19-10-2017

Deliverable D9.2 Virtual Organisation Platform Phase Two Service Specification

Deliverable D9.2

Contractual Date:	31-07-2017
Actual Date:	19-10-2017
Grant Agreement No.:	731122
Work Package/Activity:	9/JRA3
Task Item:	Task 2
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	SURFnet
Document ID:	GN4-2-17-797FB
Authors:	Niels Van Dijk (SURFnet), Mandeep Saini (GÉANT), Ann Harding (SWITCH), Christos Kannellopoulos (GÉANT), Tangui Coulouarn (DEIC), Jean-Marie Thia (CNRS)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Abstract

This document outlines the technical and service specification for Phase 2 of eduTEAMS, the platform for GÉANT that extends beyond eduGAIN to serve the AAI needs of collaborative organisations.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

In GN4-2, a subtask within JRA3 Task 2 has been working to develop, integrate and extend a set of components to prepare a service offering for Virtual Organisations, which has been branded eduTEAMS.

This work is based on the findings reported in GN4-1 Deliverable D9.2 Market Analysis for Virtual Organisation Platform as a Service [GN4-1 D9.2]. The development of Phase 1 of this activity ended in July 2016 with the successful delivery of the first stage of eduTEAMS Membership Registration and Identity Hub. This document describes and contextualises Phase 2 of the delivery of eduTEAMS, along with some proposed developments and improvements.

Following identification of requirements in the market analysis conducted in GN4-1, features were prioritised, key components to deliver those requirements were evaluated and selected, and two classifications for use eduTEAMS cases – basic and advanced – were identified. The requirements identified by the VO Platform market analysis are in line with those subsequently identified by the AARC [AARC] project as part of their wider evaluation of research requirements.

The basic use case classification focuses on long-tail usage of federated identity and group management, while the target users for the advanced use case scenario are large Virtual Organisations having a defined legal status and more complex requirements for group and attribute management, as well as control over VO-specific data.

Approaches to service delivery for the use cases were then defined in terms of software development, platform architecture, service approach and outreach. These include: a development approach that combines existing open source components with glue developed by GÉANT to deliver a platform to meet a range of use cases; a platform architecture composed of flexible interoperable components; and a service operational model which enables this common eduTEAMS software platform to deliver either single-tenant or multi-tenant service instances.

Phase 2 development of eduTEAMS takes place within the parameters of these approaches and will cover the following areas:

- General platform improvements to UIS, manageability and scalability.
- Implementation of additional membership management workflows.
- Support for non-SAML attribute authorities.
- Integration of a wider range of identity providers.
- Migration to enhanced discovery services.
- Improved ability to integrate services.

1 Introduction & Background

Scientific research is at the heart of every European University. Such research is not typically conducted as an isolated activity, but involves extensive and dynamic collaborations between networks of researchers in multiple countries. Virtual Organisations (VOs) have emerged as the organisational representation of these networks of people and resources.

During the previous GN4-1 project, a work item was started within SA5 – Trust and Identity Service Development, with the purpose of assisting these VOs to use AAI facilities more effectively and easily for their collaborations. These developments are known collectively as Virtual Organisation Platform as a Service (VOPaaS).

The development of Phase 1 of this activity ended in July 2016 with the successful delivery of the first stage of eduTEAMS Membership Registration and Identity Hub. This document describes and contextualises Phase 2 of the proposed developments and improvements to the delivery of eduTEAMS.

This introductory section of the document outlines the background to the developments proposed in Phase 2, including the preparatory work carried out in GN4-1. In particular, it highlights the use cases to be served, ranging from the long tail of collaboration to large-scale, formalised research infrastructures.

The focus of Phase 2 will be on enhancements to transition to production supporting the basic use case, and on the introduction of new features driven by concrete examples for the advanced use cases. The developments foreseen for Phase 2 of eduTEAMS development are described in in section 2.

The components that were delivered in Phase 1 are included for reference in Appendix A.

1.1 Use Cases

The requirements and details of key stakeholders in VOPaaS were collated and published during the previous GN4-1 project as Deliverable D9.2 Market Analysis for Virtual Organisation Platform as a Service [GN4-1 D9.2].

