EOSC-hub

EOSC-hub Technical Workshop

AAI technical specification

Licia Florio (GÉANT), Nicolas Liampotis (GRNET)

eosc-hub.eu

@EOSC_eu

Dissemination level: Public

EOSC-hub receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 777536.

Agenda

- A word about TCOM AAI

- AAI Technical specification
  - Adopted standards
  - High-level Service Architecture
  - Interoperability guidelines
  - Examples of solutions implementing this specification
  - Procedure to integrate a service
  - Future plans

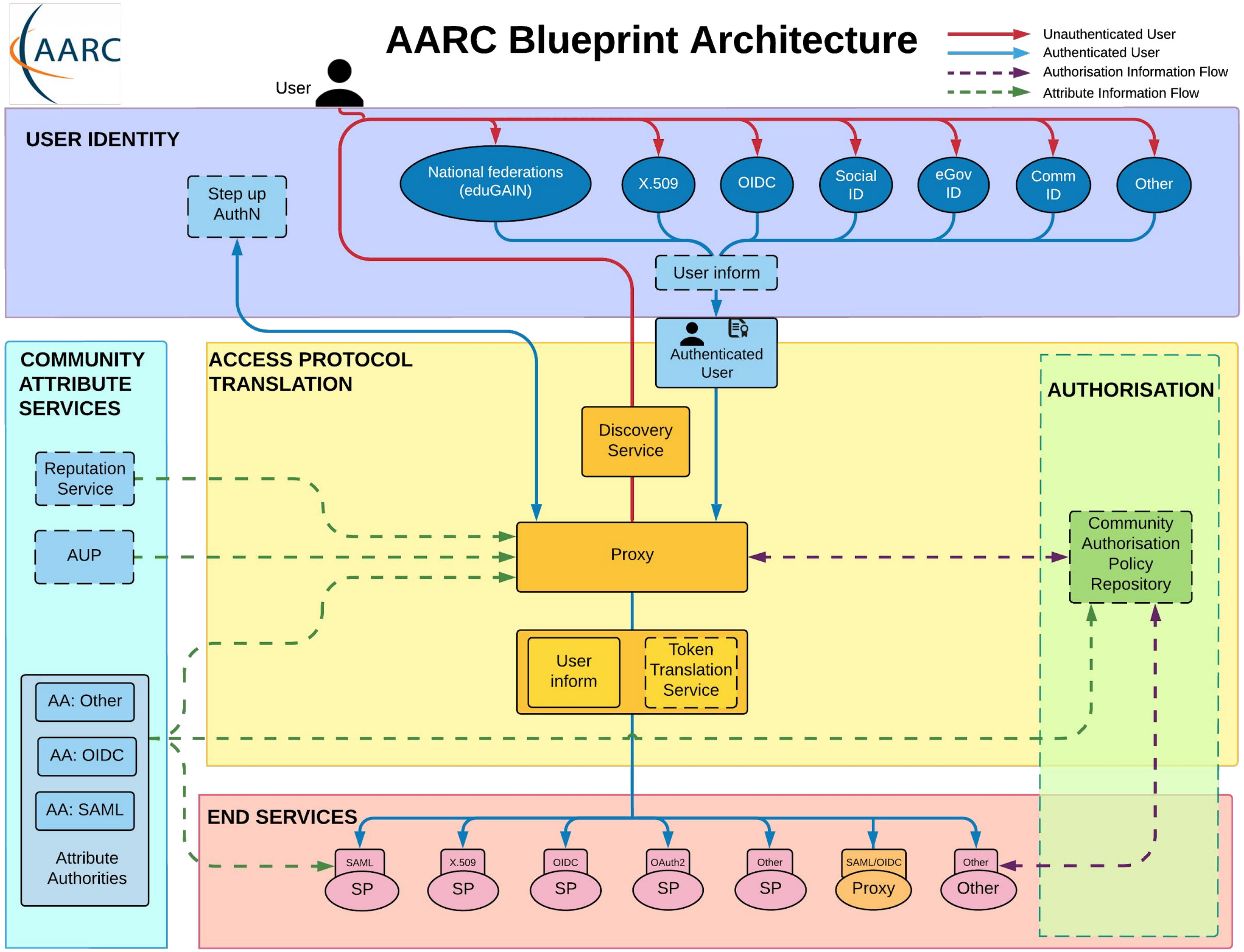
A word about TCOM AAI

- AAI Technical Coordinators in TCOM: oversee the technical development in the AAI area in EOSC-H
  - WP5 – Nicolas (where all the real work happens)
  - Also links to WP6
- Position shared with Michal Prochazka (CESNET)

