Technische Universiteit
Eindhoven
University of Technology

Education and Student Service Center

Den Dolech 2, 5612 AZ Eindhoven
P.O. Box 513, 5600 MB Eindhoven
The Netherlands
www.tue.nl

Author
Frank Vercoulen, Merete Badger, Lucio Monaco, Torsten Fransson, Laura Farinetti, Fulvio Corno

Date
28 October 2013

Version
1.0

Deliverable 5.4 - Virtual Campus Hub technical evaluation report

Virtual Campus Hub - Project nr 283747 - FP Infrastructures 2011-2

VIRTUAL CAMPUS HUB
Part of Explore Energy

SEVENTH FRAMEWORK PROGRAMME

DTU KTH TU/e

Where innovation starts

Technische Universiteit
Eindhoven
University of Technology

Table of contents

Title
Deliverable 5.4 - Virtual Campus Hub technical evaluation report

1 Introduction

The research infrastructure project Virtual Campus Hub (VCH) runs from October 1, 2011 to September 30, 2013. Four technical universities in Europe, who are all active in the field of sustainable energy, form the project consortium: the Technical University of Denmark, The Royal Institute of Technology in Sweden, Politecnico di Torino in Italy, and Eindhoven University of Technology in the Netherlands.

This report describes and discusses the technical achievements of the Virtual Campus Hub project and formulates a brief agenda for the future.

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7 2007-2013) under grant agreement no. 283746.

2 Concept and functionalities

The concept of Virtual Campus Hub (VCH) has been extensively dealt with in deliverables D5.1 & D5.2 – *Development concept and survey of available technology*, D3.1 – *Prototype implementation or e-learning tools and incubator processes*, and D6.7 – *The Virtual Campus Hub concept*. In this chapter, the VCH concept and functionalities will only be recapitulated briefly where needed for the technical evaluation.

2.1 Concept

A Virtual Campus Hub is a collection of functionalities and infrastructure services that enables seamless collaboration within *virtual organizations*, i.e. organizations that are formal or informal partnerships of two or more organizations and that therefore cross the borders of institutions, countries or communities (e.g. universtity-industry). As such, it stimulates the integration of education, research and innovation, which increasingly takes place through cross institutional, cross border and cross community *virtual organizations*.

In this project, the "proof of concept" of the Virtual Campus Hub is focused on four institutions (DTU, KTH, PoliTo and TU/e) that make some of their applications available to the other partners and to external participants, e.g. members of industry. This simulates, for example, the situation in which these four partners offer a joint master programme, part of which are joint activities where students or teachers need to access applications from partners. See figure 1 below for a graphical representation of the concept.

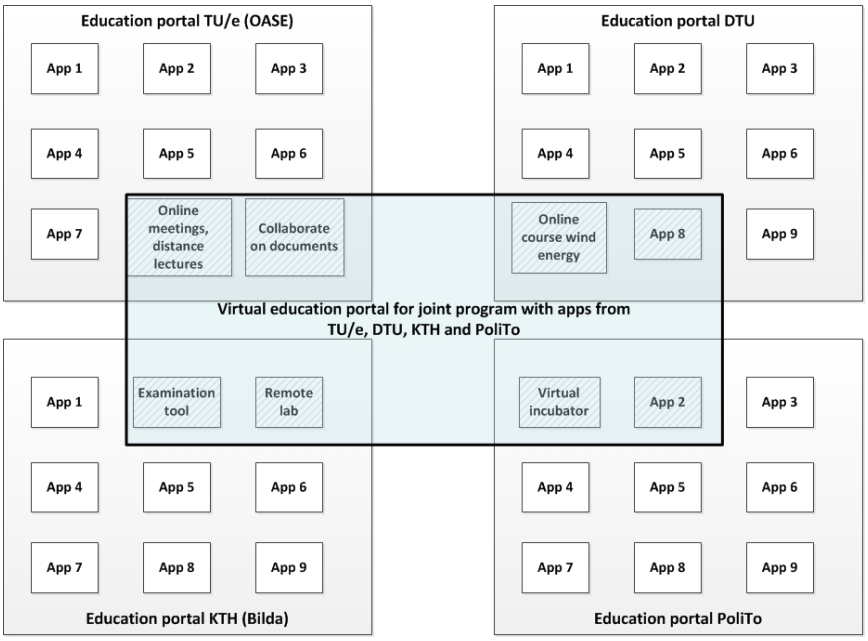

Figure 1. Concept for a virtual education portal for joint programs

As the picture shows, every institution has a well-working internal education portal, through which different applications are offered in a seamless and integrated way to students, teachers and other staff involved in education (see §2.6 for a brief discussion on current developments in this field). However, once these applications need to be shared with users outside the own institution (say users from a partner institution), providing seamless access becomes very difficult and time consuming, as

users need different (guest) accounts to access facilities, communication becomes cumbersome and information channels are not attuned to each other. In addition, the use of so many (guest) accounts may give rise to security issues. Therefore, the goal of the Virtual Campus Hub "proof of concept" is to show to what extent it is possible to create a virtual education portal for a joint programme, consisting of applications made available by the partners involved in that programme, and to which all relevant users have seamless access. Basically, what we have in mind is that in the future, such a virtual education portal should be as easily accessible and as well-integrated as the local education portals at institutions.

While the Virtual Campus Hub proof of concept is narrowly defined for practical purposes, its applicability is much wider, as the problems mentioned are common to all virtual organizations in education, research and innovation. In addition, the same problems are seen with other developments, such as increasing use of cloud services, virtual research environments (VREs) and the move from classical all-in-one learning management systems (LMS) towards "extended digital learning and working environments" (DLWEs) (see §2.6 for a brief discussion of these related developments).

2.2 End user functionalities

As discussed in the previous section, the idea behind the VCH concept is that the members of a virtual organization in education would be able to access and use applications as easily as members of the institutions involved are used to with their internal education portal. The most important of these end user functionalities are (see D5.2, D3.1 and D6.7 for more information):

1. ***Access to learning materials***: Access to online, interactive learning materials
2. ***Collaboration environment***: Collaborate on projects, share documents, etc. For students, lecturers, researchers and business contacts
3. ***Virtual conference room***: Virtual lectures, virtual conferences and virtual meetings (unified communications)
4. ***Virtual incubator***: Facilitating contacts between universities and businesses, simplify the search for experts, etc
5. ***Exchange of study program data***: For joint programs: retrieve a student's results from different partner universities, retrieve subject and scheduling information from different partners in order to present the information of the complete joint program in a coherent way
6. ***Virtual coffee house:*** Create a virtual community for students, lecturers and others who will only rarely be able to meet physically.

The Virtual Campus Hub proof of concept has dealt with functionalities 1-4. Functionalities 5-6 have only been dealt with conceptually (see D5.2), but have not been worked out further.

2.3 Infrastructure functionalities

To enable a virtual education portal in accordance with the VCH concept, a number of infrastructure functionalities are needed that "glue" the contributions from different partners together and enable seamless access (see D5.2 and D3.1 for a detailed overview). These functionalities are or could be provided by the Géant[1] infrastructure and the infrastructure of the National Research and Education Networks (NREN).

[1] http://www.geant.net

1. ***Federated authentication (cross border)***: Access to partners' applications or those of external service providers (SP) through the user's account at his home institution. Realized by connecting partner institutions as identity providers (accounts, IdPs) and service providers (applications, SPs) to their national NREN federations. IdPs and SPs are then made available to eduGAIN[2], so cross border access by partner IdPs and to partner SPs can be established. In addition, other IdPs could be added, e.g. to provide guest access or to enable collaboration with others, e.g. with industry. See figure 2 below for an overview of this federated authentication architecture.