Another project, AARC [AARC], which looked at a wider range of research requirements than those for the initial VOPaaS service, also began during the time when the VOPaaS project was conducting its market analysis. AARC is an EC-funded project that brings together 20 different partners including National Research and Education Networks (NRENs) organisations, e-Infrastructures service providers, and libraries.

AARC is driven by the requirements of research communities, with the aim of identifying building blocks and policy best practices needed to implement interoperable authentication and authorisation infrastructures (AAIs). It was agreed that eduTEAMS would support the AARC architecture and be included in AARC pilots. The requirements identified by the VO Platform market analysis were confirmed to be in line with those subsequently identified by AARC as part of their wider evaluation of research requirements once these were published.

Following identification of requirements in the market analysis, features were prioritised and key components to deliver those requirements were evaluated and selected. The primary work of JRA3 T2 in GN4-2 has been to integrate, extend and test these components to prepare a service offering which has been branded eduTEAMS. This work has included categorising the requirements into use cases, based on which development, architecture service and outreach approaches have been defined, and designing a flexible platform architecture capable of delivering a scalable service environment.

Based on the recommendations drawn from the Market Analysis conducted during the previous GN4-1 project, a number of use cases falling under two classifications – basic and advanced – have been identified for eduTEAMS. These use cases helped to identify the core architecture for the platform by providing a way to identify which components could commonly serve a wide range of use cases, and which have a more specific application. The use cases also provided a means to plan service operational models based on the degree of control and autonomy vs. skillset and expertise. Details of the two use case classifications are given below.

1.1.1 Basic Use Case

One basic use case was identified focusing on long-tail usage of federated identity and group management for collaborations that may not be covered by a legal entity or not be established for long-term sustainability. These collaborations normally do not have a formal IT environment and are not bound to any particular e-Infrastructure for service use. Based on statistics from CORDIS, of the 13,643 projects funded by the EU under Horizon 2020 from 2014 to 2020, over 4,000 have more than one participant organisation and therefore by implication have collaboration requirements [CORDIS].

In the basic use case, it is anticipated that collaborations will have neither the wish nor the ability or requirement to operate or customise the service. To serve this market segment, the eduTEAMS service operator is required to control the functional capabilities of the service being offered on behalf of the collaborations. The eduTEAMS service operator is expected to take responsibility for the legal requirements that are placed on the eduTEAMS platform, for example with regard to data protection and privacy of the data held on the eduTEAMS platform. From a deployment scalability perspective, all of the platform capabilities serving the basic use case are best deployed as a multi-tenant service, supporting many collaborations within one functional application.

To scale a multi-tenant service, a lightweight and tightly specified approach to service delivery is needed. This includes requirements to implement restrictions on the data about users and their entitlements that can be stored and delivery of a set of off-the-peg workflows, allowing basic group management and prohibiting creation of arbitrary attributes.

1.1.2 Advanced Use Cases

The second set of target users are large Virtual Organisations having more complex requirements for group and attribute management as well as control over VO-specific data and shared resources. Unlike the basic use case, where a simple set of requirements meets the needs of a large number of user groups and is therefore expressed in a single use case, it is anticipated that there will be a number of distinct, advanced use cases driven by how these larger organisations already operate. These organisations, which are typically represented by a legal entity, are able and indeed likely to prefer to assume the operator role for the delivery of a service instance.

More complex group and resource management requirements and integration with the VO's existing systems are requirements for the advanced use case. In addition, as the VO requires control over data, support for creation of additional attributes is foreseen.

Some collaborative organisations may also have some pre-existing functionality in place that overlaps to some extent with the core eduTEAMS platform, but with more customisations relevant to their services. In this type of scenario, these organisations may prefer to either integrate or outsource the tool they are already using into an eduTEAMS environment. Support for the advanced use cases should therefore enable a fully tailored and independent service solution based on the eduTEAMS components for these organisations.

Through connecting eduTEAMS to established infrastructures GÉANT is well positioned for collaborative service delivery with partners. GÉANT's lead role in ensuring sustainability of support by directly developing and supporting leading components for membership registration, attribute management and cross-sector technology translation make it an attractive partner for such collaborative endeavours. The service-provider neutrality that the GÉANT eduTEAMS platform offers is also seen to be another very important feature.

1.2 Approach

Having outlined the use cases, approaches to service delivery were defined. These cover software development, platform architecture, service approach and outreach. Phase 2 development takes place within the parameters of these approaches.