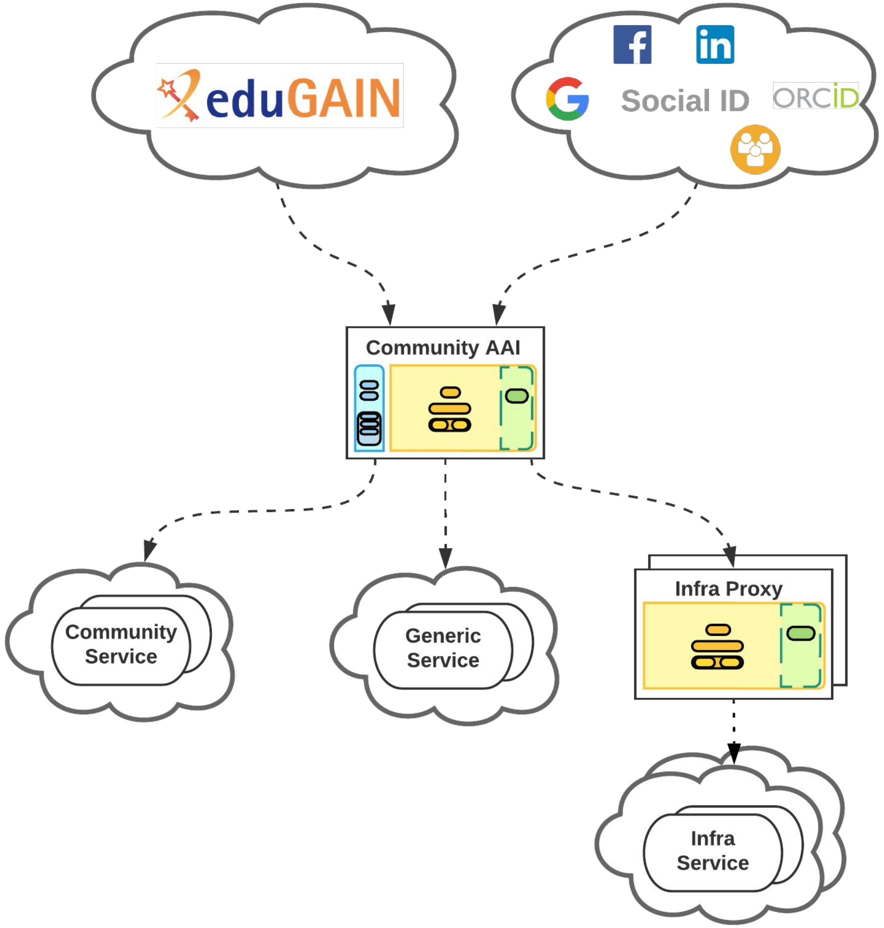
AAI technical specification

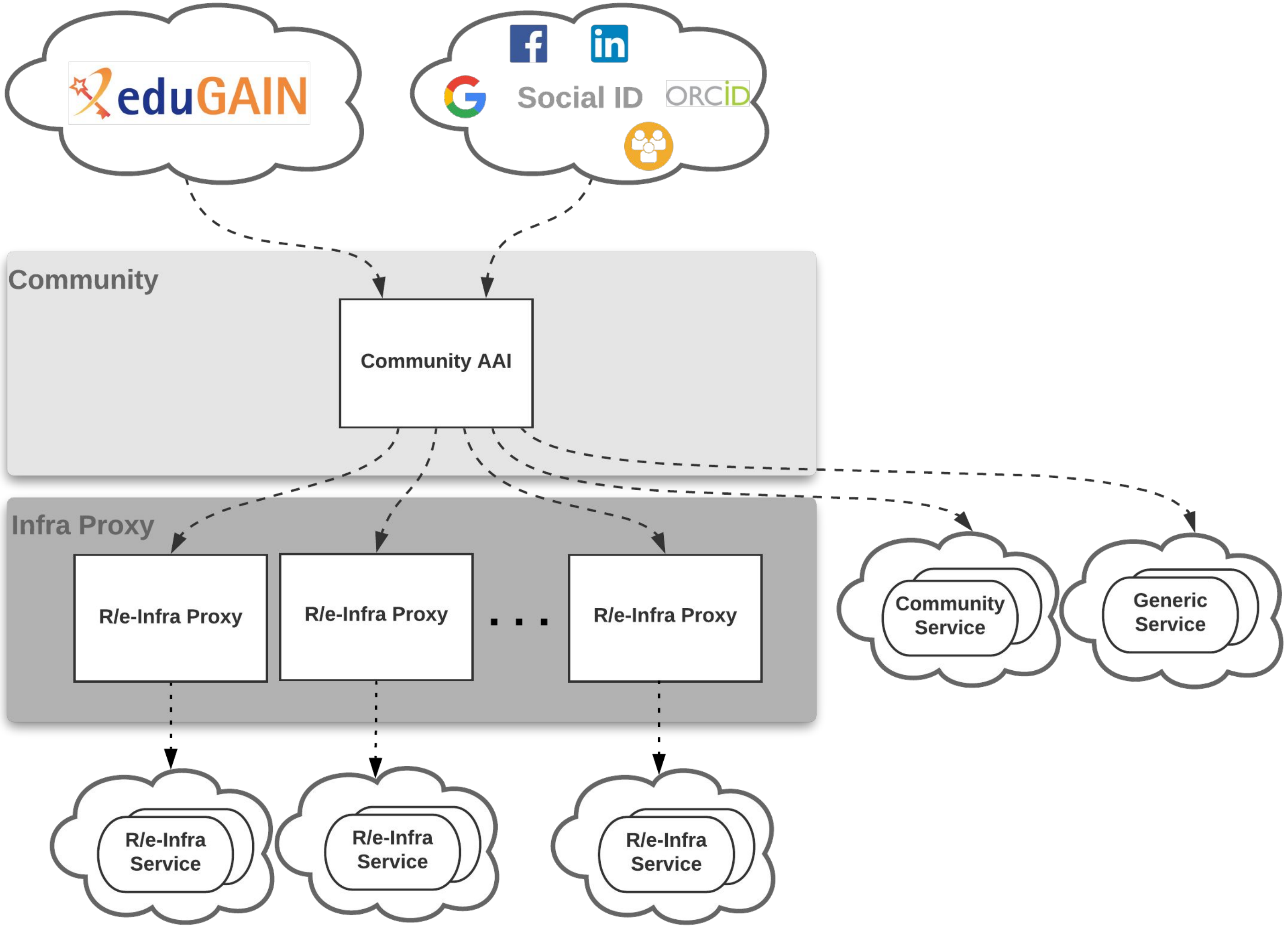
High-level Service Architecture

