

EOSC AAI Implementation

Christos Kanellopoulos - GEANT

Slavek Licehammer - MUNI

Nicolas Liampotis - GRNET



**EUROPEAN OPEN
SCIENCE CLOUD**

Agenda

- **Introduction**
- **Implementing the EOSC AAI**
- **The evolution of the EOSC AAI**

EOSC Authentication and Authorization Infrastructure (AAI)

<https://op.europa.eu/s/phe7>

Authors

Klaas Wierenga, Leif Johansson, Christos Kanellopoulos, David Groep, Davide Vaghetti, Nicolas Liampotis

Contributors

Mark van de Sanden, Johannes Reetz, Sadaf Alam, Mikael Linden, Jens Jensen, Niels van Dijk, Andrea Ceccanti, Sander Apweiler, Bjorn Abt, Alex Vermeulen, Patrick Fuhrmann, Marcus Hardt, TF-members

SRIA - Strategic Research And Innovation Agenda

The purpose of authentication and authorisation infrastructure (AAI) in EOSC is to support the FAIR principles for data and services while enabling high-trust collaborations to be established and maintained with little or no friction to the end user

First Principles

- **User Experience is the first measure of success**
- **All trust flows from the communities**
- **There is no centre in a distributed system**

Extending the first principles

- The EOSC AAI is based on multi-lateral interactions and multilateral trust. Explicit, bilateral interactions are out of scope.
- The EOSC AAI model honours the autonomy and integrity of all members, and thus does not require unbounded trust between them
- The EOSC AAI enables the flow of attributes and properties that relate to collaborations, and are used for access to content, services, resources
- EOSC AAI Users give scoped and time-bounded permission for transfer of attributes