1.2.1 Software Development

The development approach for eduTEAMS is to deliver a platform composed of a flexible set of components that can be combined into different operational models to meet the requirements of basic and advanced use cases. Phase 1 of the eduTEAMS platform software development focussed primarily on the components common to both basic and advanced use cases.

In terms of core functionality, both use cases overlapped strongly on the need for group management, the ability to transport attributes at scale and the need for integration of external identities. This drove the priorities of Phase 1 delivery, as outlined in Appendix A. Phase 1 of eduTEAMS development was completed successfully by the delivery of the eduTEAMS Membership Registration and eduTEAMS

Identity Hub components in August 2016. More information about Phase 1 is available in Appendix A. This release enables the highest priority requirements identified by research communities in the GN4-1 Market Analysis to be met.

New features added in Phase 2 of the eduTEAMS platform development will focus on more complex, advanced use cases for virtual organisations. This will build on the infrastructure and components delivered in Phase 1 to enhance them and will extend the platform with further components as needed. In parallel, the robustness and scalability of the Phase 1 components will be continuously improved.

The principle of using well-established open-source platforms such as COmanage will continue to be followed, with GÉANT strengthening its ties with Internet2's TIER programme where Grouper and COmanage are developed, as well as by directly supporting COmanage and pushing features upstream. Where functionality beyond the core components is needed and exists in community solutions, GÉANT can act as a broker connecting the creators and owners of a range of key infrastructure components such as Perun [Perun], HEXAA and Grouper [Grouper] to the individual virtual organisations to ensure that the VO has sustainable support for their choice.

Although GÉANT does not support the software and deployment environment it uses for eduTEAMS infrastructure outside the eduTEAMS service models, these components are all provided as Open Source software. This prevents vendor lock-in for the VOs and allows for potential collaboration between similar deployments, e.g. on a national level by NRENs.

1.2.2 Platform Architecture

The core eduTEAMS platform architecture is composed of existing interoperable modular components. In the advanced use cases, this architecture can be extended, or different elements swapped for compatible existing VO infrastructure. An important requirement for the architecture was to ensure compatibility with the AARC Blueprint Architecture [BPA]. The AARC BPA provides a framework for interoperability of federated identity components between infrastructures. It is aimed at software architects and technical decision makers who design and implement access management solutions for international research collaborations and should be supported to promote its long-term sustainability and scalability.

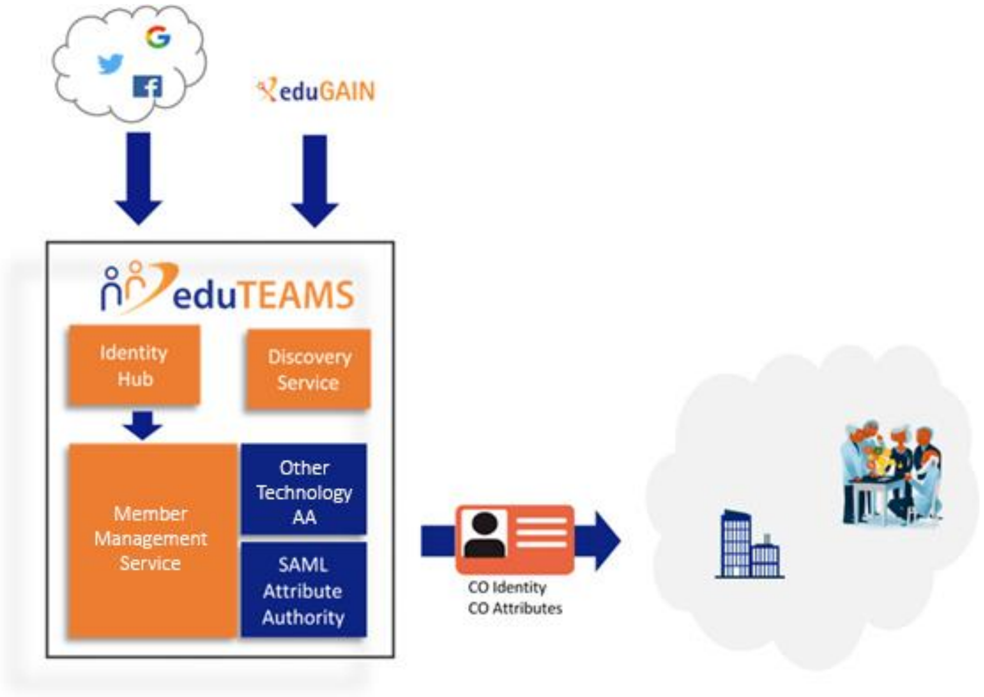

Figure 1.1: eduTEAMS high-level architecture

The diagram above shows the elements of the eduTEAMS high-level architecture. The main elements in this architecture are as follows:

- The Membership Management Service provides a platform for managing groups, attributes and enrolment for participants in research collaborations. It includes:
  - a registry for the research collaboration persistent Identifier for individuals;
  - research collaboration-specific workflows for on-boarding;
  - attribute authorities to provide additional attributes and groups information for the participants in the context of the collaborations.
- The Identity Hub allows research collaborations to work flexibly with participants from outside the footprint of the academic identity federations in eduGAIN, using external identity providers (e.g. Google, LinkedIn etc.).
- The Discovery Service allows research collaborations to easily customise the list of organisations that users can choose to log in to while at the same time providing a modern visual appearance with mobile support.
- A Proxy Service will interact with the components in the diagram as a gateway between the resources of the research collaboration and any externally provided services.

1.2.3 Service Development

The infrastructure components of the eduTEAMS platform delivered during both Phase 1 and Phase 2 can be used to address either use case type. The primary differences between the basic scenario and the advanced use cases are the degree of expertise within the communities, the need for control over information about users, and the degree of additional customisation and support for integration with existing VO infrastructures. The approach used is to address these differences primarily in service development, rather than in software implementation. This leads to the development of two operational modes, multi-tenant for the basic use case and single tenant for advanced use cases.

The basic use case envisions an eduTEAMS service operated by GÉANT for the benefit of all users of Identity Federations whose institutions participate in eduGAIN. Many GÉANT members do not have a collaborative platform in place, or are mainly focused on national collaboration so that they have no clear solution for service-independent, cross-border group and attribute management.

For the basic eduTEAMS use case, access to the eduTEAMS service should primarily be routed through the NRENs or their respective Identity Federations. This means that NRENs/Identity Federations can deliver a service by enabling a Collaborative or Virtual Organisation to gain access to the eduTEAMS infrastructure. At the same time, they may take on the responsibility for adding content services such as wikis, NREN file sharing or cloud services, or other collaborative tools on top of eduTEAMS to enhance collaboration (inter)nationally for their communities.

It is envisioned that for the advanced use eduTEAMS cases, services will be delivered by GÉANT as an infrastructure service, but operated on a functional level by technically skilled staff of the VOs themselves. This implies the operational environment is a single tenant model, with one VO occupying one service instance. Such a neutral environment therefore provides the advantages of flexibility and control to the research community while enabling responsibility for updating and managing infrastructure to remain with the eduTEAMS operator.

In contrast to the multi-tenant, off-the-peg approach, meeting advanced use cases will require custom implementation, which carries scaling concerns. CORDIS indicates there are 38 projects with 40 or more partners, i.e. of a similar size and complexity to GÉANT’s and other major e-Infrastructures and research infrastructures. By leaning on a common eduTEAMS platform as the basis, GÉANT can then work in partnership with communities to broker expertise for additional features.

The flexibility resulting from building two operational models using a common eduTEAMS platform will allow research communities to operate according to their requirements and abilities, enabling them to benefit from a fully independent AAI infrastructure regardless of who operates the services connected to the platform.

While service development in Phase 1 concentrated primarily on the business and operational models to address the basic use case, preliminary estimates and proposals for piloting with a number of advanced use cases were also prepared. These proposals will be tested by piloting in parallel to Phase 2 development.

In parallel with running the pilots, the task will run the necessary Product Lifecycle Management processes to proceed to production. This includes identifying a business model and sustainability strategy for addressing the advanced use cases, taking into account the funding and operational environment of developments such as the European Open Science Cloud, as well as of NREN and VO-specific environments.

1.2.4 Outreach

The outreach approach for eduTEAMS is to engage both research communities and NREN/Federations. While the research requirements remain relatively stable, since the initial market analysis several national federations are starting to look at replacing legacy group management and authorisation systems or introducing a service offering in this space where previously they did not. While this interest was partially anticipated in the basic use case, NRENs are also introducing advanced scenarios. Outreach will therefore be flexible about which service option NRENs wish to pilot.