Starting point: AARC BPA

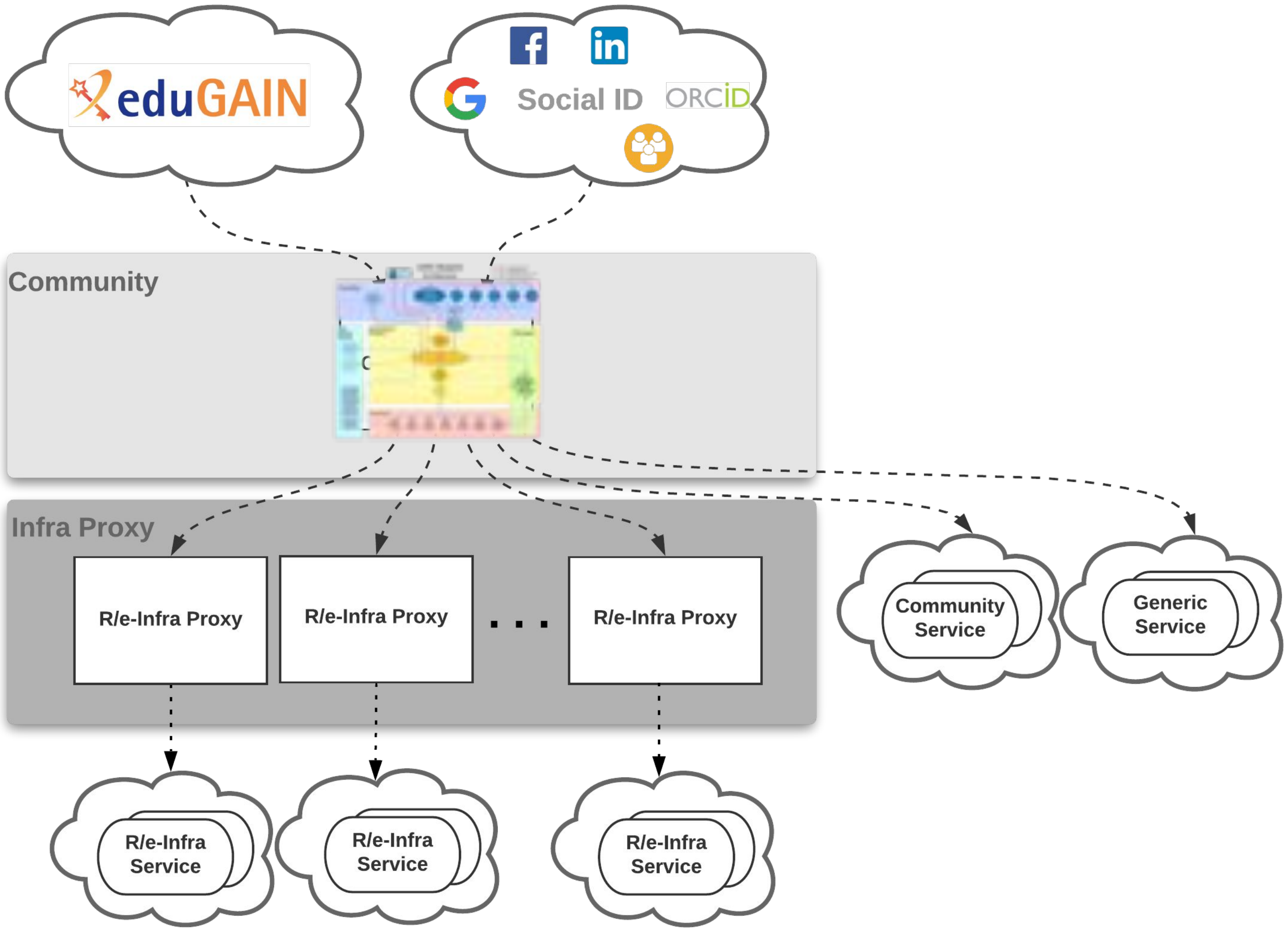


Architecture: Implementation of the AARC BPA
"Community-first" approach



