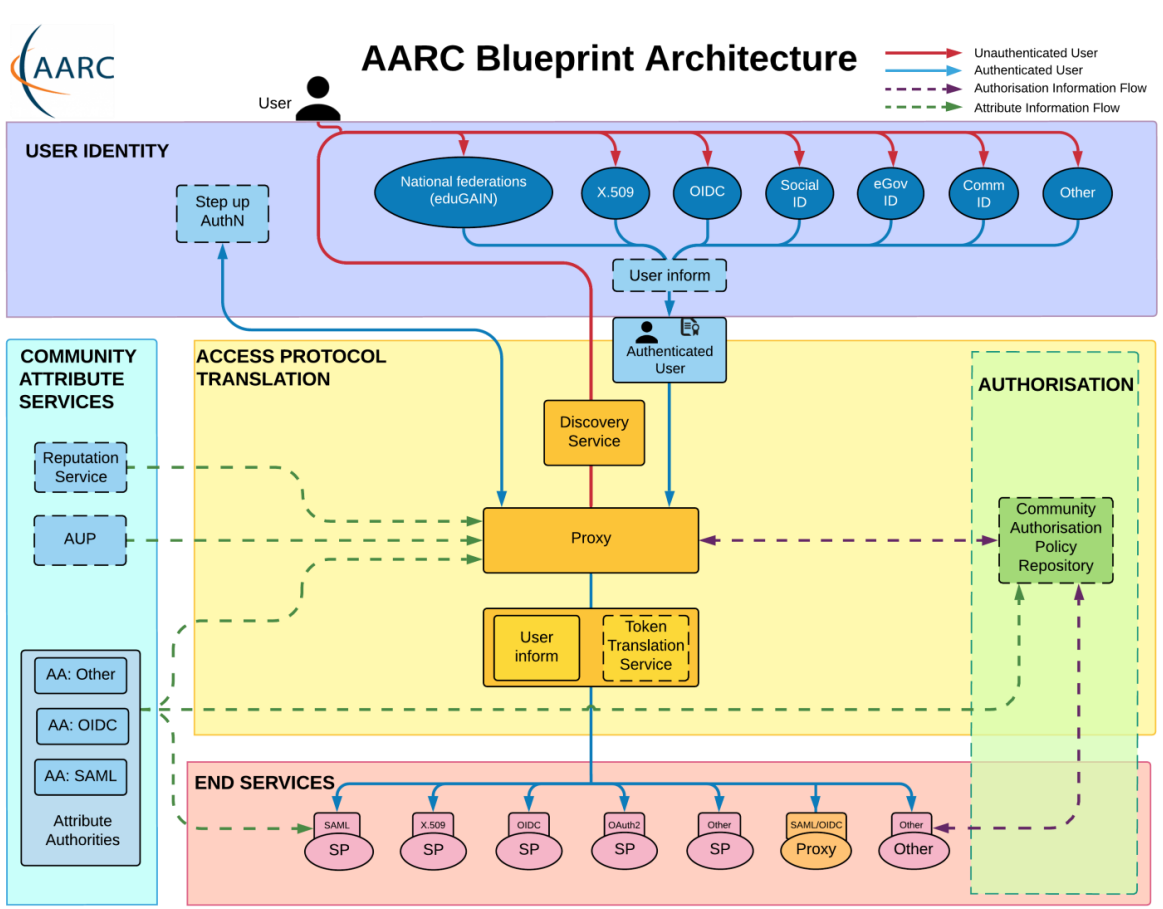
Identity Federations /eduGAIN

Research collaborations

Evolution of the Blueprint Architecture