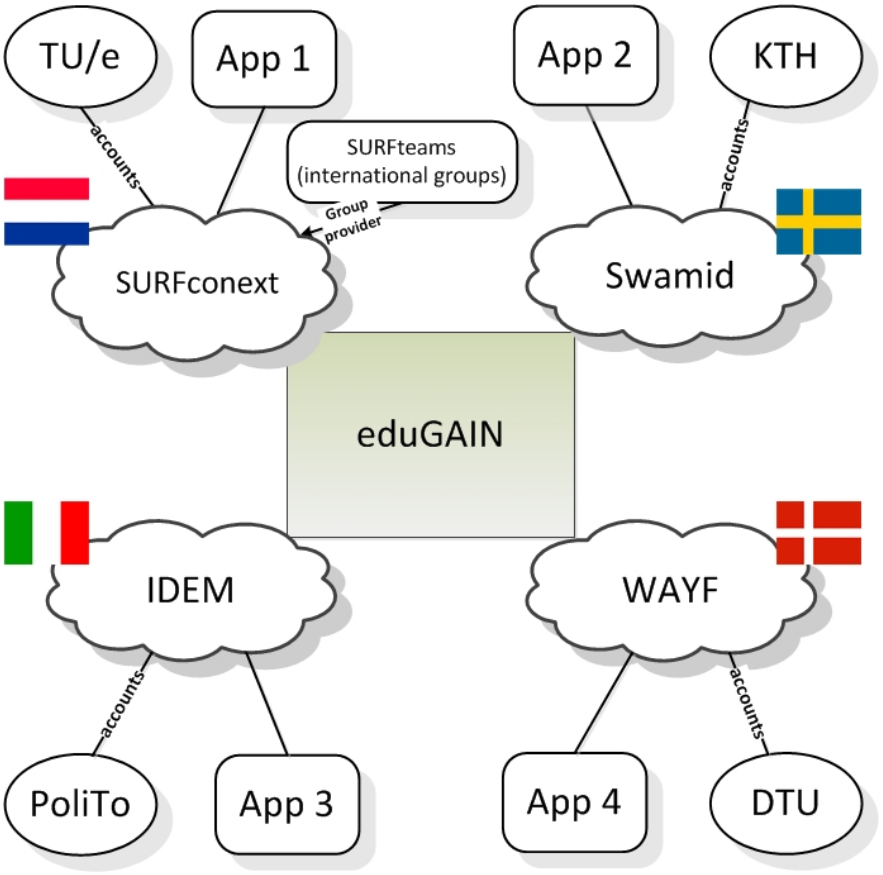

Figure 2 The VCH architecture with respect to federated authentication and group management

2. ***Group management***: Enables the creation of cross-institutional and cross border groups, which information can be used for authorizing access of groups to more than one application (SP) at once. An application has to be enabled for use of this external group information, but it enables scaling up a collaboration without having to register all users separately in all applications that are or will be part of the virtual education portal (or any other collaboration portal). This means the administrative load associated with user management can better be kept under control once a collaboration scales up. SURFteams via SURFconext[3] (SURFnet, NL, also available as open source via OpenConext[4]) and COmanage[5] (Internet2, US) are the best known examples of group management functionalities provided by NRENs[6]. See figure 2 above for its place in the VCH architecture.

[2] http://www.edugain.org
[3] http://www.surfnet.nl/en/Thema/coin/Pages/default.aspx, for detailed technical information on group management, see https://wiki.surfnet.nl/display/surfconextdev/Group+API+SURFconext
[4] http://www.openconext.org
[5] http://www.internet2.edu/comanage, see also http://www.terena.org/activities/vamp/ws2/slides/Heather.pptx
[6] Both are based on the Grouper application developed by Internet2: http://www.internet2.edu/grouper

3. ***Account linking / ID-mapping***: An infrastructure functionalitiy that is needed when access to applications or the retrieval of data from applications is related to a user's registration in a local administrative database. Think of the retrieval of a student's grades across different institutions (with the student having different ID's in each institution's administrative database or when a student needs to register for a course at a partner institution and this registration must be checked against all kinds of admission requirements (e.g. prior knowlegde, registration for a certain programme, etc.). Another example is a student that moves from one partner institution to another or to an industry partner that is involved in the collaboration and still needs access to resources. In these cases, there needs to be a mechanism to relate a user's different IDs from different institutions to each other. An example from research is the US initiative Orcid[7], which provides mobility of identities for researchers. There is also a Géant GN3+ project dealing with this[8].
4. ***Exchange of presence and calendaring information***: Infrastructure functionalities that are needed to efficiently organize and setup online meetings, remote lectures and the like (unified communications). This goes both for formally planned meetings and lectures and for ad hoc meetings. At present, setting up online meetings and lectures in cross-institutional and cross-border settings is time-consuming and cumbersome, as it is difficult for the organizer to obtain the information needed (availability, contact information, contact for technical support, etc.).
5. ***Exchange of audio and video across products/platforms***: Originally not foreseen (not present in D5.2 and D3.1 as a required infrastructure functionality), but has come up as a essential requirement for unified communications across borders (to realize the end user functionality for the virtual conference room), in addition to the functionality dealt with above (exchange of presence and calendaring information). Products/platforms differ greatly in their standards for audio and video and at the moment, new UC hub products are only partially able to bridge these differences.
6. ***Exchange mechanism for formal study program data***: An infrastructure functionality needed to retrieve or edit program data from the different partners' administrative databases, e.g. course and scheduling information for joint programs, grades, etc. Next to a technical exchange mechanism, you also need to agree on a (set of) functional standard(s), e.g. IMS[9] or RS3G[10]. In case of publicly available data (such as course information), no authentication and authorization mechanism is needed. However, with sensitive or personalized data, the exchange mechanism must also provide for (federated) authentication and authorization (group management). In most cases, also account linking / ID-mapping will be needed in order to be able to find the relevant data in the different administrative databases.

2.4 Presentation

As described in deliverables D.5.1-5.2 and D3.1, the original idea was to present the applications contributed by the different partners in a flexible portal environment with reusable components based on common standards[11]. The reason behind this is that institutions are usually involved in more than one collaboration at a time, so different portal setups will be needed. But they do not want to redo the same work for every collaboration they are involved in. In addition, it makes it easier to integrate an external cloud service in a collaboration portal (see also §2.6).

However, priority was given to getting the basic connections working, as the need to get seamless access is highest and integrated access through an advanced portal is only likely to become

[7] http://orcid.org
[8] GN3+ Subtask Account Linking in JRA3T2.
[9] http://www.imsglobal.org
[10] http://rs3g.sci.uma.es/drupal7
[11] In the case of VCH, the OpenSocial standard, initiated by Google, was chosen. However, at the time of writing, it is unclear if this standard will still be supported in the future. There are, however, other standards available as well, such as those for Java portlets.

important once collaboration with a virtual organization intensifies. See also the discussion in the last chapter (§5.6). For the VCH project therefore, the aim was to create a portal page with:

1. Single sign-on functionality
2. Links to all applications contributed by partners

2.5 End user, infrastructure and presentation functionality in this project

In this project, we have focused on the following four end user functionalities (see also deliverable D3.1):

1. ***Access to learning materials***: Access to online, interactive learning materials
    - (DTU) Online course on wind energy (itslearning)
    - (KTH) Remote cascade lab (web application)
    - (KTH) Continuous examination tools (KTH Bilda)
2. ***Collaboration environment***: Collaborate on projects, share documents, etc. For students, lecturers, researchers and business contacts
    - (TU/e) Collaboration environment (MS Sharepoint)
3. ***Virtual conference room***: Virtual lectures, virtual conferences and virtual meetings (unified communications)
    - (TU/e-SURFnet) Unified communications (hub)
4. ***Virtual incubator***: Facilitating contacts between universities and businesses, simplify the search for experts, etc
    - (PoliTo) StartApp (web application)

At the infrastructure side, three functionalities have been dealt with:

1. ***Federated authentication (cross border)****:* Using NREN federations and eduGAIN (see §2.3).
2. ***Group management****:* Via the SURFteams functionality from SURFnet (see §2.3).
3. ***Exchange of presence information:*** Via the local unified communications infrastructure at TU/e combined with a UC hub product (in this case a product that promises to fill some gaps in this respect). In practice, this also means the UC hub needs to provide an exchange mechanism for audio and video, as standards differ widely among UC products (see §2.3).

At the presentation side, two functionalities were used:

1. ***Single sign-on****:* Login once, then access VCH applications without logging in again.
2. ***Direct links to all VCH applications****:* Easy access to all applications from the VCH portal page

In the table below, the scope of the VCH proof of concept is shown with an overview of end user functionalities provided in this project and the corresponding infrastructure functionalities that have been dealt with. The column "*Planned for VCH portal"* shows which functionalities were initially intended to be part of the VCH portal (see ch. 3 for what has been realized and what not).