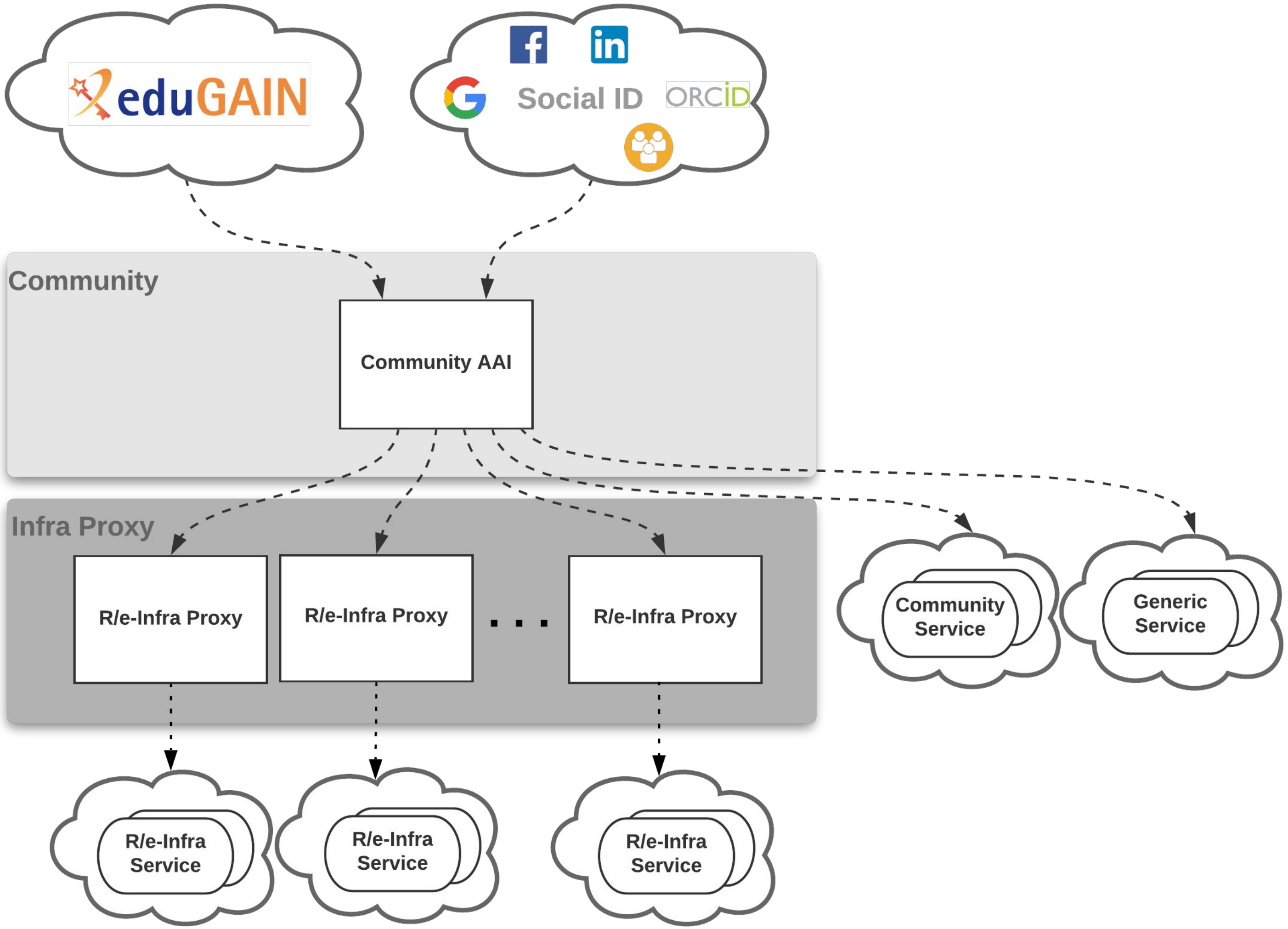


Architecture



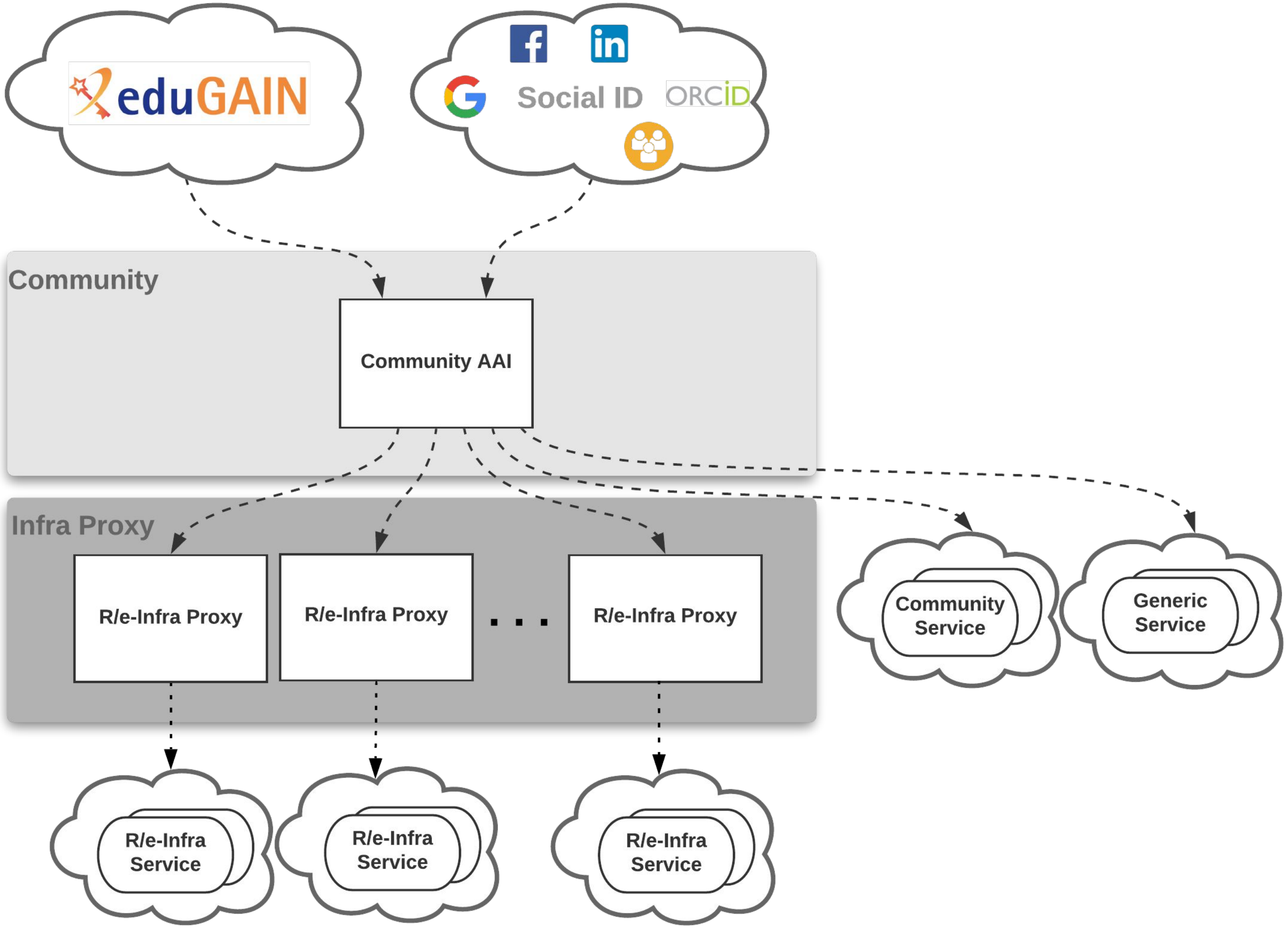
- Implementation of the AARC BPA “Community-first” approach:
  - Researchers register once with with their Community AAI
  - Researchers always sign in via their Community AAI for accessing:
    - **Community-specific** services
    - **Generic services** (e.g. RCauth.eu Online CA)
    - General-purpose **R/e-Infra services**