In Phase 1, piloting took place with Umbrella [UMBRELAID], the AAI platform for the synchroton community, enabling improvements in UI and workflow to be included in the first release of the eduTEAMS platform. This close collaboration with communities is planned to be continued in Phase 2. Demonstrations were delivered to Jisc and SURFnet and briefings took place to SWITCH, GARR, the Life Sciences Community [CORBEL] and to a range of infrastructures via a dedicated AAI session for the European Open Science Cloud pilot project [EOSCPILOT].

In Phase 2, this outreach will translate to committed pilots with Umbrella (continued), EUDAT, Jisc and SURFnet. Interoperability pilots in the context of AARC to trial and pilot eduTEAMS with other e-Infrastructures and research infrastructures are also committed. The goal of these interoperability pilots will be to demonstrate that the eduTEAMS platform is compliant with the AARC Architecture, and therefore fully and openly interoperable, including with solutions that currently serve particular e-Infrastructures.

Expressions of interest from SWITCH, GARR and the Life Sciences Community, following the briefings, will be followed up with the intent to operate pilots.

2 Phase 2 Specification

2.1 Phase 2 Technical Specification

The following features have been identified for inclusion on the Phase 2 eduTEAMS development roadmap, based on direct feedback from pilots, trials and workshops, pre-existing items identified in the market analysis, and improvements on operations and manageability related to transitioning from pilot to production. Development roadmap priorities are listed below. These will be reviewed and set for every release based on pilot and trial feedback.

The target date for the delivery of Phase 2 is July 2018. The delivery strategy for phase 2 will be frequent 'point' releases between the time of writing of this report and July 2018.

2.1.1 General Platform Improvements

- Implementation of an instance of eduTEAMS Membership Management Service to manage service provisioning permissions and workflows.
- Ensuring the scaling model works to engage with nation level entities, in response to results from stress testing.
- Allow provisioning data to LDAP backend at national entity.

2.1.2 Membership Management Service

- *Simplify or enhance existing workflows based on use cases.*

  A key workflow is onboarding of users to access services. The MMS already provides a number of these workflows, which are part of the base COmanage application. Phase 1 piloting demonstrated that some communities require either simpler or more enhanced workflows. For example, OpenAIRE representatives identified that the existing COmanage onboarding and user management workflows are too complex for their user base. At the other end of the spectrum, engagement with the Life Sciences communities has shown that they have very specific onboarding requirements that go beyond what COmanage supports e.g. automation of adding new communities. Such functionality is very important for the integration of eduTEAMS MMS with other e-Infrastructure providers, which are already supporting a number of scientific communities.

- *Deploy a more modern GUI for COmanage.*

  The latest version of COmanage comes with a revamped GUI that is both more modern and functional while bringing much better support for mobile devices and improved accessibility following Web Content Accessibility Guidelines [WCAG]. In Phase 1, GÉANT worked with COManage developers to enhance its usability. This work will continue in Phase 2.

- *Test and deploy a Data Connector to contact Attribute Authorities, specifically ORCID [ORCID].*

  Many groups that eduTEAMS is targeting already have existing legacy systems that they are using to manage their collaborations. Extending the MMS to implement Data Connectors for external sources will enable the smoother adoption of eduTEAMS. ORCID specifically is a service that is already widely accepted by scientific communities and funding bodies. Being able to integrate the ORCID identifiers in the MMS will enable users of the services to seamlessly use ORCID information to organise their users.

- *Deliver a proxy component for attribute aggregation based on OIDC*

  Version 1.0 of the MMS supports attribute aggregation as a SAML AttributeAuthority (SAML AA) using the SAML2.0 AttributeQuery mechanism, thus supporting integration with SAML-based SPs using back-channel mechanisms.

  A proxy component that can provide an OIDC interface towards the SP, and which will be able to act as a SAML SP in eduGAIN, will enable the integration of MMS with SPs using the more lightweight OIDC protocol and would allow support of front-channel attribute query.