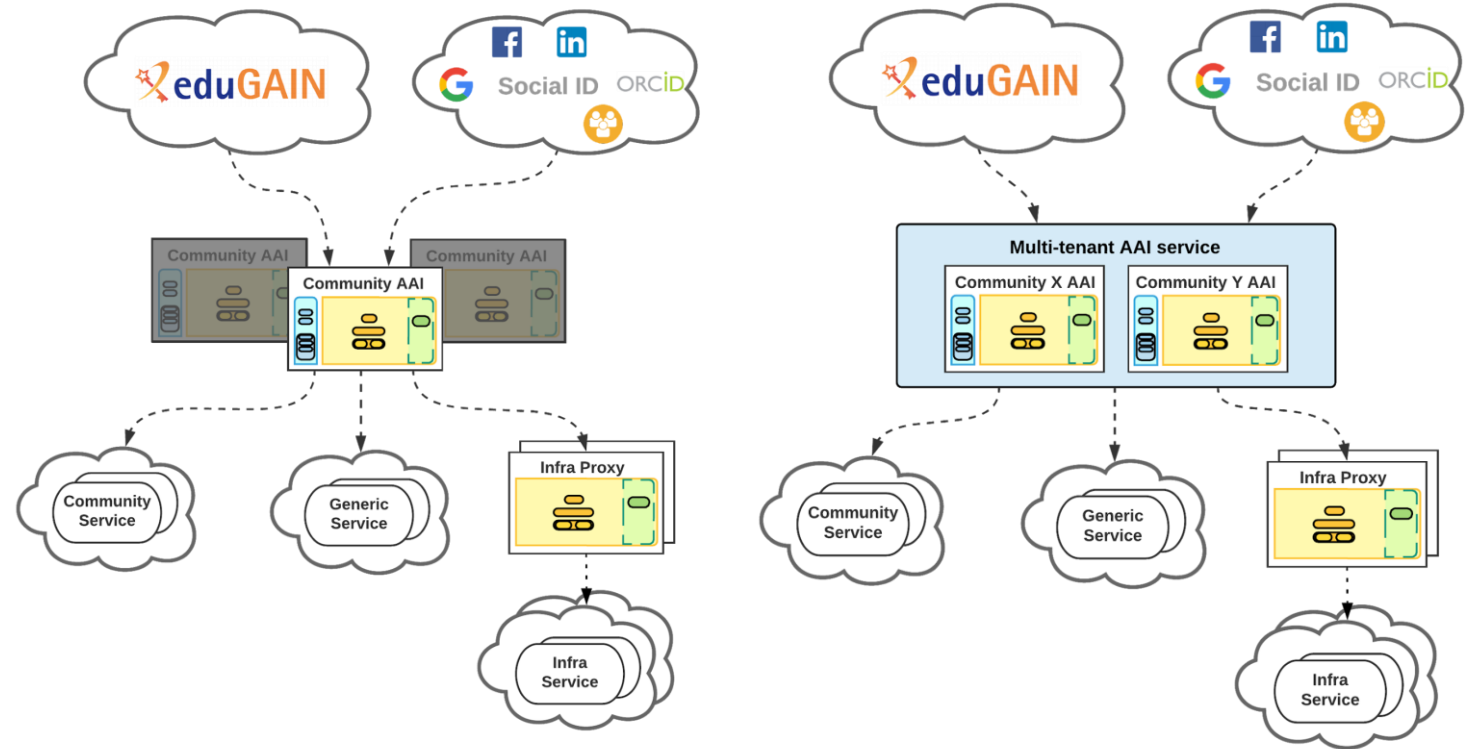
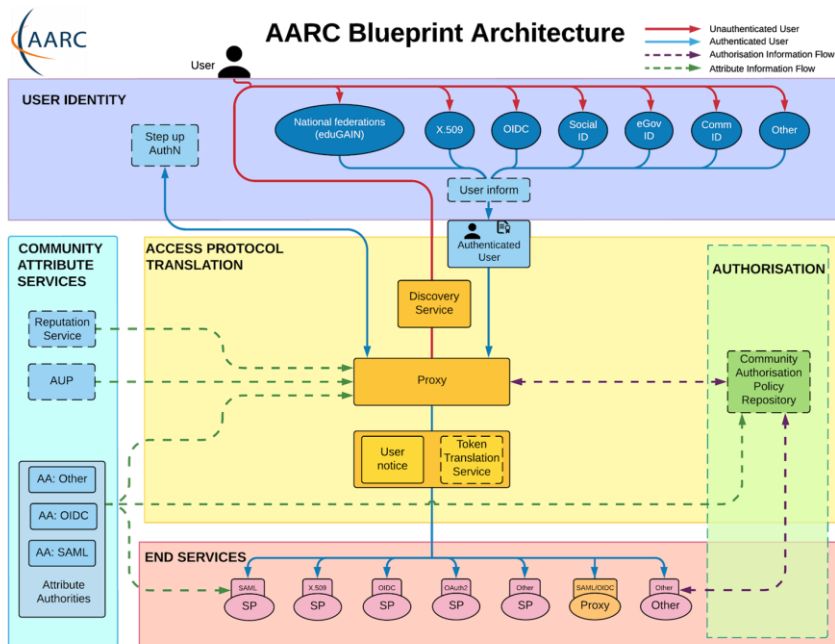
A Jump Point for the EOSC AAI

- Not reinventing the wheel; Build on top of the outcomes of AARC
 - The AARC Blueprint Architecture (BPA) with all of its extensions and the ongoing governance within the AEGIS group provide just the starting point for the work ahead
- In particular the AARC BPA:
 - builds on existing best practice in the scientific community
 - provides clear guidance for how campus identity integrate with science
 - comes with the beginnings of a governance structure in the AEGIS group
 - has international buy-in