Architecture



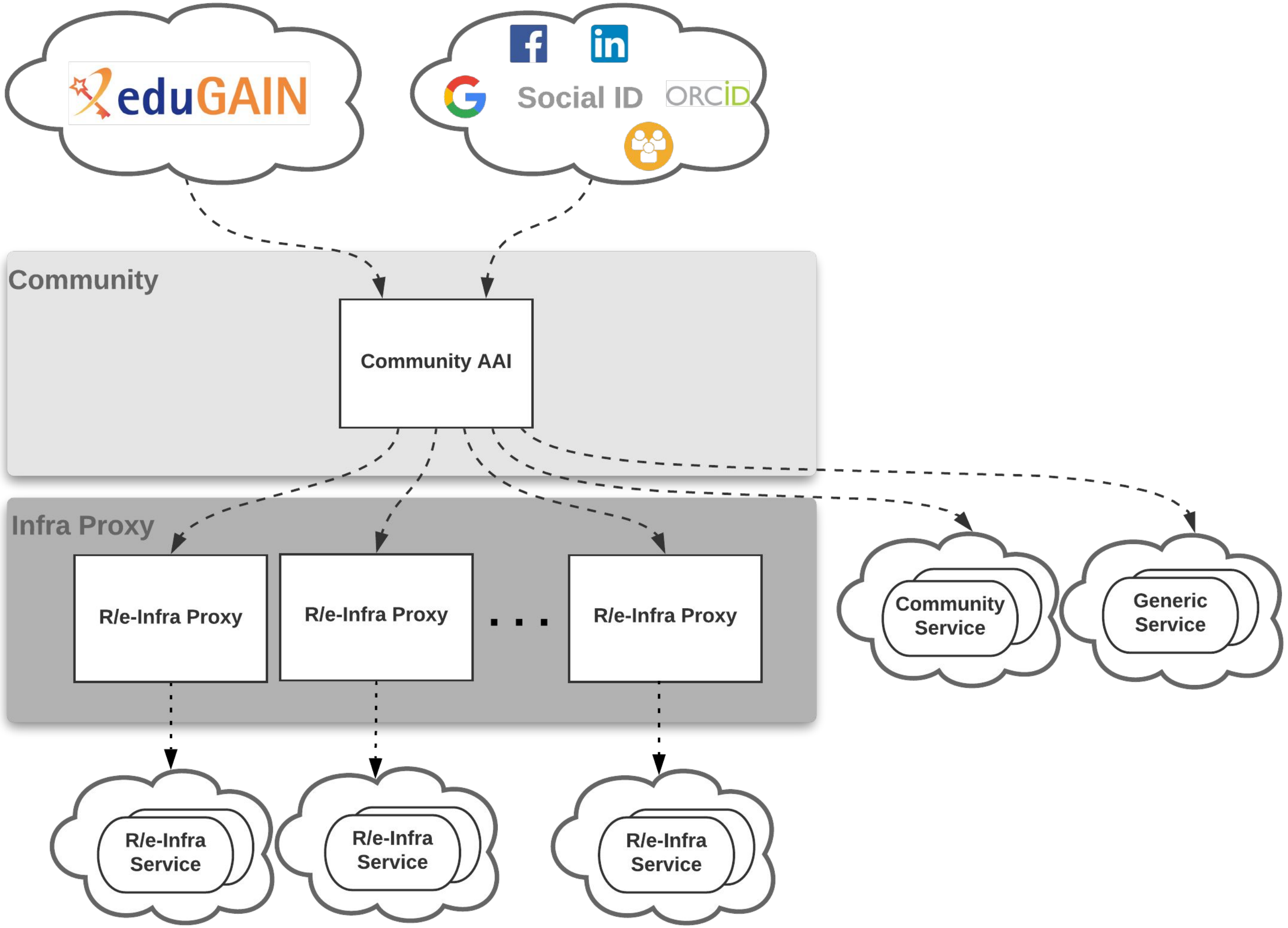
- EOSC AAI layers:
  - **Community:** Enables the use and management of community identities for access to EOSC resources
  - **Infra Proxy:** Enables access to resources offered by Service/Resource Providers connected to the R/e-Infrastructures.

Architecture



- Researchers register once with with their Community AAI
- Researchers always sign in via their Community AAI for accessing:
  - **Community-specific** services
  - **Generic services** (e.g. RCauth.eu Online CA)
  - General-purpose **R/e-Infra services**

Architecture



- Different Community AAI service offerings:
  - B2ACCESS
  - Check-in
  - eduTEAMS
  - INDIGO-IAM
- Communities operating an AARC BPA-compliant Community AAI can connect to the Infra Proxy layer to gain access to EOSC resources
- Infrastructures operating an AARC BPA-compliant Infra Proxy can connect to the Infra Proxy layer to make their resources available to different communities

AAI technical specification

Adopted standards

see also online document

EOSC-hub

Adopted standards

Standard	Short description	References
Security Assertion Markup Language (SAML) 2.0	OASIS standard for exchanging authentication and authorisation data between parties.	https://www.oasis-open.org/standards#samlv2.0
OAuth 2.0	Standard for authorisation that enables delegated access to server resources on behalf of a resource owner	"The OAuth 2.0 Authorization Framework", RFC 6749, https://www.rfc-editor.org/info/rfc6749
OpenID Connect 1.0	Identity layer on top OAuth 2.0. Enables Clients to (i) verify the identity of the End-User based on the authentication performed by an AS; (ii) obtain basic profile information about the End-User in an interoperable and REST-like manner	“OpenID Connect Core 1.0”, https://openid.net/specs/openid-connect-core-1_0.html

Adopted standards (Cont.)

Standard	Short description	References
X.509	ITU-T standard for a public key infrastructure (PKI), also known as PKIX (PKI X509)	"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, https://www.rfc-editor.org/info/rfc5280 "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile", RFC 3820, https://www.rfc-editor.org/info/rfc3820
Lightweight Directory Access Protocol (LDAP)	Provides access to distributed directory services that act in accordance with X.500 data and service models	https://tools.ietf.org/html/rfc4511

Adopted standards (Cont.)