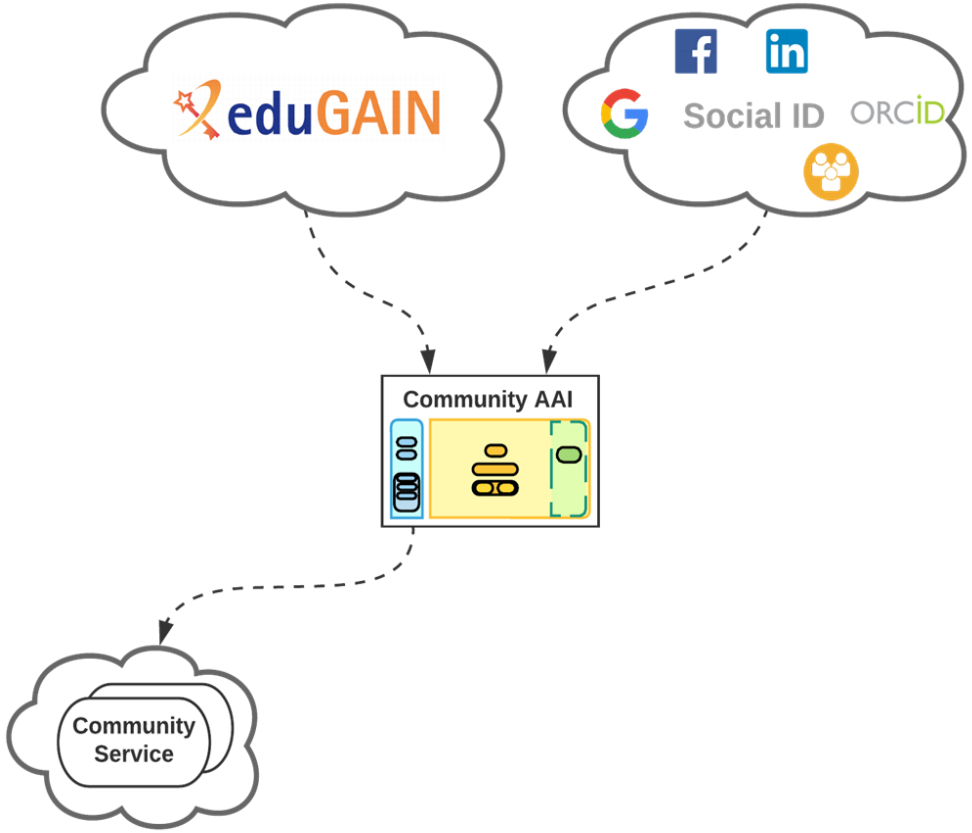


AARC-BPA-2017

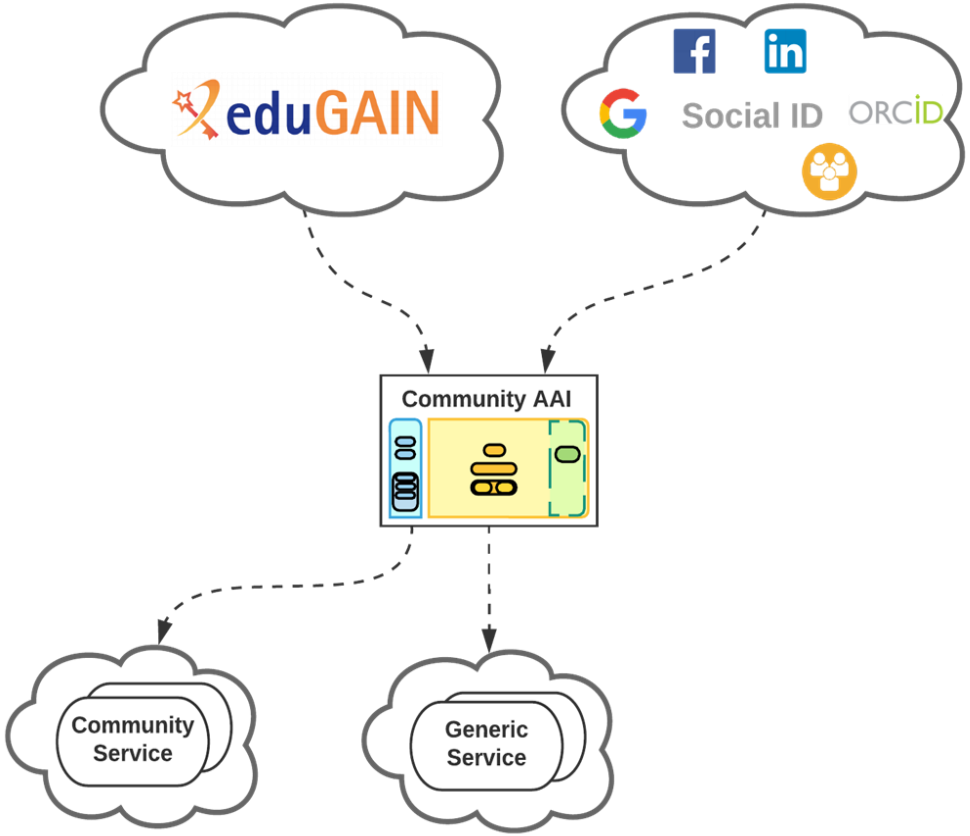