EOSC AAI Architecture: Starting Point

- Started from AARC-BPA-2019 and the AARC Interoperability Guidelines

<https://doi.org/10.5281/zenodo.3672784>

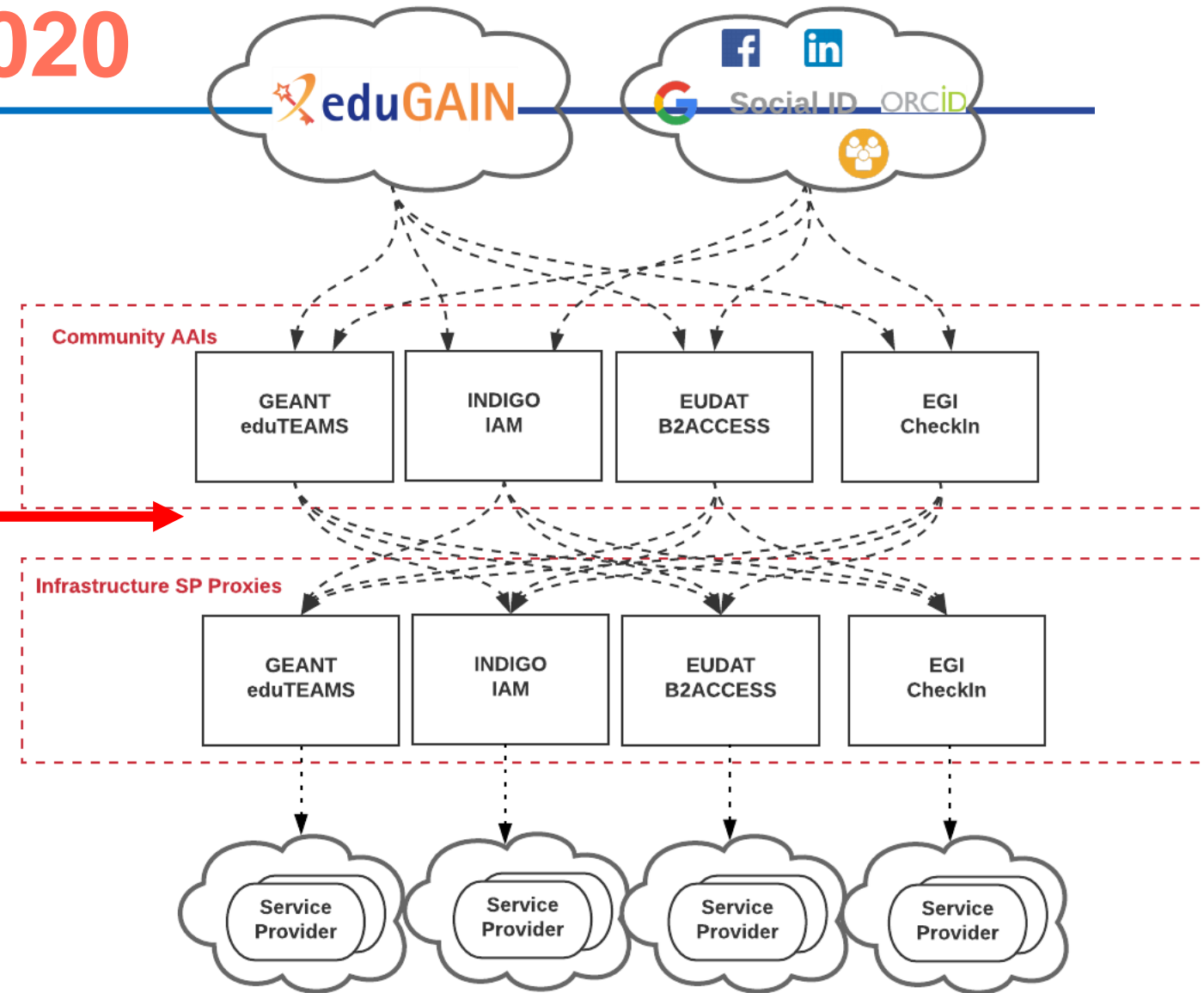


The EOSC AAI in 2020