  The main benefits of the front-channel attribute queries are that (a) the MMS and the SP do not have to establish a pre-shared identifier for the users and (b) user consent can be managed per user at the time of the attribute release. The downside of the OIDC proxy-based attribute aggregation is that SP cannot query MMS without user interaction, but this is already supported by the existing SAML AA interface.

  A pilot with EUDAT's B2Access component will drive this feature.

- *An additional REST API (OAuth) to source attributes, supplementing the existing SAML AA.*

  Given the implementation of the OIDC-based attribute aggregation, it will be trivial to implement a similar OAuth2 interface, which can be used for back-channel attribute release similar to the SAML AA. This capability will allow OIDC/OAuth2 to query MMS asynchronously, without the need for user interactions. This is a very common requirement when there is no continues interaction between the user and the service.

- *Support for Step Up Authentication in collaboration with JRA3 Task 3 on MFA, and AARC and REFEDS recommendations and profiles respectively.*

  Support for step-up authentication is a requirement that has been identified by many communities that are dealing with sensitive data or are sharing highly valuable resources. Providing step-up authentication capabilities interacting directly with the MMS will allow users of the service to benefit from one integrated group management solution. JRA3 Task 3 on MFA is already working in collaboration with AARC2 and REFEDS on providing an initial service offering that can be integrated by the eduTEAMS MMS.

2.1.3 Identity Hub

In global research some communities may include researchers without federated identities, thus a "guest identity" type solution is required. Further integration and testing of more ID providers is therefore important.

Expanding this component gives users without access to a federated identity a broader range of options for participating in a virtual organisation without having to set up or maintain an additional identity. Some examples of commonly used Identity Providers outside R&E include:

General ID providers:

- Paypal [PAYPAL]
- MojeID [MOJEID]
- Government provided eIDs, in coordination with eduGAIN and eIDAS [EIDAS] interoperability pilots.

Other commercial and non-commercial ID providers, including corporate use:

- Onegini [ONEGINI]
- UnitedID [UNITEDID]
- Okta [OKTA]
- PingID [PINGIDENTITY]

2.1.4 Discovery Service

- Introduce revamped discovery services with new capabilities, when they become available, as developed in RA-21 project [RA21].

2.1.5 Integration with Services

- *Implement support for simple non-web access*

  Terminal access via SSH is one of the top-ranking requirements expressed by the scientific communities. The AARC project has tested a solution based on the ability for users to store and self-manage SSH keys, in a similar manner to the way users manage their SSH public keys on GitHub and similar services. The AARC tests were successful and the solution was very well received by the communities participating in the tests.

- *Implement support for Moonshot*

  Driven by requirements from Jisc and Umbrella (in collaboration with other projects).

- *Deliver a Service Provider Proxy (SP Proxy) component*

  Advanced use cases from scientific collaborations require a turn-key solution for managing access to their resources. Typically, these collaborations need to be able to integrate a wide range of services that are developed and operated by different teams using different technologies. Most of these services are internal to the communities and thus should not be exposed to the public. The SP Proxy component provides an important abstraction layer that enables the implementation of solutions that hide the AAI complexities between the various components of the infrastructure. The SP Proxy component will follow the Blueprint Architecture guidelines of the AARC project [BPA] and will enable any central entity operated by a VO to aggregate attributes from the Membership Management Service, use the upcoming Step-Up authentication capabilities of the platform and support multi-protocol SPs (SAML, OIDC, OAuth2).

The need for this component was re-affirmed at the recent FIM4R meeting in Montreal [FIM4R-11], in which all the scientific collaborations presented their needs for such SP proxies acting as integration gateways.

2.2 Service Specification Phase 2

For the basic use case, it is planned for the service to be operated by GÉANT in multi-tenant mode and be offered to virtual organisations at no additional cost. Demand for this operational mode will be assessed during pilots and a decision on sustainability will be made based on NREN interest and adoption vs. cost of delivery.

Service offering and support models for the multi-tenant mode will follow the 'channel' approach, with the NREN/Federation as the initial point of contact for a virtual organisation and eduTEAMS providing support to the NREN.

The advanced use cases are based on a single-tenant delivery model with the virtual organisation itself acting as the operator. In its capacity as the platform provider, GÉANT will operate the infrastructures in close collaboration with NREN partners and deliver or broker custom developments on a cost-recovery basis via appropriate mechanisms ranging from project collaborations to direct cost recovery. NRENs can also take on the role of operator themselves for a service instance if their national requirements are a better fit for the advanced use case.