End user functionality	**Application**	**Infrastructure functionality**	**Planned for VCH portal**
Access to learning materials	DTU Online course on wind energy	Federated authentication Group management (partly)	Y Y
	KTH Remote labs	Federated authentication	Y
	KTH Continuous examination tools	-	N
Collaboration environment	TUE Collaboration environment	Federated authentication Group management	Y Y
Virtual conference room	TUE unified communications hub	Exchange of presence information Exchange of audio and video across platforms	N N
Virtual incubator (Start-up Pre-incubation Support)	PoliTo StartApp	-	Y
Portal	TUE web site	Federated authentication	Y

2.6 Related developments

It is useful to mention three other technological developments that we have not dealt with directly in the VCH project, but which are so closely related to the VCH approach, that the results from this project are also relevant in the context of these developments:

1. ***Increased use of cloud services:*** An increasing number of service providers offers its services through the cloud, meaning that an institution does not need to maintain and host the application on its own servers anymore. The servers are located elsewhere and only a connection via the internet between the institution and the service provider is needed. Increasingly, NRENs serve as brokers between HE institutions and cloud service providers, both with respect to purchasing and contract management and with respect to realizing the necessary technical connections. For example, in the Netherlands, SURFnet has made deals for the Dutch HE community with a large number of cloud service providers and realized the technical connections through its federation SURFconext.[12] As this is the same platform as was used for VCH, and as also SURFnet may make use of eduGAIN in the future to provide services from international service providers or to international customers – in fact, the cloud service itslearning was connected to the VCH proof of concept via SURFconext and thus provided to DTU – the relevance of VCH for cloud service provision across higher education in Europe is clear.
2. ***Virtual Research Environments (VRE):*** Next to providing collaboration facilities to virtual organizations in research, which problems and solutions are comparable to what has been done in VCH, an increasing number of facilities essential for researchers is only available as external service. Think of the specialized, extensive research databases, better known as "Big Data" to which researchers in turn may contribute with their own research data. To make effective use of these facilities, it is essential for institutions to connect to these research infrastructures, which is usually done through the federated identity management facilities

[12] For a list of cloud service providers currently connected through SURFconext, see http://www.surfnet.nl/en/Thema/coin/cloudservices/Pages/default.aspx

provided by NRENs (federations, Géant-eduGAIN). Again, therefore, many of the problems and solutions investigated in VCH also hold for the research community (and vice versa).

3. ***Extended education portal**:* As the use of cloud services increases and connecting to them in a seamless way, e.g. through NREN federations, becomes easier (see above), increasingly the question arises what the future of the education portals at institutions will be. At present, these portals usually consist of an all-in-one learning management system (LMS), a student information system (SIS) and some applications around these central building blocks, all hosted internally by the institution itself and difficult to access by external participants in education. The rise of cloud services and the potential of the VCH concept – making applications available to others outside the own institution – threaten to turn this model of the education portal upside down and replace it by what a recent report by SURF in the Netherlands has called the "extended education portal"[13]: a collection of internal and external services, which are glued together through the NRENs' infrastructure for federated identity management. For example, this could mean that present all-in-one LMSs are replaced in the future by a more dynamic and flexible collection of internal and external applications, which can better be adapted to local needs and changes in pedagogy, while still being more efficient and cost-effective than the present all-in-one solutions. In addition, this "extended education portal" would in principle be much better accessible by outsiders, as the underlying technological platform is the same as the one on which the Virtual Campus Hub is based (NREN federations, Géant-eduGAIN).

[13] For the SURF report on the extended education portal, see http://www.surf.nl/en/publicaties/Pages/DevelopmentsDLWE.aspx

3 Achievements

In this chapter, an overview is given of the functionalities realized (end user, infrastructure and presentation functionalities). Also the choices made during realization are discussed, as well as some of the implications of these choices and the gaps identified.

3.1 Identity providers (IdPs)

Identity providers connected
At this moment, the following IdPs have been connected to the Virtual Campus Hub (see also picture below):

1. Eindhoven University of Technology (TU/e)
2. Royal Institute of Technology, Stockholm (KTH)
3. Technical University of Denmark (DTU) through WAYF (DK)
4. FEIDE OpenIdp (NO) for guest accounts
5. OneGini for access through social network accounts (Google, Facebook, Twitter and LinkedIn)
6. SURFguest (NL) for guest accounts
7. SURFnet (NL) for testing purposes
8. GARR (IT) for testing purposes

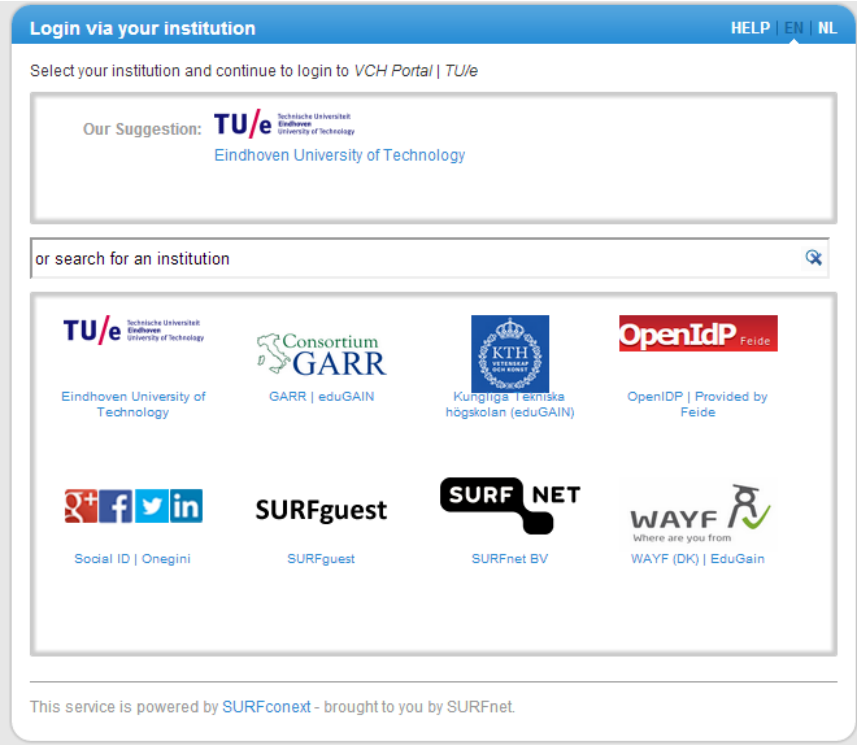

Figure 3. The logon screen where the federated user needs to select his IdP

For these IdPs to be available to the Virtual Campus Hub, the metadata for all these IdPs needed to be published to eduGAIN. As a result, any service (application) connected to a federation that is member of eduGAIN is able to pick up these metadata and thus to connect one of these IdPs to their service (mutual agreement is needed as well, of course).

Choices made, implications and gaps identified

Connecting an identity provider (IdP) is the responsibility of the organization that wishes to make its user identities available to external services in order for their users to be able to access these external services. When using federated identity management provided by the NREN federations and Géant-eduGAIN, this IdP will be connected to its national NREN federation, which will in turn this IdP's metadata to eduGAIN in order for this IdP to be available for service providers in other countries. In these other countries, the connection between IdP and the service provider (application) is also mediated through the NREN federation. So an international link between IdP and SP consists of the connection IdP <-> NREN federation 1<-> eduGAIN <->NREN federation 2 <-> SP.

For Virtual Campus Hub, the IdPs from the partners involved and others needed to be connected to their national NREN federation (SURFconext NL, Swamid SE, WAYF DK and IDEM IT) and subsequently be made available to eduGAIN and to the different VCH services (applications), among them the VCH portal. Below, an overview of the IdPs that we intended to connect, the results and the problems encountered:

1. **TU/e IdP**: No problems occurred. The TU/e IdP was already connected to SURFconext (NL) before the start and SURFnet has made the IdP metadata available to eduGAIN without problems (after formal agreement from TU/e that this could be done). Also making this IdP available to the applications connected (VCH portal at TU/e, DTU itslearning and TU/e MS Sharepoint) was no problem, also because in the end, all VCH services were connected through SURFconext (see next section).
2. **DTU IdP**: The DTU IdP had already been successfully connected to WAYF (DK) before the project. Making it available to eduGAIN turned out to be no problem after WAYF joined eduGAIN end of 2012 (also because no agreement from DTU was needed, as WAYF uses an opt-out policy; this means that all Danish IdPs are made available to eduGAIN unless they explicitly say they don't want to be in eduGAIN). However, making the DTU IdP available to the services (which were connected via SURFconext) was more problematic, because it was unclear which kind of attributes were needed and how the values of these attributes should be defined. WAYF and SURFconext have worked this out together and the problem was solved fairly quickly. However, it also showed that the present process for updating metadata to eduGAIN is fairly time-consuming, so simple changes took more time than expected. As a result, users from DTU were also able to use their own DTU accounts for their own DTU itslearning application, where before the VCH project needed separate accounts from itslearning to access this application.
3. **KTH IdP**: The KTH IdP had already been successfully connected to Swamid (SE) before the project and making it available to eduGAIN was no problem. However, when making it available to the services connected via SURFconext, the KTH IdP and SURFconext turned out to be incompatible, as they were using different versions of SAML[14]. As a result, SURFconext was unable to support the encryption required by the KTH IdP. To solve this issue, SURFnet built a proxy to circumvent this problem, after which the KTH IdP was available for the VCH services. This problem was the main reason that the connection of the KTH IdP to the VCH services was considerably delayed (until September 2013). It also took some time before the cause of the problem was found, as it was unclear if this was a problem at KTH or at the federations involved (Swamid, SURFconext) and coordinating all the parties involved was not easy.
1. **PoliTo IdP**: PoliTo has made a strategic decision to focus on the STORK eID[15]. As a result, the PoliTo IdP has not been connected to IDEM (IT) and therefore also not to eduGAIN and the VCH services. However, there are some initiatives to connect STORK eID to eduGAIN and STORK and eduGAIN have planned a technical proof of concept for the connections eID-

[14] Security Assertion Markup Language, the protocol through which the single sign-on features are realized. See http://saml.xml.org/saml-specifications for its specification and https://blog.surfnet.nl/?p=1417 for an explanation.
[15] STORK is the European initiative to establish an European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. See https://www.eid-stork.eu.

eduGAIN to be delivered in the 2nd half of 2014.[16] To show that a connection with Italy via eduGAIN can be established, GARR (IT) has been made available as IdP to the VCH services through eduGAIN.