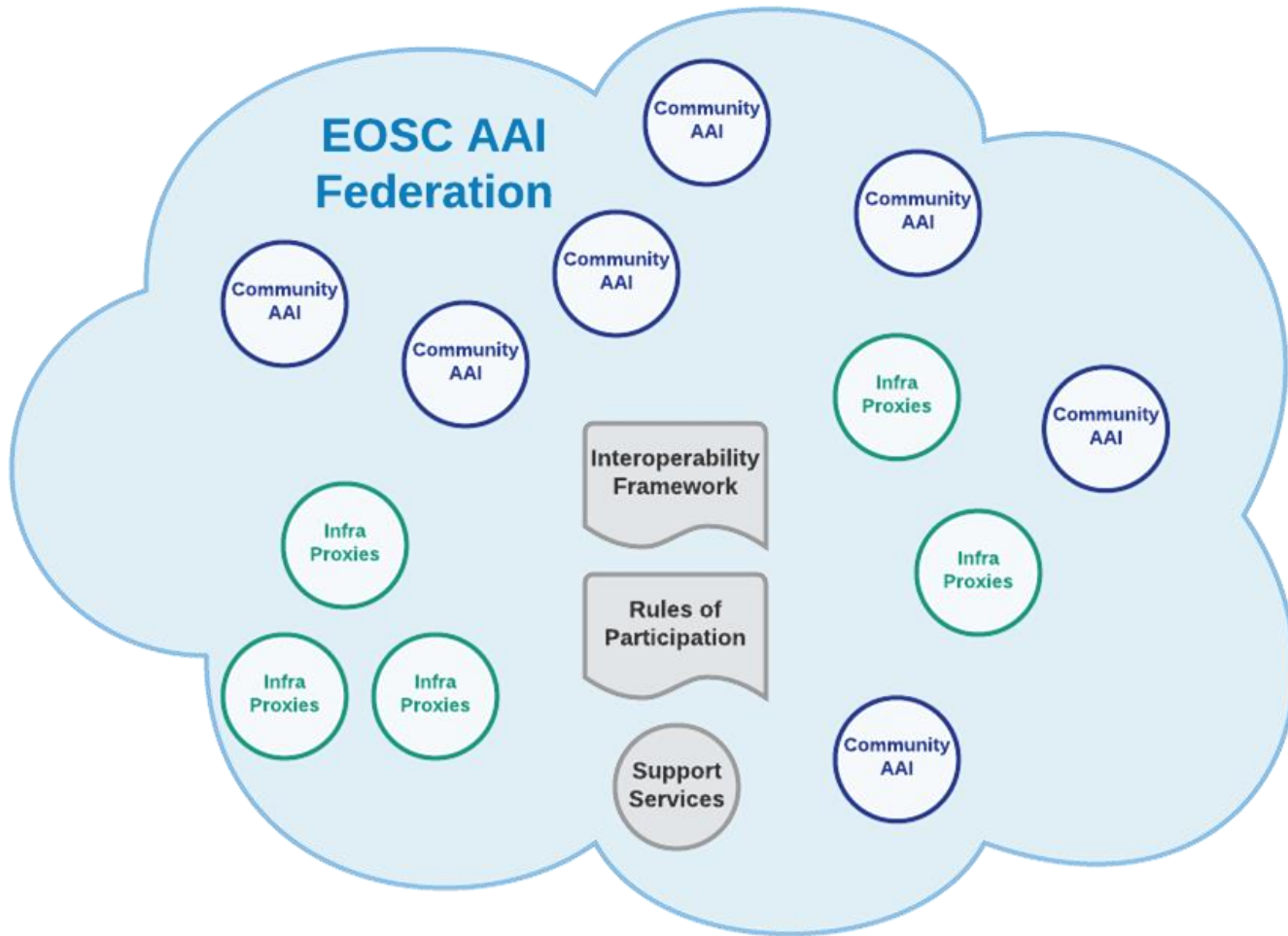
Members of the EOSC-Hub
AAI

Interoperability through the
implementation of the
AARC BPA Guidelines

- Each entity has to connect to each other entity (peer to peer)
- Cannot scale beyond a handful of Proxies