Protocol/API	Short description	References
OAuth 2.0 Token Introspection	Protocol that allows authorised protected resources to query the authorisation server for determining the set of metadata for a given OAuth2 token, including its current validity.	https://tools.ietf.org/html/rfc7662
OAuth 2.0 Token Exchange	Protocol for requesting and obtaining security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation	https://tools.ietf.org/id/draft-ietf-oauth-token-exchange-14.html

Adopted standards (Cont.)

Protocol/API	Short description	References
OAuth 2.0 Device Authorization Grant	Enables OAuth 2.0 clients on input-constrained devices to obtain user authorisation for accessing protected resources without using an on-device user-agent	https://tools.ietf.org/html/draft-ietf-oauth-device-flow-15
System for Cross-domain Identity Management (SCIM) 2.0	Open API for managing identities	SCIM: Core Schema , RFC7643, https://tools.ietf.org/html/rfc7643 SCIM: Protocol, RFC7644, https://tools.ietf.org/html/rfc7644 SCIM: Definitions, Overview, Concepts, and Requirements, RFC7642, https://tools.ietf.org/html/rfc7642

Adopted standards (Cont.)

- Questions:
  - Are we missing anything?
  - Why the distinction: Standards vs. Protocols/APIs?

AAI technical specification

Interoperability guidelines

Technical interoperability guidelines

- Attributes for expressing user information should follow the REFEDS R&S attribute bundle, as defined in [REFEDS-R&S]
- VO/group membership and role information, which is typically used by relying parties for authorisation purposes, should be expressed according to [AARC-G002]
- Capabilities, which define the resources or child-resources a user is allowed to access, should be expressed according to [AARC-G027]
- Affiliation information, including
  - user's affiliation within their Home Organisation (e.g. university, research institution or private company)
  - affiliation within the Community, such as cross-organisation collaborations, should be expressed according to [AARC-G025]

Technical interoperability guidelines (Cont.)

- Assurance information used to express how much relying partins can trust the attribute assertions about the authenticating user should follow:
    - REFEDS Assurance framework (RAF) [RAF-version-1.0]
    - Guideline on the exchange of specific assurance information [AARC-G021]
    - Guideline for evaluating the combined assurance of linked identities [AARC-G031]
    - Guideline Expression of REFEDS RAF assurance components for identities derived from social media accounts [AARC-GO41]
    - Guidelines for expressing the freshness of affiliation information, as defined in [AARC-G025]
- OAuth2 Authorisation servers should be able to validate tokens issued by other trusted Authorisaton servers → requires extending existing flows (e.g. OAuth2 Token Exchange flow [OAuth2-Token-Exchange-draft])

Policy interoperability guidelines

- Compliance with the GÉANT Data Protection Code of Conduct version 1 (DPCoCo-v1) [DPCoCo-v1] → reflects the Data Protection Directive and means compliance with applicable European rules (see [AARC-G040])
  - To explicitly declare compliance with DPCoCo-v1, the privacy notice of each EOSC AAI service should include a reference to DPCoCo-v1
- The entities of the EOSC AAI registered with eduGAIN should meet the Sirtfi [Sirtfi-v1.0] requirements and express Sirtfi compliance in their metadata in order to facilitate coordinated response to security incidents across organisational boundaries.
- To reduce the burden on the users and increase the likelihood that they will read the AUP as they access resources from multiple service and resource providers, the EOSC AAI services should adopt the WISE Baseline AUP model [WISE-AUP]

AAI technical specification

Examples of solutions implementing this specification

Examples of solutions

- AAI services:
  - B2ACCESS
  - Check-in
  - eduTEAMS
  - INDIGO-IAM
- Membership Management Systems:
  - Perun
  - COmanage Registry
  - HEXAA
- Token Translation Services:
  - WaTTS
  - MasterPortal
  - RCauth.eu

AAI technical specification

Procedure to integrate a service

Procedure to integrate a service

- B2ACCESS
- Check-in
- eduTEAMS
- INDIGO-IAM
- Perun
- COmanage
- WaTTS
- MasterPortal
- RCauth.eu

AAI technical specification

Future plans

AAI Roadmap

https://confluence.egi.eu/display/EOSC/Roadmap

Thank you for your attention!

Questions?

Contact

licia.florio@geant.org
nliam@grnet.gr

EOSC-hub

eosc-hub.eu @EOSC_eu