VOPaaS

Virtual Organisation Platform as a Service

Niels van Dijk

GÉANT Trust and Identity Service Development

Technical Product Manager, SURFnet, The Netherlands

AARC General Meeting

Nov 4, 2015, Milano

About GÉANT

- GÉANT is Europe’s leading collaboration on network and related infrastructure and services for the benefit of research and education, contributing to Europe's economic growth and competitiveness. The organisation develops, delivers and promotes advanced network and associated e-infrastructure services, and supports innovation and knowledge-sharing amongst its members, partners and the wider research and education networking community.
- GÉANT has 41 member countries and is owned by its core NREN membership, and also has Associate members including commercial organisations and multi-national research infrastructures and projects.
- Almost all members of GÉANT operate Iden and GÉANT operated the eduGAIN interfede members also collaborate to design and deliver services.

VO Platform as a Service

Goal:
Investigate the conditions that would allow GÉANT to provide services to support Virtual Organisations

- Focus on delivery of Technical services (IAAS or PAAS)
- Out of scope:
  - Technical development
  - Policy & LOA development

Activities:

- Gather requirements and priorities with/from communities
- Look at *existing* tools and technologies
- Operations and Market
- Look into delivery model
- Investigate business case & sustainability

Requirements for building on Federated AAI as a VO

- The FIM4R paper (April 2012) was one of the first to articulate collective requirements for using Federated AAI for VOs
- Many VOs have chosen to build the AAI infrastructure using the national and eduGAIN infrastructures
- Identity Federations and Identity providers are however traditionally focused on Campus use cases, which introduces a number of challenges for VOs in leveraging Federated AAI
- The VOPaaS project has performed a survey among several small and large Pan-European VOs to (re-)validate the FIM4R requirements
- From the results of this Survey, functional requirements were analyzed,
- A number of services were proposed to be put in place to support VOs on a Pan-European level.