AARC-BPA-2019

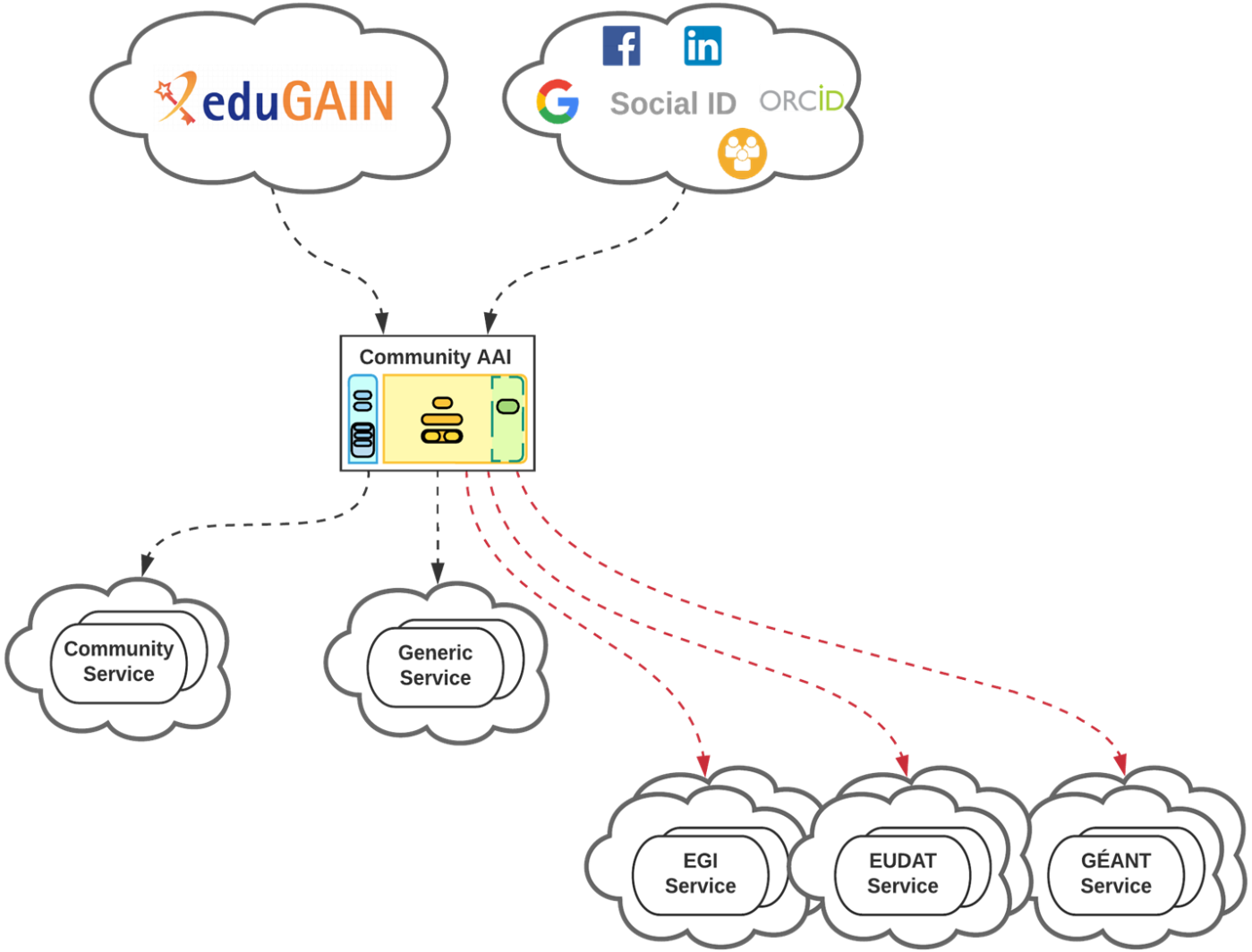
Evolution of the Blueprint Architecture
Accessing Community Services