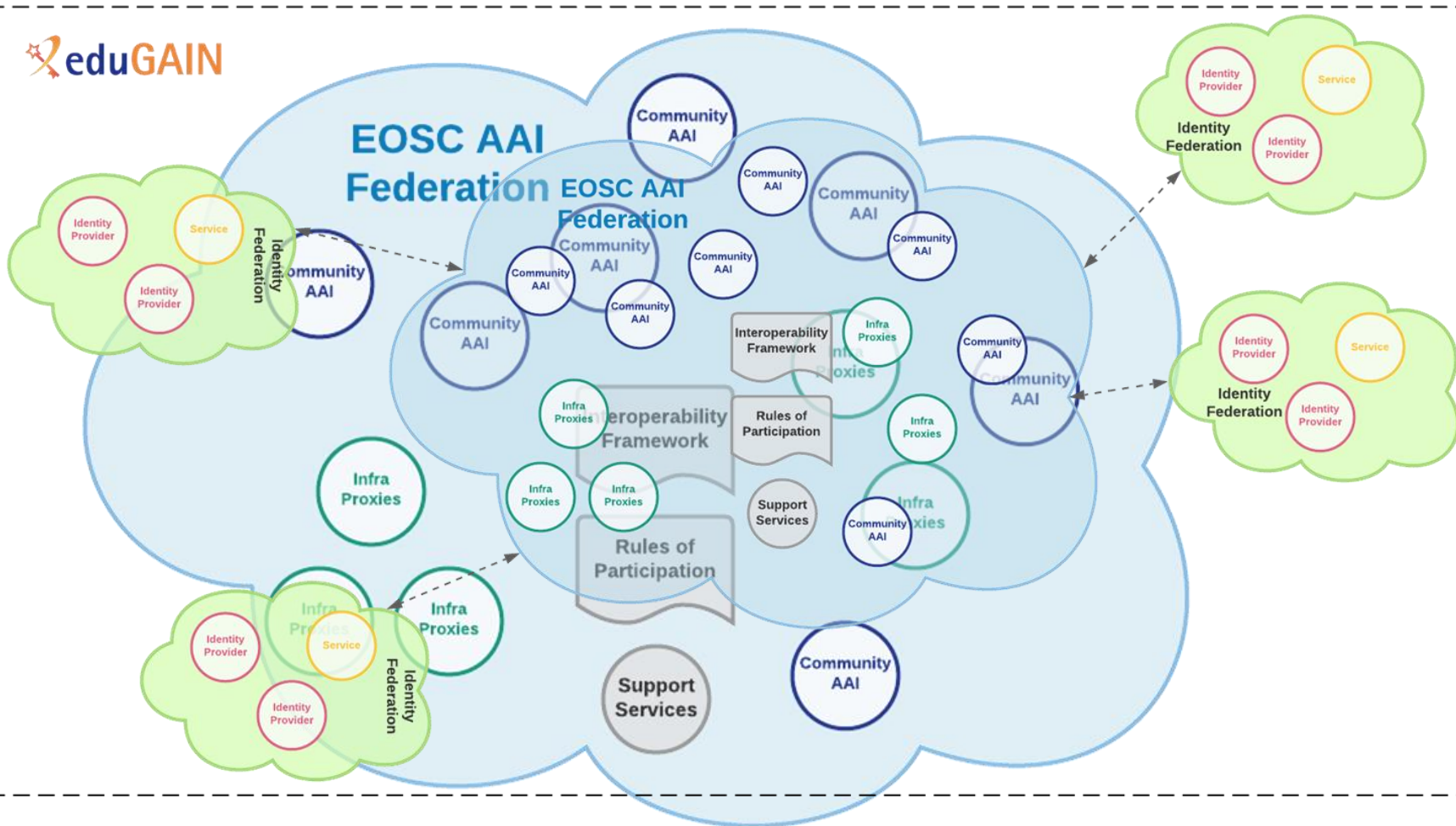


The EOSC AAI Federation



- Community AAI and Infrastructure Proxies connect once with the EOSC AAI Federation (register metadata, URN namespaces, policies etc)
- Technical interoperability conformance tested and monitored by the EOSC AAI Federation.
- GDPR and Security Policy conformance (Policy Notices, Acceptable Use Policy etc) assessed by the EOSC AAI Federation.
- Community AAI and Infrastructure Proxies discovery and establish trust with the rest of the Community AAI and Infrastructure Proxies through the EOSC AAI Federation

The EOSC AAI Federation



- Community AAIs and Infrastructure Proxies connect once with the EOSC AAI Federation (register metadata, URN namespaces, policies etc)
- Technical interoperability conformance tested and monitored by the EOSC AAI Federation.
- GDPR and Security Policy conformance (Policy Notices, Acceptable Use Policy etc) assessed by the EOSC AAI Federation.
- Community AAIs and Infrastructure Proxies discovery and establish trust with the rest of the Community AAIs and Infrastructure Proxies through the EOSC AAI Federation

THANK YOU



**EUROPEAN OPEN
SCIENCE CLOUD**