2. **Industry IdPs**: No industry IdPs (i.e. IdPs from companies involved in activities of VCH) have been connected to VCH. First of all, this is due to the fact that this possibility does not exist yet within the Géant infrastructure (federations do not allow industry to connect to the public Géant infrastructure as IdP), except for a few pilots (e.g. the pilot of SURFconext with the public-private partnership NBIC-CTMM[17]). Second, the pilot from SURFconext just mentioned showed that setting up an industry IdP and use it for a public-private collaboration is a project in itself because of its complexity; as such, it is out of scope for this project. But see the discussion of this issue in the last chapter (Ch.5: Agenda for the future).
3. **Guest IdPs**: To provide access to other users than those of the project partners and to those whose IdP has not been connected to VCH, 3 guest IdPs have been connected:
    - *FEIDE OpenIdP* (NO)[18]: This is a guest IdP provided by the Norwegian federation FEIDE and which anybody can use. In addition, it is available in eduGAIN and SURFnet has made it available to the VCH services through SURFconext. Its advantage is that its procedure for creating guest accounts is all in English.
    - *OneGini (NL)*[19]: An OpenSocial IdP that makes it possible for users to use their account from Facebook, Google, Twitter or LinkedIn to access the VCH services.
    - *SURFguest (NL)*: A service for guest accounts provided by SURFnet, but the service is mostly in Dutch, which makes it not very useful for VCH users.
4. **Other IdPs**: SURFnet (NL, SURFnet employees) and GARR (IT, GARR employees) have been made available as IdPs to eduGAIN and the VCH services for testing purposes.

[16] Oral communication with the people from eduGAIN present at TERENA VAMP 2013, Helsinki.
[17] See for more information http://www.surfnet.nl/en/Thema/coin/indepraktijk/Pages/Default.aspx and http://www.surfnet.nl/en/Thema/coin/indepraktijk/Pages/PilotNBIC,CTMMandNLeSC.aspx
[18] https://openidp.feide.no
[19] https://www.onegini.me

3.2 Service providers / applications (SPs)

In this section the core applications from the VCH partners that have been connected to VCH and those that had originally been planned to be connected are discussed. The group management functionality and the portal, which are also services from a technical point of view, are there to support the core applications.

3.2.1 DTU Post educational course on wind energy

To offer the post educational course on wind energy, DTU bought a license for itslearning[20], a learning platform that is offered as a cloud service (with its servers located in Norway). At first, all users obtained a separate itslearning account to access the system.

Problems identified
To connect the DTU itslearning service to VCH, following the architecture proposed in figure 2 (§2.3), the idea was to connect DTU itslearning to WAYF (DK) and subsequently make it available to eduGAIN in order for the VCH IdPs to connect to it. However, four kinds of problems came up:

1. *WAYF (DK) was not part of eduGAIN yet:* This has been solved by WAYF becoming member of eduGAIN at the end of 2012.
2. *Itslearning DK was a reseller with little technical knowlegde on the VCH architecture*: This led to itslearning DK being very reluctant to participate. Therefore, itslearning passed the request on to the Dutch branch of itslearning, which had already been connected to the Dutch federation (SURFconext) and thus knew how to connect to the VCH infrastructure. It was decided that DTU itslearning would be connected to VCH through SURFconext and, if successful, the connection would be migrated to WAYF (DK).
3. *Different parties that had not been involved at an early stage were needed to help realize the connections:* As DTU Department of Wind Energy had bought itslearning externally where DTU as a whole uses another learning platform, and as DTU would have to to build up a lot of knowlegde on federated identity management first, they could not be involved to help work out the technology to get itslearning connected. In addition, DTU itslearning is an external cloud service, which means most of the work had to be done by itslearning anyway.
4. *Confusion about the best way to connect as federations' architectures differ:* During the phase which led to the involvement of itslearning NL for realizing the connection, confusion arose among the different technicians involved (from federations, the chief architect of itslearning in Norway and the specialist from itslearning NL) on how a connection to a federation could be realized. It turned out that federations have different architectures: some use a so-called hub-and-spoke architecture (SURFconext, WAYF), others use a so-called mesh architecture (SWAMID), which has consequences for the way the connection is established. Itslearning is not able to connect to a mesh architecture, it concluded, but is able to connect to a hub-and-spoke federation. In the end, the conclusion was therefore that itslearning could be connected to VCH through either SURFconext or WAYF.

Solutions implemented
As a result, itslearning NL and SURFnet were involved to first realize a connection between itslearning and SURFconext and coordination was temporarily moved from DTU to TU/e. At first, a test environment was set up and once this was successfully connected to SURFconext and eduGAIN, this configuration was incorporated in DTU's itslearning site in the itslearning production environment.
The result was that:

[20] http://www.itslearning.com

1. DTU users could login to the DTU wind energy course with their own DTU account where before they had to use a separate itslearning account (they are still able to use their itslearning account as well if they prefer).
2. Users from the other IdPs that had been made available to eduGAIN and to this VCH service (itslearning) could login to the DTU site with their own account.

To enable users to use the federated logon, the configuration added an extra attribute[21], to the itslearning account, which identifies the user as a federated user and enables him to login through his own institution with his own account.

As the itslearning application was not enabled for external group management (see §3.2.6) and no automatic mechanism for user provisioning was implemented, due to the fact that getting the federated logon working was taking all the time and resources available, all federated users needed to be registered in itslearning first before they were able to access the service (cf. the TU/e MS Sharepoint environment in §3.2.3, where this is not needed). At the federation level (SURFconext), a filter was implemented to only enable federated access to the DTU itslearning service for the members of the so-called Virtual Campus Hub group (see §3.2.6 on group management). But this filter is not really needed, as at this moment only users that have explicitly been registered as federated users – through the extra attribute mentioned – are able to access the itslearning service. The filter will therefore be removed when migrating the connection from SURFconext to WAYF.

Migration of itslearning connection from SURFconext to WAYF
The final phase, migration of the connection from SURFconext to WAYF, was meant to bring the connection of DTU itslearning in accordance with the architecture planned in the beginning (see figure 2, §2.3). However, two problems have prevented this from happening, one of them has been solved in the meantime, the other is still waiting to be solved:

1. *The federation architecture of SURFconext and WAYF differ*: WAYF does not have a so-called service proxy to easily connect a service to different IdPs, the result of which is that the connection of itslearning to WAYF is more complicated than to SURFconext. Itslearning has come up with a solution for this, so this problem is solved.
2. *WAYF is not able to update service metadata to eduGAIN yet*: This means WAYF is not able to connect services (applications) through WAYF to eduGAIN yet. It plans to enable this, but when WAYF will be able to do so is not known yet.

As a result, it is not possible at the moment to migrate the connection of itslearning from SURFconext to WAYF without losing the connection to eduGAIN. Maintaining the connection as it is is also no option, because SURFconext would have to ask a fee to maintain the connection for members outside the (Dutch) SURFnet community. In addition, moving DTU as customer from itslearning DK to itslearning NL is also no option, as itslearning NL would not be able to offer the full range of support services to DTU that are part of the contract, next to providing the technical connection to SURFconext-eduGAIN.

Therefore it was decided that the connection with SURFconext will remain in place until the VCH pilot has ended, after which itslearning will establish a regular federated logon connection between DTU (as IdP) and their itslearning DK service through WAYF, without the connection to eduGAIN. This enables DTU to keep using their own DTU accounts to login to the wind energy course after the VCH project has ended. Once WAYF is ready to connect services to eduGAIN, the connection of DTU itslearning to eduGAIN will be reestablished.