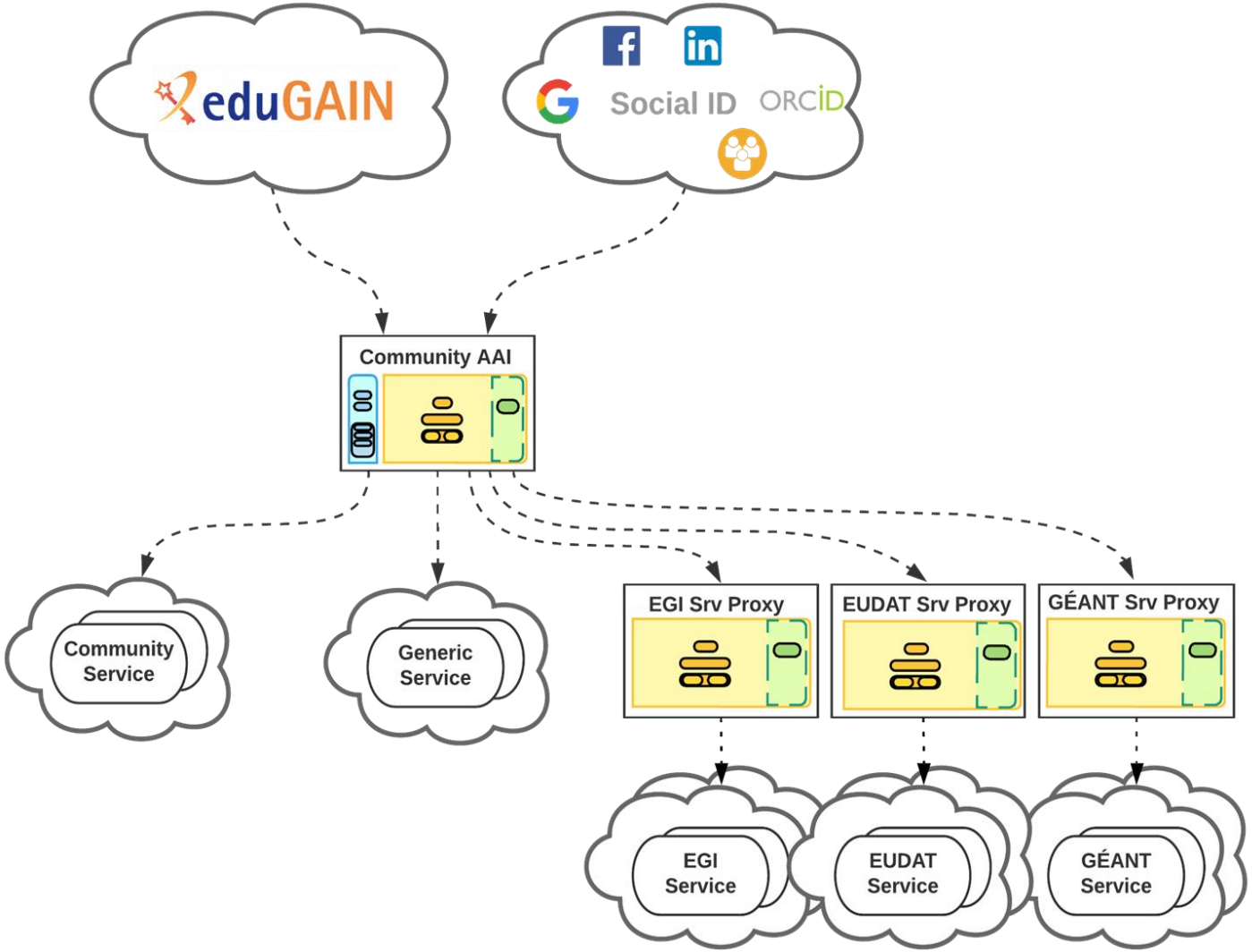
Evolution of the Blueprint Architecture
Accessing Generic Services