The service offering for single-tenant mode should also follow the channel approach where possible, as the NREN/Federation plays a key role in channelling the virtual organisations towards the service and may also be engaged in cost recovery mechanisms for organisations they connect, similarly to the business model in use by TCS. Support, however, is offered directly to the VO Operator by eduTEAMS.

Operational considerations such as Service Level Specifications will be refined for both single-tenant and multi-tenant offerings, including provisioning time for access to the service, availability and other relevant operational metrics mandated by SA2.

3 Conclusion & Timeline

Work on delivering the items described in this Phase 2 eduTEAMS Specification began at the end of Period 1 of GN4-2.

The features described in the specification will be assigned to release cycles delivered iteratively, with priorities driven by the results of pilots. The timeline for these cycles is shown in Figure 3.1. Smaller point releases are also expected, alongside updates specifically to support pilots. These will be aggregated for the general platform in the cycles shown below.

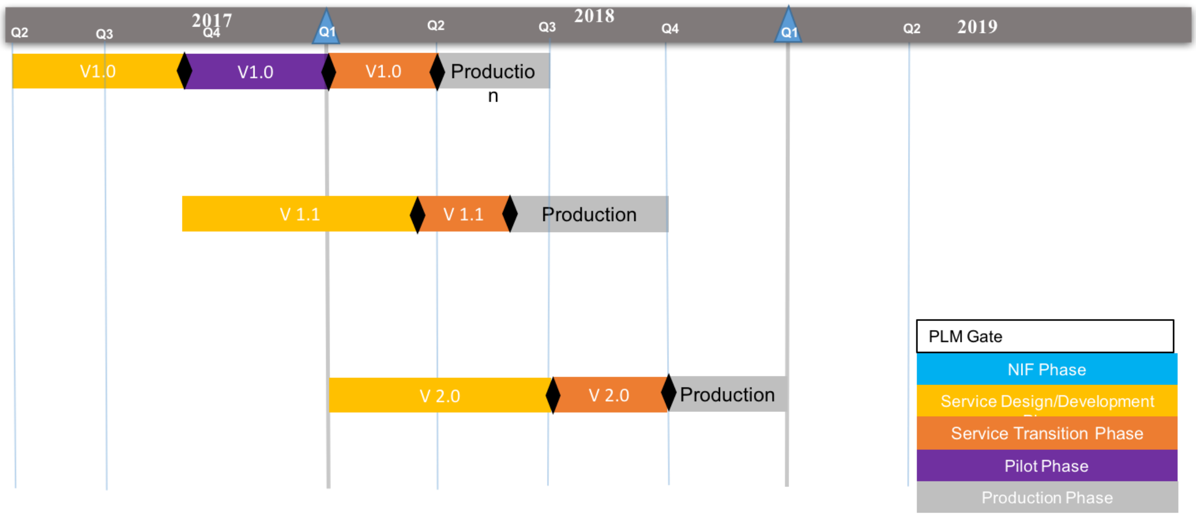

Figure 3.1: eduTEAMS Phase 2 release cycles

Appendix A eduTEAMS Phase 1 Delivery

A.1 Phase 1 Approach

Phase 1 focussed primarily on the use case for basic usage scenarios. Solution components were integrated and tested, and technical trials and pilots took place with both NREN and research community candidate users. At the same time, requirements gathering continued for advanced use cases.

From the requirements identified in the market analysis [GN4-1 D9.2] and complementary AARC work carried out, Phase 1 addressed the highest priority needs and collated them into a single basic use case.

Development cycles were focussed on two main infrastructure components to support group management and guest access requirements. Delivery was via a combined approach of integrating well-known existing components and contributing requirements upstream, developing and enhancing components where there was no alternative, and simply sourcing a compatible functionality from an NREN with a production service.

A.2 Phase 1 Infrastructure

In Phase 1, eduTEAMS release 1.0 the following components were delivered:

A.2.1 eduTEAMS Membership Management Service

Based on COmanage 2.0, with upstream enhancements contributed and commissioned by GÉANT.

- A registry for research collaboration Persistent Identifiers.
- Research collaboration-specific Workflows for on-boarding.
- VO specific information supported via "eduPersonEntitlement", a standard URI that indicates a set of rights to specific resources. This ensures a high degree of interoperability.
- SAML AA.