[21] The added attribute is eduPersonPrincipleName (ePPN), see https://wiki.surfnet.nl/x/bQEWAg#AttributesinSURFconext-Principlename and http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#eduPersonPrincipalName. In case of SURFconext, ePPN = userID@institution, e.g. username@dtu.dk.

3.2.2 KTH Remote labs

KTH has developed a number of remote laboratories (three as part of the VCH project) that allow users to carry out experiments on distance having access to real laboratory equipment. In VCH focus has been also on enabling cross-institutional use of the labs through their integration in the VC Hub technology.

Problems identified and solutions implemented

The existing remote labs at KTH were self-standing applications[22] without any sort of authentication and authorization mechanism. At first, KTH investigated the possibility of implementing the labs in an existing learning platform, including CompEdu (KTH), Moodle[23] and Bilda (KTH), that could then be connected to VCH. The conclusion was that this was not possible or at least too complicated to be of use since:

- CompEdu is a content platform missing most of the functionalities required to a remote lab such as scheduling tool, assessment tool, student tracking;
- There was no Moodle instance installed at KTH and additional plugins had to be developed for supporting the labs;
- Reluctance of KTH to make modifications to the Bilda system considered to be working with a philosophy (especially regarding user groups) different from the one proposed in the VC Hub.

The decision was therefore made to develop a separate and simple web application that handles only authentication and authorization for the access to the GUI for the control of the labs[24]. With respect to connecting the web application to VCH, two main problems occurred:

1. *People with knowledge on how to connect the application were hard to find, both internally and externally:* KTH had to build up knowlegde on this and it was hard to get the different parties, that had not been involved at an early stage, on board (June 2012, September 2012). In the end, SWAMID, the Swedish federation, helped to set up servers and making basic connections, developing and implementing also a dedicated IdP discovery service. KTH tried to overcome the lack of internal human resources looking for external companies that were able and willing to connect the remote cascade labs application to VCH (May 2013), but was unsuccessful in this attempt. In the end, SWAMID served as knowledge broker to bring KTH into contact with the IT department at Karolinska Institutet (September 2013), who had done something comparable with library services. Discussion is presently ongoing on whether the group could work on the application and how this would be done after the project end.
2. *At first, the cause of connection problems, local at KTH or at federation level, was difficult to determine:* Therefore, it took a while before KTH understood they were not able to realize the connection themselves.

As a result, the remote cascade labs has have not been connected as a service (SP) to VCH yet Absence of restricted access allows for cross-institutional use of the labs[25] but represents a considerable limitation to the VCH philosophy.

[22] The graphical user interfaces (GUIs) are based on the LabSocket system, http://www.labsocket.com. The application is written in php and it is running on Apache web server hosted at KTH.
[23] http://moodle.org
[24] KTH tried to implement an authentication mechanism on the server as well as to modify the application itself.
[25] http://www.energy.kth.se/proj/projects/Remote_labs/RL/RL_website/Home.html

3.2.3 TU/e collaboration environment (MS Sharepoint)

In order to provide a collaboration environment which enables members of partners to share files and to collaborate on projects, TU/e setup a MS Sharepoint site, which was to be connected to the Virtual Campus Hub infrastructure.

Problems identified
Manuals for connecting MS Sharepoint to the VCH infrastructure and to enable it for external group management (see §3.2.6) were available from SURFnet[26]. However, the following problems came up:

1. *Different parties that had not been involved at an early stage were needed to realize the connections:* It took much time, therefore, to get all parties aligned and on board.
2. *As federated identity management is new to TU/e, a lot of knowlegde had to be built up to get the connections working:* The SURFnet manuals were followed and the people from SURFnet offered support, but when problems occurred that were not discussed in the manuals, TU/e was unable to solve them. In addition, also some errors in the manuals were found, especially with respect to applying the configuration described to the situation at TU/e.
3. *The existing ADFS configuration could not be used to enable both TU/e's IdP and its services (SP):* Due to a bug in SURFconext, an extra ADFS server was needed to enable the connection of the TU/e services (MS Sharepoint, VCH portal) to SURFconext. This bug will be fixed, but not in the short term.

Solutions implemented
Internal deliberations at TU/e led to a solution such that the IT department would be able to realize the connection with the VCH infrastructure, following the SURFnet manuals. At first, however, TU/e could not get the connections working properly, including the connection with group management (see §3.2.6), so SURFnet served as a knowledge broker by providing an external consultant with experience in the field, who successfully helped TU/e to get a working configuration. The bug in SURFconext with respect to ADFS server was dealt with by adding an extra server to connect the VCH services provided by TU/e to SURFconext. The connected MS Sharepoint site was then used as the project team site.

3.2.4 Unified communications hub (TU/e-SURFnet)

In order to provide a seamless communications experience across the partner institutions, and therefore also across borders, TU/e and SURFnet worked out a pilot that could have shown how this could be realized. Unified communications within an organization is relatively easy to achieve, but connecting different communication products in use at different partners with each other is very difficult. It was, however, identified as being the second biggest barrier for international collaboration (after getting seamless access to resources). Before dealing with the pilot setup itself, the terms unified communications (UC) and unified communicatons hub (UC hub) will be briefly explained.

What is unified communications?
Basically, unified communications stands for the combination of the available means of communication into an integrated whole. It therefore would provide most of the following list of functionalities:

- Online meetings (voice, video, chat, desktop sharing): Plan and setup meetings
- Integration with traditional telephony (POTS[27]): Call to and be called from traditional phone numbers

[26] Connecting MS Sharepoint: https://wiki.surfnetlabs.nl/download/attachments/22413486/SURFconext+for+SharePoint+2010+Setup+guide+version+2.pdf , Group management plugin for MS Sharepoint: https://wiki.surfnetlabs.nl/display/surfconextdev/Microsoft+SharePoint+as+a+group+consumer

- Presence (online availability): Is someone available, busy, out of office, etc
- Single sign-on (use your institution's account to access all functionalities): No separate accounts and integration with the institution's authentication infrastructure. For VCH: integration with the infrastructure for federated identity management.
- Integration with traditional videoconference (H.323): Institutions have a large installed base of (expensive) high quality equipment for videoconferencing, e.g. for remote lectures and meetings. This is unlikely to be replaced in the short term with equipment for desktopconferencing (via PC or alike).
- Any device (can be accessed through PC, (smart)phone, etc)
- Calendaring (general availability): Sharing calendar information among users

For Virtual Campus Hub, this would mean that the members of a virtual organization (VO) with partners in different countries would be able to communicate as easily with the other members of the VO as with the members of their own institution (depending on the status of the local facilities, of course). And that implies that people would be able to keep using their own tools, which have been tested thoroughly, for which technical support is available and which have been integrated with the own institution's infrastructure.

What is a unified communications hub?
As crossing an institution's border through unified communications is far from self-evident, as different organizations use different products that use different standards for audio, video, presence, calendaring, authentication etc, a (still relatively small) market for bridging products has emerged. None of the products is able (yet) to provide bridges on all the aspects of unified communications mentioned above and per aspect, to bridge all standards used by the different products, but it is a start. SURFnet made an analysis on the products available that might be used in a VCH setting.[28] Some of them focus on bridging audio and video (traditional videoconference with desktop platforms or between different desktop platforms), others on bridging different desktop conferencing products (Skype, Google Hangouts, Adobe Connect, MS Lync, Cisco Jabber, IBM Sametime etc), and some try to do both.

The available infrastructure at TU/e and at partners
TU/e is migrating to MS Lync as its main communication platform, and has integrated this with its traditional phone exchange (eventually to be phased out) and with the rest of its Microsoft products (MS Exchange, MS Sharepoint). In addition, its Lync environment is configured as a so-called open (Lync) federation, which means that any external user with Lync is able to setup an online meeting with any TU/e user and vice versa. Finally, TU/e has a Polycom RMX videoconferene server (virtual rooms) at its disposal to which traditional videoconference sets can connect, but which also has a bridging component for MS Lync (e.g. to enable participation in remote lectures of people on the move).