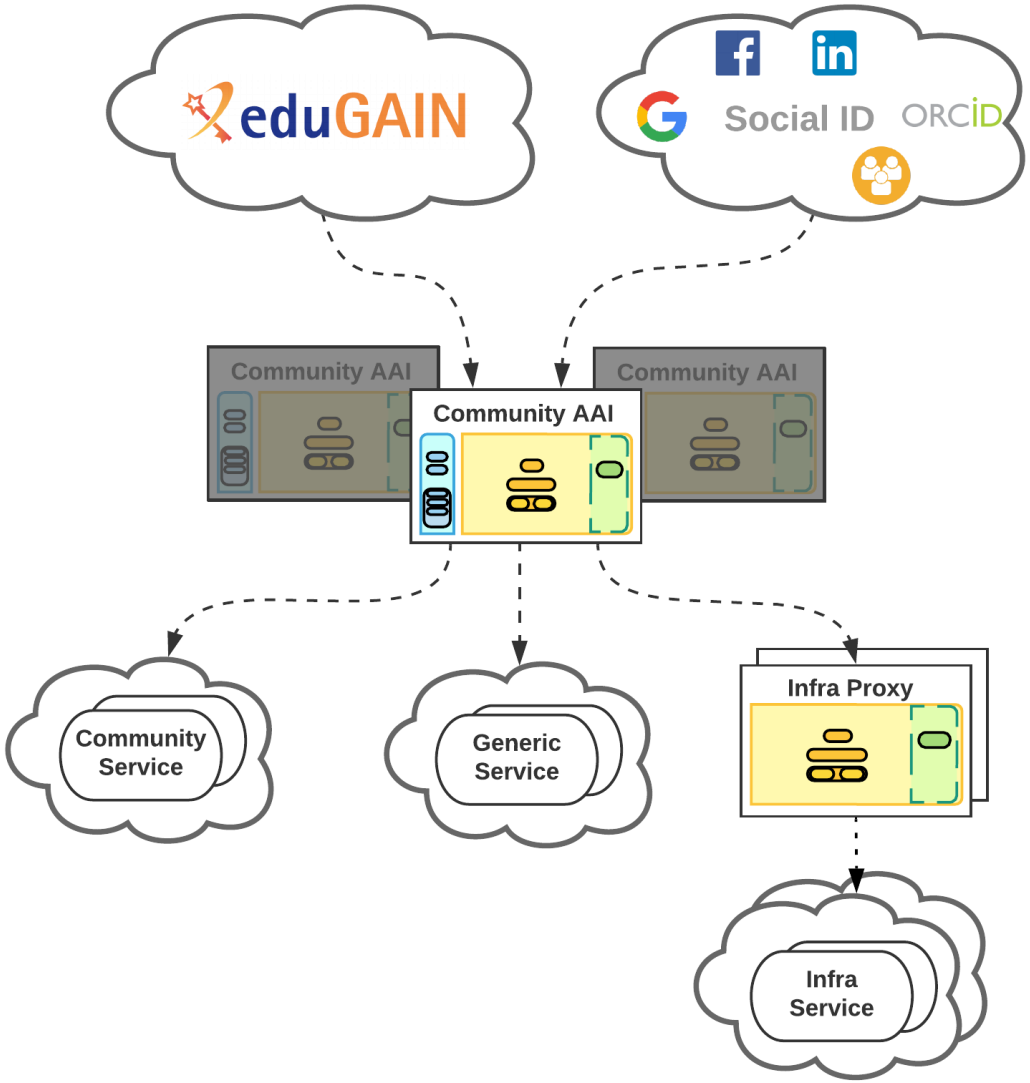
Evolution of the Blueprint Architecture
Accessing infrastructure services