A.2.2 eduTEAMS Identity Hub

Based on SaToSa [SATOSA], with enhancements contributed by GÉANT, the Identity Hub provides the following features:

- Support for OpenID Connect Identities:
  - Google and Facebook implemented and tested.
- Support for OAuth Identities:
  - ORCID ID implemented;
  - Github implemented;
  - Linkedin implemented.
- Account linking to enable recovery of access in the event of a loss of primary account.

A.2.3 eduTEAMS Discovery Service

This service is offered semi-independently of the platform, based on the CESNET Discovery Service.

- The default integration of the service is simple “one line configuration” presenting a list of trusted Identity Providers for the Service Provider.
- Uses production system of an NREN, with customisation for eduTEAMS

Appendix B Overview of Requirements Delivery

This appendix lists the requirements/features as described in the GN4-1 Market Analysis deliverable [GN4-1 D9.2], and outlines which features were addressed in eduTEAMS Phase 1, which will be addressed in Phase 2, and what is externally provided through NREN partnerships, by REFEDs or as part of eduGAIN.

Requirement	Phase 1	Phase 2	Provided externally
Attribute Management	Delivered	Enhancements	
Guest Identity/External ID Provider	Delivered	Enhancements	
VO Identifier	Delivered		
Group Management	Delivered	Enhancements	
SP Proxy		Planned	
Membership Registration	Delivered	Enhancements	
Assurance			REFEDS Assurance Framework
Discovery/Centralised WAYF	Delivered	Enhancements to use new discovery service developments	Agreement with CESNET Discovery Service for immediate requirements
Step Up Authentication		Planned	Collaboration with JRA3 T3
Provisioning	Delivered		
Non Web SSO		Planned	

Requirement	Phase 1	Phase 2	Provided externally
Delegation	Delivered	Enhancements	
Attribute Release	Delivered	Enhancements	Research & Scholarship Entity Category[1]
Account Linking for recovery	Delivered		
Test Accounts			eduGAIN Access Check
SP Monitoring		Planned	
Integration Support		Planned	
Incident Response		Planned	SIRTFI adoption
Change logs		Planned	
eduGAIN integration	Delivered		eduGAIN[2]

Table B.1: Requirements delivered in each phase of eduTEAMS

[1] https://refeds.org/category/research-and-scholarship

[2] https://www.geant.org/Services/Trust_identity_and_security/eduGAIN

References

[AARC]	https://aarc-project.eu
[BPA]	https://aarc-project.eu/architecture/
[CORBEL]	http://www.corbel-project.eu/home.html
[CORDIS]	https://data.europa.eu/euodp/en/data/dataset/cordisH2020projects
[EIDAS]	https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[EOSCPILOT]	http://eoscpilot.eu/
[FIM4R-11]	https://indico.cern.ch/event/647693/
[GN4-1 D9.2]	https://www.geant.org/Projects/GEANT_Project_GN4-1/Documents/D9-2_Market-Analysis-for-Virtual-Organisation-Platform-as-a-Service.pdf
[Grouper]	https://www.internet2.edu/products-services/trust-identity/grouper/
[MOJEID]	https://www.mojeid.cz/
[OKTA]	https://www.okta.com/
[ONEGINI]	https://www.onegini.com/
[ORCID]	https://orcid.org/
[PAYPAL]	https://paypal.com
[Perun]	https://perun.cesnet.cz/web/references.shtml
[PINGIDENTITY]	https://www.pingidentity.com
[RA21]	https://ra21.org/
[SATOSA]	https://github.com/SUNET/SATOSA
[UMBRELAID]	https://www.umbrellaid.org/
[UNITEDID]	https://unitedid.org/
[WCAG]	https://www.w3.org/WAI/intro/wcag

Glossary

AAI	Authentication and Authorisation Infrastructure
BPA	Blueprint Architecture
HEXAA	Higher Education External Attribute Authorities
LDAP	Lightweight Directory Access Protocol
MMS	Membership Management Service
OIDC	OpenID Connect
SAML	Security Assertion Markup Language
SaToSa	SAML to SAML
SSH	Secure Shell
SP	Services Provider
VO	Virtual Organisation
VOPaaS	Virtual Organisation Platform as a Service