At the other partners' premises, different tools are used for online meetings. In the Nordic countries, Adobe Connect is widely used, for which federated logon across the Nordic countries is provided through the Kalmar2 inter-federation[29]. At KTH, a conference room has been set up by KTH itself (KTH Multisal) that offers audio and video bridges with several products such as Skype, Adobe Connect, traditional videoconference etc. At PoliTo, Big Blue Button is used for online meetings, an open source product that also has been connected to the Dutch federation SURFconext by SURFnet (not as part of the VCH project, though)[30]. And all also make use of traditional videoconferencing,

[27] POTS: Plain Old Telephony Service
[28] Examples of products with a focus on bridging audio and video are Bluejeans (http://bluejeans.com) and Polycom CloudAxis (http://www.polycom.com/products-services/realpresence-platform/cloudaxis.html). An example of a product bridging desktop conferencing (presence, chat, desktop sharing etc) is Nextplane (http://nextplane.net). And an example of a product that offers both (although through different products) is Vidyo (http://www.vidyo.com/solutions/unified-communications, http://www.vidyo.com/products/vidyogateway and see also the CERN website at http://information-technology.web.cern.ch/services/fe/vidyo).
[29] http://www.kalmar2.org
[30] http://www.surfnet.nl/en/Thema/coin/cloudservices/Pages/Default.aspx

often including a videoconference server (virtual room, MCU). Of course, many other products, that are not officially part of the internal IT infrastructure, are used by many people as well (e.g. Skype).

The (intended) pilot
As there is no obvious general solution available yet, the idea for the pilot was to take the TU/e infrastructure as a starting point and to try to fill the gaps with respect to involving members of the other partners (DTU, KTH, PoliTo) in online activities, thereby sticking to the principle that everybody should be able as much as possible to keep using their own local tools. As most online activities are mainly about audio and video, including sharing of some content (e.g. a presentation), it was decided that the focus would lie on the exchange of audio and video and less on “desktop conferencing facilities”, such as presence, chat, etc.

The second idea was to focus on solutions that SURFnet eventually would be able to connect as a cloud service through SURFconext, thus also enabling its integration with the Virtual Campus Hub infrastructure. As a result, one of the main requirements towards vendors was that they would be able to connect to SURFconext during the pilot or soon afterwards.

To see which kind of solutions would be useful for a pilot with cross border unified communications, the main gaps in TU/e’s infrastructure were identified:

1. The Lync version presently in use at TU/e (Lync 2010) is not very good at involving guest users in conferences (the plugin needed is not very reliable). The latest version of Lync (Lync 2013) is supposed to have solved this problem, but as this version is not in use at TU/e yet, this remained an important gap for the pilot.
2. The bridging component in use between the Polycom RMX videoconference server and MS Lync is not very good at sending content (e.g. presentations) between the two platforms. Investment in a better bridging component would be needed to solve this issue.
3. (Lync) federated users are not able to participate in TU/e videoconferences yet. This is due to the configuration of the so-called MS Lync Edge servers. This configuration can be changed, but requires an extra investment.

On this basis, SURFnet started contacting vendors, but only got a positive response from Polycom and, eventually, from Vidyo. As Polycom was most eager to participate in a pilot, the decision was taken to choose Polycom and later, if time and budget allowed, to do another pilot with Vidyo.

The unified communications platform of Polycom is CloudAxis, which uses the RMX servers and its RealPresence platform as its basis and adds functionality for sending invitations, importing and using contacts from different platforms (such as Skype, Google, Facebook etc) and basic chat during sessions. In addition it enables access through any device and connection with MS Lync (via the RMX-Lync bridge). So in essence, it is a separate platform, which can make use of existing resources (RMX) and of existing bridges (RMX-Lync), but does not really connect video streams from one platform (e.g. Cisco) with that of another (e.g. Microsoft). The hub function mainly takes place at the contact level, as users get an invitation through their own platform (Skype, Google, Facebook), click a link and then enter a session on the Polycom RealPresence platform. Only a MS Lync client can directly access a RealPresence session. So CloudAxis covers some aspects of a unified communications hub, but by far not all of them.

First, a pilot was done with the Polycom CloudAxis demo platform during the KIC InnoEnergy Select MSc project of the year event in Eindhoven in May 2013. As this was a demo platform, there were only limited possibilities to solve problems and capacity was limited, so a number of technical problems occurred. Therefore, an agreement was made to setup a pilot environment at TU/e, with the CloudAxis platform tightly integrated with the existing RMX and Lync infrastructure; this was to be done by one of the Polycom partners in the Netherlands. In addition, Polycom, with support from SURFnet, investigated the possibilities to support SAML-2, the protocol that is needed to connect an

application to SURFconext and thus to the VCH infrastructure. In the end, however, the pilot did not take place, because of the cost involved for the Polycom partner and because of changed priorities at Polycom.

3.2.5 PoliTo Start-Up Pre-Incubation Support (StartApp)

PoliTo has developed a web application, the StartApp tool, together with I3P, the incubator for the region Piemonte Valle d'Aosta, in order to support the incubator processes. As the users of this application are mostly from outside the university, connecting the StartApp tool to the VCH infrastructure was seen as of little added value (see also §4.2). In addition, PoliTo is not part of IDEM, the Italian federation, a connection that is needed to connect to the VCH infrastructure. Therefore, PoliTo's contribution as a service provider is not discussed further in this deliverable. For more information, see deliverable *D4.3 e-Link evaluation report*.

3.2.6 Group management (SURFnet)

For group management, the SURFteams application provided by SURFnet and part of its federation SURFconext was used (see also §2.5). With this service, groups can be created with members from different IdPs (in fact, with members from all IdPs connected to this service). Subsequently, other services can use this information to provide access to these groups. For VCH, only the TU/e collaboration environment (MS Sharepoint) was enabled for group management. For the DTU course on wind energy (itslearning), the group information was used to filter federated access to itslearning at the application level (see below).

As this group management service (SURFnet) is a general production service offered to all higher education institutions in the Netherlands (as part of the SURFconext service), there were no connection problems. Only the relevant IdPs had to made available to this service, like to the other VCH services. This went without problems.

Creating and managing groups
For VCH, only the so-called *ad hoc* group functionality was used. An *ad hoc* group is a relatively small group that is created by invitation. For bigger groups that need to work together structurally (*virtual organizations)*, the different IdPs can also provide internal group information to SURFteams (e.g. all students following a certain programme within the institution) after which these internal groups can be combined at SURFteams level to one group (e.g. all students following a certain programme at all partner universities involved). For a discussion of the latter, see §5.1.

Once a group is created in SURFteams, members are invited by email. By clicking a link in the email or by going directly to the SURFteams application in the VCH portal (*My virtual campus group memberships*), a user then decides through which IdP he will become member of this group. That is done by loggin on to this IdP (so the user must have a valid account at this IdP) and then accept the invitation (or decline it). Once accepted, his membership of the group can be used to provide direct access to applications. For the VCH proof of concept, one ad hoc group, Virtual Campus Hub, was created.

Connection to the TU/e collaboration environment (MS Sharepoint)
To enable external group management through SURFteams for the collaboration environment, a plugin for MS Sharepoint was installed.[31] With this plugin, in combination with the configuration of MS Sharepoint to enable it for federated identity management, it was not necessary anymore to create

[31] Group management plugin for MS Sharepoint: https://wiki.surfnetlabs.nl/display/surfconextdev/Microsoft+SharePoint+as+a+group+consumer

(federated) accounts separately in Sharepoint. The federated accounts which are member of the VCH group could directly be read into Sharepoint without any extra administration (see figure 4 below). However, with this plugin, the list needs to be refreshed by hand every time group membership changes. On the other hand, it is also possible to make a selection of group members to give them access.