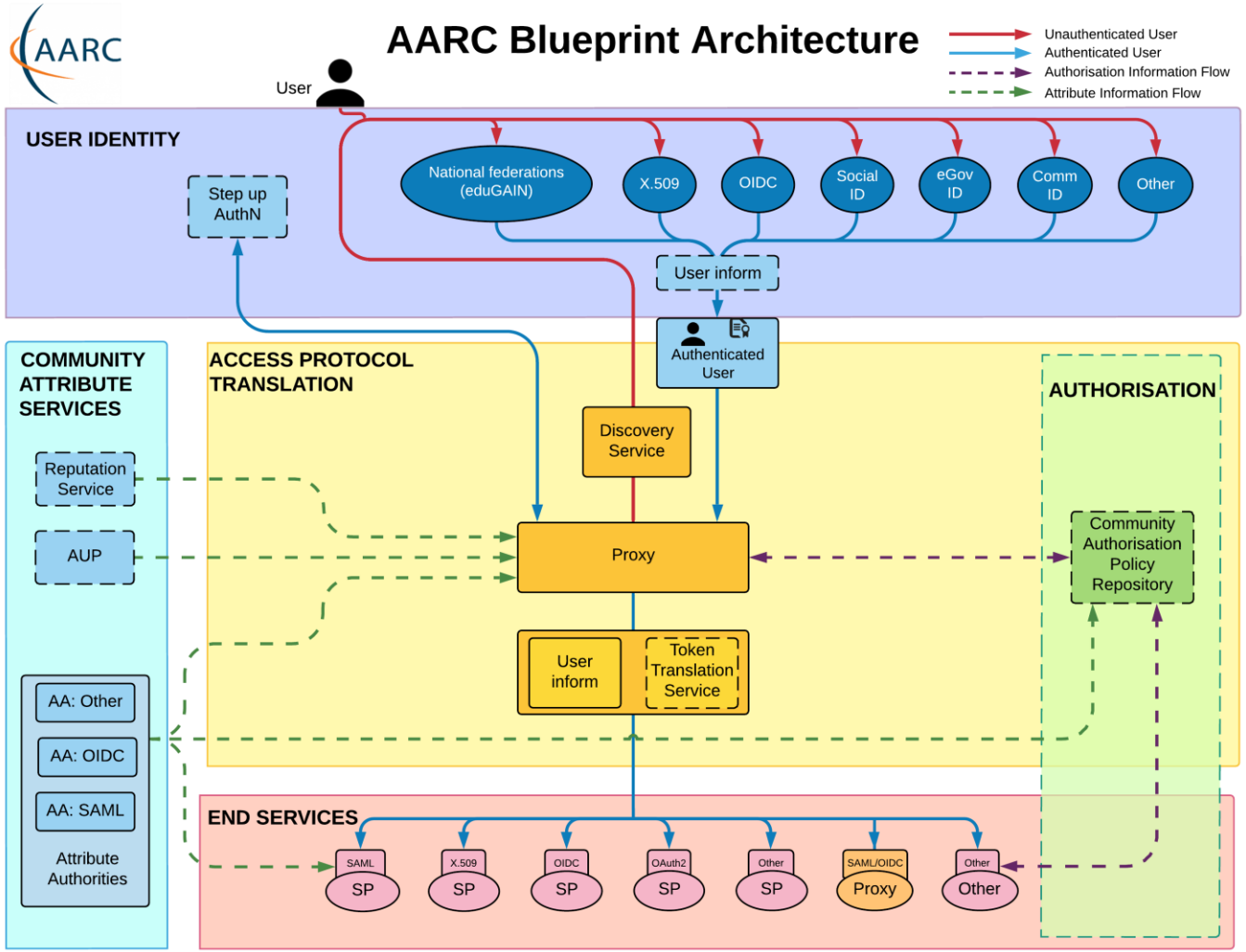


Evolution of the Blueprint Architecture
Accessing infrastructure services

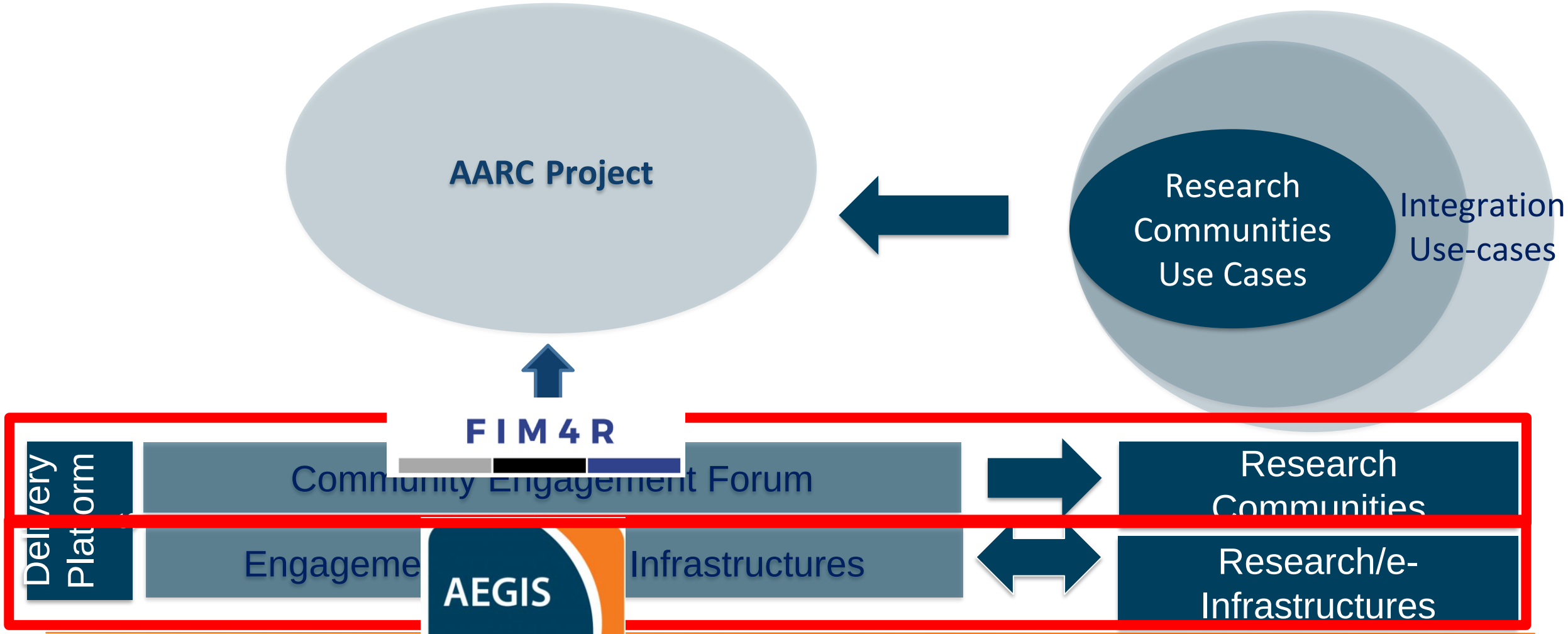


Evolution of the Blueprint Architecture

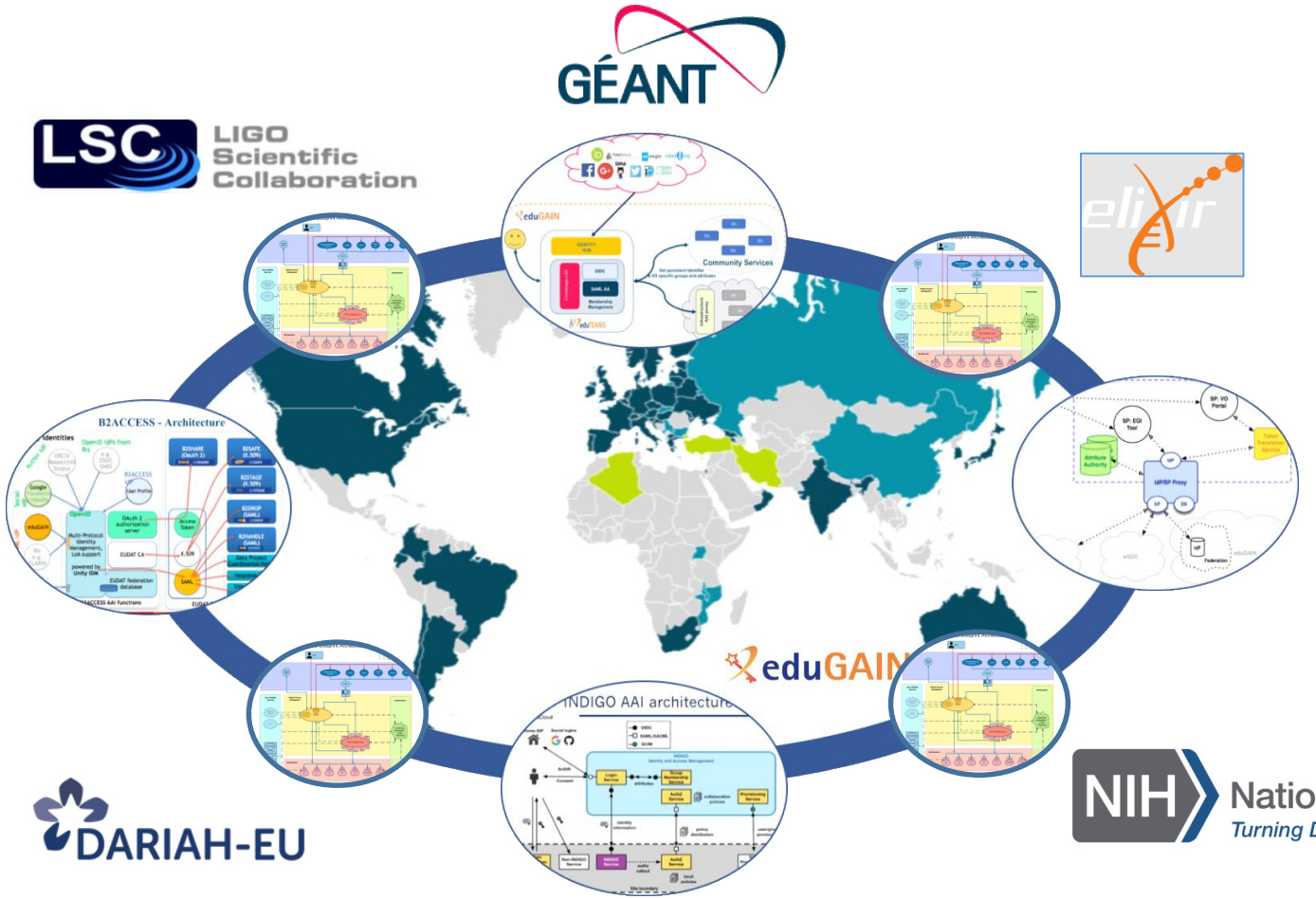




Delivery Platforms in AARC2

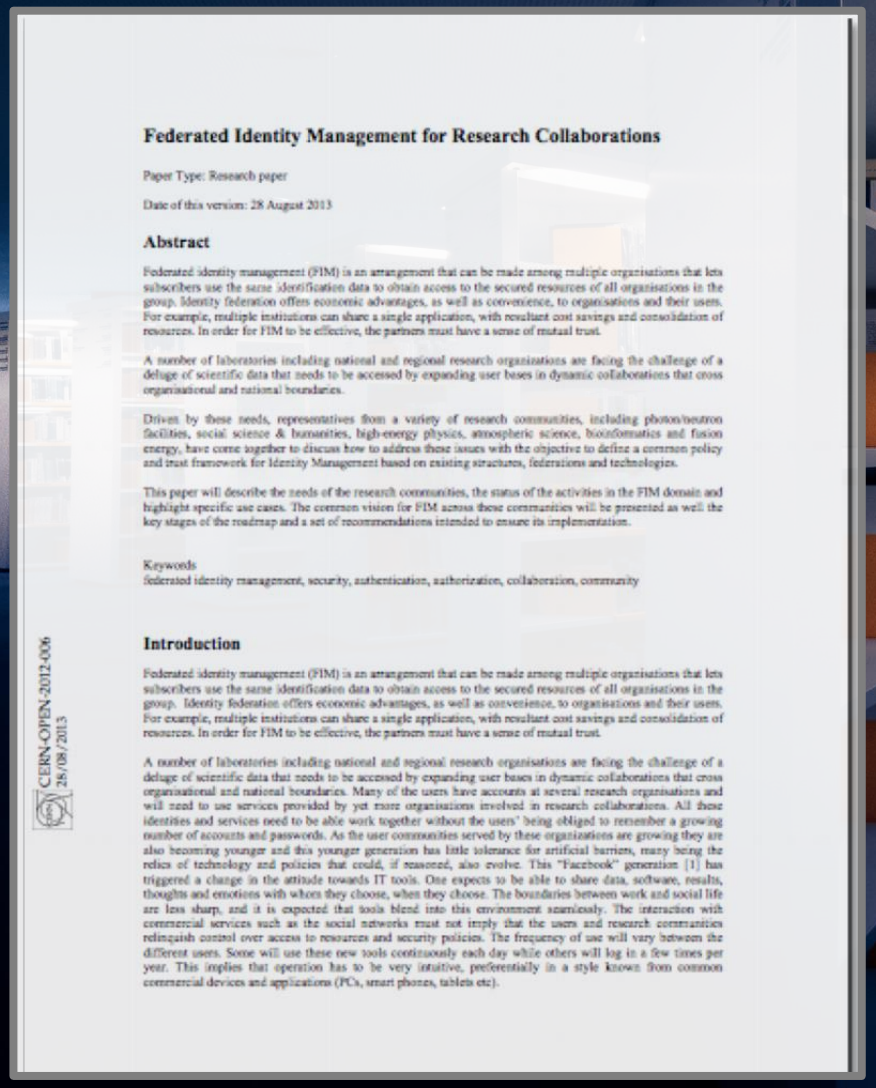


AARC Blueprint Architecture Implementations



https://aarc-community.org/about/aegis/

FIM4R



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 lets 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 savings 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 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 organisational and national boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based 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 stages of the roadmap and a set of recommendations intended to ensure its implementation.