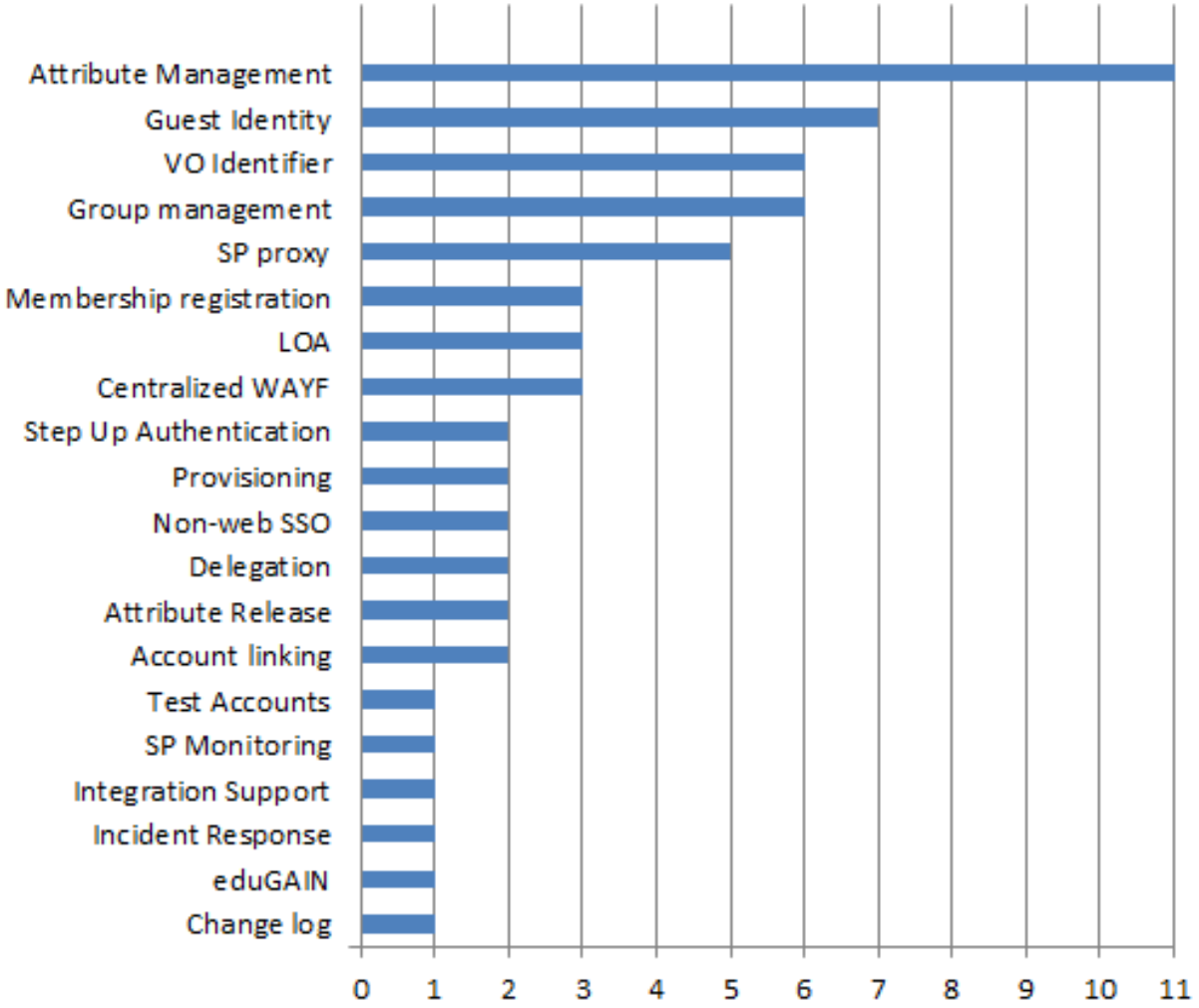
VOPaaS Market Analysis

- Interviews and desk study conducted with:
  - Umbrella (Large neutron and photon facilities)
  - CLASSe (Shared IaaS)
  - DARIAH (Humanities)
  - CERN (High Energy Physics)
  - CLARIN (Humanities and social sciences)
  - Virtual Campus Hub (eLearning, Renewable Energy)
  - ELIXIR (Life Sciences, Bioinformatics)
  - GÉANT VAPIRE (NREN collaboration).

- Broad NREN/federation participation:
  AMRES, CESNET, DFN/LRZ, GARR, IUCC, NIIF, RENATER, SUNET, SURFnet, SWITCH

- Final DRAFT report:
  https://wiki.geant.org/display/gn41sa5/Market+Analysis

VOpaas Market Analysis Results



Function requirements for VOPaaS

Functional requirements identified

- **Persistent Identifier** - Allow the VO to identify the user even if (s)he changes IdP
- **VO Membership Registry** - To become members of the VO a certain workflow must be followed
- **'External' Identities** - Many VO users will not be in eduGAIN
- **Attribute Management** - Attributes beyond the IdP are needed for VO roles and rights, or to provide extra context (e.g. ORCID, Grant number)
- **Group Management** - groups may also be used to define roles and rights
- **(de)Provisioning** – Identity, attributes and groups need to be provided to Services
- **Service Proxy and Attribute Aggregation** – A centralised infrastructure to operate on behalf of the VO Service Providers

Deployment model *

Basic Services

- Operated by GÉANT
- Also for VOs that are not legal entities
- Operated as a (set of) Services

Advanced Services

- Operated by GÉANT *on behalf of* a *VO*
- Somebody – a legal entity - must take responsibility for that data
- Operates as per VO applications on VM ‘boxes’

Basic Services

Basic Services

- **VO Membership service**
  - registry for **VO persistent Identifier**
  - VO specific **Workflows for onboarding**
  - **Limited set of attributes**
  - Accessible through eduGAIN & extIDp

- **External Identity Provider (extIDp)**
  - One persistent (SAML) IdP for many ‘Guest’ Identity Providers, including:
    - Social (Google, Twitter, Linkedin, Facebook)
    - NREN operated & Commercial Guest IdPs (OpenIDP, UnitedID.org, eduID.se)
    - eGOV (STORK)
    - BankID
  - Provides LOA: eIDAS by default, others upon request from SP
  - Available and accessible through eduGAIN

Advanced Services

Advanced Services

- **(advanced) Attribute Management -** Whatever you can come up with
- **(advanced) Group Management -** Groups in groups, etc.
- **Provisioning -** For web and non-web resources, ‘application specific connectors’
- **Service Proxy and Attribute Aggregation** – To have a central point for technology and policy
- Accessible through eduGAIN & extIDp
- Managed by VO operator
- May be delivered as a paid service

Tools

Basic Services

- VO Membership service: COmanage
- External Identity Provider (extIDp): SaToSa

Advanced Services

Attributes and Groups: Comanage, HEXAA and PERUN

- SP Proxy: OpenConext

VOPaaS Future

2015

- ~~Market Analysis~~
- Cost Benefit Analysis & Business Model
- Deploy pilot platform

Q1 2016

- Run pilots with Basic Services, in collaboration with AARC
- Support application integrations

2016

- Production service for Basic Services
- Deploy Pilots for Advanced Services
- Possibly: pick up new services as developed within GEANT, AARC or others

GÉANT

Networks • Services • People

www.geant.org

This work is part of a project that has applied for funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).