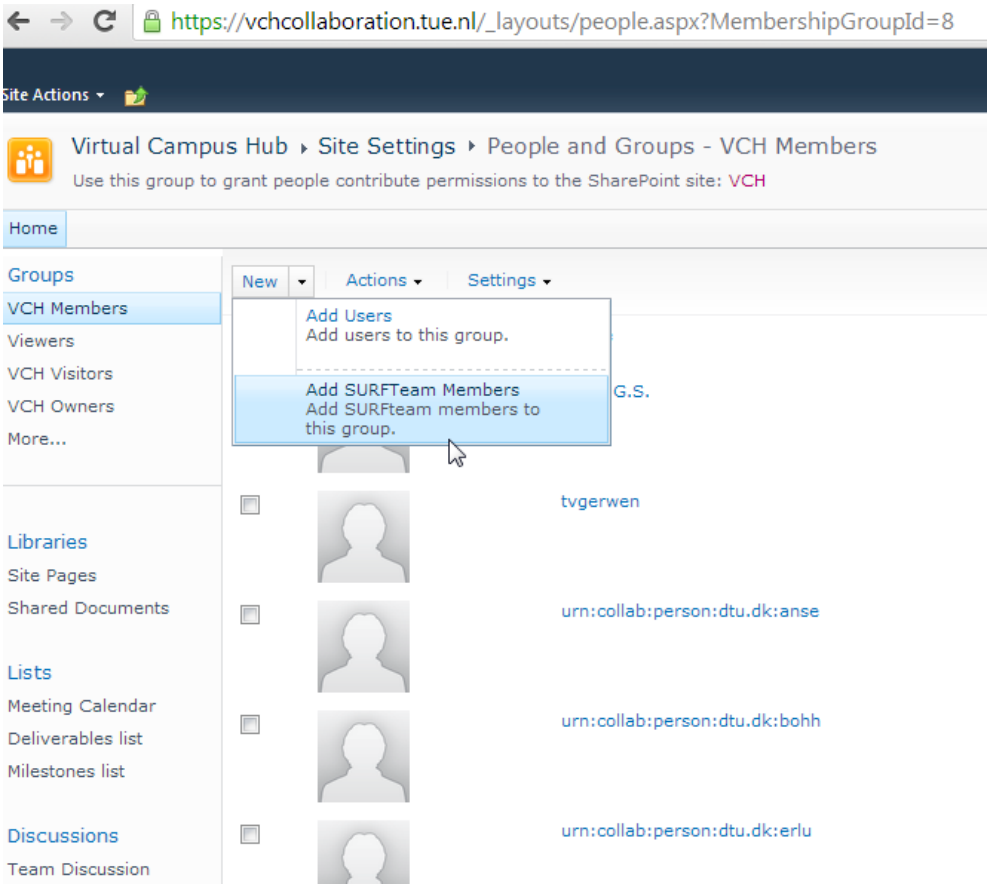

Figure 4. Providing access to federated users via SURFteams

The plugin proved stable and reliable during the project and no technical problems occurred. Only during setup it proved necessary to configure it such that in MS Sharepoint the federated users in the list were presented with somewhat readable names (see figure 4). The externa consultant provided by SURFnet helped TU/e realize this change.

Connection to DTU course on wind energy (itslearning)

DTU itslearning was not enabled for external group management, as all of the time available had to be spent on getting the federated login working (see §3.2.1). However, it was discussed that the IMS-LTI specification[32] might be a way to connect itslearning with SURFteams and thus enable it for external group management. In the Netherlands, the same specification has been used to enable SURFteams for other learning platforms, notably Sakai.[33]

The group information was used to filter access to DTU itslearning, meaning that only the federated users that are member of the SURFteam Virtual Campus Hub were allowed to access the application. However, this was not of added value, as all federated users had to be entered separately into the itslearning system as well to let them access the application (contrary to the TU/e collaboration environment, where this was not needed), so eventually this filter was removed.

[32] For more information on IMS-LTI, see http://www.imsglobal.org/lti.
[33] http://www.sakaiproject.org

3.2.7 Portal (TU/e)

The Virtual Campus Hub portal (https://vch.tue.nl) is a simple website (.NET, IIS) with (single sign-on) deeplinks to the services (applications) provided by the VCH project:

1. DTU course on wind energy (itslearning): https://www.itslearning.com/elogin/autologin.aspx?CustomerId=1956
2. TU/e collaboration environment (MS Sharepoint): https://vchcollaboration.tue.nl
3. KTH remote lab[34]: https://egiswamid.egi.kth.se/secure
4. PoliTo Start-up Pre-Incubation Support (StartApp): http://toce.polito.it/vchub
5. My Virtual Campus Hub group memberships (SURFteams): https://teams.surfconext.nl/teams/home.shtml?view=gadget

The technical information on connecting this IIS website as service provider to SURFconext can be found on the SURFconext Wiki[35]. Information on how to get access to the portal can be found in deliverable *D5.3 Virtual Campus Hub Technology*[36].

All of these services can exist independent of the portal, incl. the federated login (if they have been connected to the VCH infrastructure). In fact, if a user goes directly to the URL belonging to a service, the same federated logon procedure will be used as when logging on to the portal. What the portal does is to present all links on one page, so a user does not need to search for all these links. The single sign-on feature is provided by Surfconext and is not part of the VCH portal itself.

Problems and solutions

The problems with getting the portal connected were almost the same as with getting the TU/e collaboration environment (MS Sharepoint) connected. The main difference was that setting up the portal was less complex, which meant that the TU/e developers, with help from SURFnet and the available documentation[35], were able to get the connection to SURFconext working.

[34] http://www.energy.kth.se/proj/projects/Remote_labs/RL/RL_website/Home.html
[35] https://wiki.surfnet.nl/display/surfconextdev/Get+Conexted
[36] http://www.virtualcampushub.eu/Deliverables.aspx

4 Conclusions

In this chapter, the main conclusions from the experiences and ideas with respect to realizing the technical connections to the Virtual Campus Hub as presented above are discussed. In the next chapter, an agenda for the future is formulated based on these conclusions. These conclusions have been integrated in a broader set of conclusions on Virtual Campus Hub in deliverable *D6.7 The Virtual Campus Hub Concept* (§6.3 Points of attention using Géant/eduGAIN).

4.1 Technology

The main conclusion with respect to the technological aspects of the VCH proof of concept are:

1. ***Reliability***: The connections and the functionalities realized in the VCH proof of concept have proved to be very reliable. On the one hand, this is not surprising, because both the infrastructure (NREN/Géant/eduGAIN) and the applications connected are proven technology. On the other hand, realizing the connections has been far from easy, so some bugs afterwards were to be expected. There were none worth mentioning, however, once the relevant configuration issues had been solved. The conclusion from using this pilot environment is therefore that the VCH infrastructure is a reliable one.
2. ***Scalability***: Once the basic connections had been realized, it turned out to be very easy to add extra IdPs (once these had been made available to eduGAIN). This makes the federated identity management model very well scalable from the view of a service provider (SP), because once this SP has been connected, there is no work at the SP-side needed to add additional IdPs. The same goes for adding extra services (SPs), even if there can be quite some work involved to get an SP connected. The advantage lies in the fact that connecting an SP is completely independent of the connection of other SPs to the infrastructure, so there are no interaction effects. This implies that adding new services to a collaboration can happen gradually without having to redesign the connections with SPs already connected. In addition, as said, the IdPs made available to one of the SPs connected can without effort be made available to newly added SPs (only formal agreement is needed is most cases, but the technical work involved is neglegible).
3. ***Easy integration of cloud services***: As the case of DTU itslearning has shown, providing services within a collaboration is not limited to partners' internal applications. It is also possible to include external cloud services in a collaborations' service offering. In fact, from the point of view of the other partners using such a cloud service, it is hard to see the difference, because they access these services in the same way as the other ones.
4. ***Group management***: Group management has proved to be a powerful and reliable functionality with much potential to provide access to members of cross border collaborations, even if was only applied in a limited way in this project. It is a pity, therefore, that only few federations offer this functionality at the moment (such as Surfconext, NL and Internet2, US). This also means that it is difficult to apply in cross border collaborations (involving eduGAIN), as most service providers are most likely to use the solution of their local federation and not the one of another, "far-away" federation. In addition, there is no mechanism available yet to exchange group information between federations, which means that it cannot easily be used in a cross border collaboration yet (see also §5.1).
5. ***Towards federated identity management as a utility service****:* While the federated identity management service has proved to be very reliable, it has not turned out to be the "black box" we expected it to be at the beginning, far from it. Architectures and implementations between federations differ, it is sometimes unclear where the cause of a certain problem can be found (partner or federation level) and updating of metadata to eduGAIN may take quite some time. So while we as partners expected the main problems to lie with the local partners, crossing

borders turned out to be new also for NRENs. For the future, a model needs to be worked out for implementing cross border federated identity management efficiently, such that the process between federations and eduGAIN becomes a black box to institutions and they can "plug in to it" like a utility service. In addition, a clear division of labour and responsibilities between partners and federations is needed (see also §4.2).

6. ***Unified communications hub technology in earlier stage of development than federated identity management***: The attempt to get a pilot with unified communications across borders off the ground showed that this is much less proven technology than federated identity management, the main focus of the VCH project. It is also still quite expensive, there are few bridging standards available and there has been limited interest from vendors to participate in this VCH pilot and to enable their applications for federated identity management. This also means that the scalability of using unified communications across borders is limited, as the partners in different collaborations are not very likely to use the same tools, so different UC hubs for different collaborations an institution is involved in will be needed. As this is also very expensive, the most likely scenario at present is that every institution or every collaboration will analyze its gaps and find out itself how to best fill the gaps identified. In most cases, that will mean adding a separate platform to the existing infrastructure, until more generally applicable UC hub technology becomes available that is also able to integrated with the VCH infrastructure.