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

Introduction

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets 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 savings 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).

CERN-OPEN-2012-006
28/08/2013

June 22, 2018

Journal article | Open Access

Federated Identity Management for Research Collaborations

Christopher John Atherton; Thomas Barton; Jim Basney; Daan Broeder; Alessandro Costa; Mirjam van Daalen; Stephanie Dyke; Willem Elbers; Carl-Fredrik Enell; Enrico Maria Vincenzo Fasanelli; João Fernandes; Licia Florio; Peter Gietz; David L. Groep; Matthias Bernhard Junker; Christos Kanellopoulos; David Kelsey; Philip Kershaw; Cristina Knapic; Thorsten Kollegger; Scott Koranda; Mikael Linden; Filip Marinic; Ludek Matyska; Tommi Henrik Nyrönen; Stefan Paetow; Laura A D Paglione; Sandra Parlati; Christopher Phillips; Michal Prochazka; Nicholas Rees; Hannah Short; Uros Stevanovic; Michael Tartakovsky; Gerben Venekamp; Tom Vitez; Romain Wartel; Christopher Whalen; John White; Carlo Maria Zwölf

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

What’s next?

FIM4R to continue former AARC work ?

- R/Communities are testing the BPA
- Could we get inputs ?
- Is there an opportunity via FIM4R to support some pilots?

- Training: could FIM4R help with some training events?
- Or maybe webinars?
- Which ones would be relevant?

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).