4.2 Organization

1. ***Involvement of all relevant stakeholders****:* The discussion in chapter 3 has made clear that during this project, many efforts were needed to get all relevant stakeholders on board, quite a few of which did so quite reluctantly, for many good reasons. For future projects that deal with cross border infrastructure, it is clear that these stakeholders need to be involved from the start, preferably already when the proposal is written. On the other hand, we have learned, most people at end user organizations that are in a position to initiate such projects have no idea that something like federations and federated identity management exists, so more publicity on what happens at the infrastructure side might help as well.
2. ***Federation as (technical and legal) knowledge brokers****:* In this VCH project, no partner has been able to realize the connections on its own. In fact, all partners that tried got stuck at some point, because of limited knowledge on how to deal with federated identity management and, as it was unknown matter, also without knowlegde on who would be able to help them out. The federations have been of great help in this, eventually, but it was also clear that this position of knowledge broker was not seen as one of their main services. However, federations seem to us the organizations that are best-placed to have a good overview over the sector that deals with their core technology and taking the role of knowlegde broker towards institutions more seriously would help the adoption of federated identity management considerably, we think. As the technology gets more common, also legal issues become more important and also here the federations seem best-placed to take up this role.
3. ***Coordination between partners and federations****:* The fact that during the VCH project there was sometimes confusion about who needed to take up a task and on where the cause of a certain problem was to be found, points to the need for a different coordination structure in future projects. As it is difficult for a local partner to oversee all things that happen or need to be done at the federation level and vice versa, a better model could be that one of the federations coordinates the work to be done at the federation level and one of the partners coordinates the other partners (as has been done in this project). But other models may work as well and a precondition is of course, as mentioned above, that federations are involved from the beginning.
4. ***Industry IdPs and other kinds of IdPs ("Homeless users")***: A barrier to the full realization of the VCH concept was that part of the VCH target population is unable to participate in a

seamless way, as the Géant infrastructure is in principle only intended for institutions of higher education and affiliated research institutes. This is strange, as research and education have been collaborating with industry and other entities for a long time already and integration of education, research and innovation is also high on the EU agenda. But as it comes to federated identity management, accepting this reality seems hard to do. It is also one of the reasons PoliTo has not been connecting its Start-up Pre-Incubation Support application (StartApp), as the added value of this is limited as long as their main target group (people from outside the research and education sector) are not able to participate through an IdP and will have to make use guest accounts. However, just providing these “homeless users” with separate guest accounts is not the solution. It would be better, it seems, if the world of federated identity management for higher education and research would embrace the rest of the world and would find ways to integrate these identities with their own (see also §5.3).

5 Agenda for the future

5.1 Scaling up collaborations 1 (group management)

Upscaling group management

While group management in the VCH proof of concept has been a small-scale pilot, real collaborations tend to intensify and become larger-scale if successful. This means the administrative load of managing groups and their access to applications becomes an important factor, which cannot be dealt with using the *ad hoc groups* model applied in the VCH pilot, based on a group administrator inviting the different members by email (see §3.2.6).

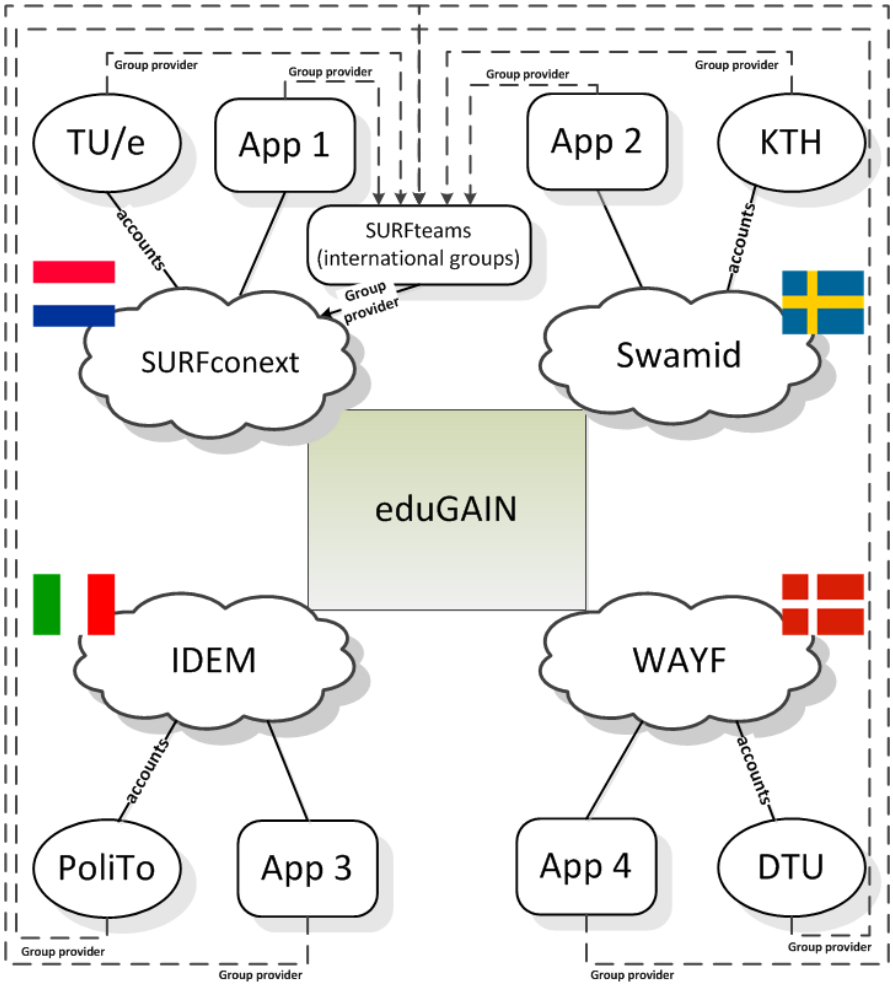

Figure 5: VCH architecture with IdPs and SPs as group providers to the central external group management service SURFteams

For large-scale collaborations, different models are needed. A possible model is the one offered by SURFconext and COmanage[37], shown in figure 5 above. In this model, the institutions participating in a collaboration or the applications they have connected also serve as group providers to the central group management service (such as SURFteams used in VCH), e.g. by providing a group with all 1st year students of a certain joint programme following the programme at that institution, a group with all students at an institution following a certain joint course or a group of lecturers from an institution involved in a joint course. The central group management service may then combine these different

[37] Both use Grouper for their group management service: http://www.internet2.edu/grouper.

groups from institutions into one group with, for example, all 1st year students from all locations involved in a certain joint programme, possibly adding *ad hoc members* at the central level through the invitiation procedure described before. This information can then be used by applications connected to provide access. Changes in groups are managed decentrally (every institution manages its own groups), which means groups can better be kept up-to-date, while the overall information is available to everyone in the collaboration. While this model is quite powerful, more experience with setting up such models and managing them in a cross border collaboration is needed.

Exchange of group information across federations
A weak point with group management at present, and thus also with the models discussed above, is that there is no mechanism available to exchange group information between federations and via eduGAIN. This means at present a collaboration must choose one of the federations as its group management provider (if it offers this service). This may be problematic, as institutions usually are involved in more than one collaboration at the same time, which might require them to enable the same applications for different group management implementations (in use at different federations). Its unlikely they are willing to do that, so the inability of federations and eduGAIN to exchange group information poses a serious barrier for using group management in cross border collaborations. Some ways of solving this have been discussed at the recent TERENA VAMP workshop[38], but there is still a long way to go.

5.2 Scaling up collaborations 2 (account linking)

When a collaboration scales up, two things can be expected (see also the discussion on this in §2.3):

1. The collaboration intensifies, probably implying that also access to applications that are well-integrated with the local administrative systems is needed.
2. Increased mobility of the members of a collaboration, meaning they would be changing identity more often, while still requiring access to the resources they had access to with their previous identities, e.g. when a student, a lecturer or a researcher moves several times in a relatively short timespan between institutions and/or companies within the same collaboration network. See also the next section (§5.3).

As a result, account linking or ID-mapping, is likely to become an important issue once collaborations have adopted federated identity management and want to take further steps in their collaboration. There are no clear solutions available yet[39], however, but work on this is being done in GN3+[40,41].

[38] See the notes of the Open Session on harmonizing group management at TERENA VAMP 2013: http://www.terena.org/activities/vamp/ws2/slides/OpenSpace_notes.pdf
[39] An exception is the US initiative Orcid, which provides researchers with a mobile identity: http://orcid.org
[40] GN3+ Subtask Account Linking in JRA3T2.
[41] See also the notes of the Open Session on account linking at TERENA VAMP 2013: http://www.terena.org/activities/vamp/ws2/slides/OpenSpace_notes.pdf

5.3 Participation of industry (as IdPs)

The inability of industry to connect as IdPs to the Géant infrastructure has been identified as an important barrier to provide seamless access to collaborations in education and research, as public-private partnerships for these collaborations are increasingly common. However, there have been some interesting experiments in this field[42] and some ideas proposed to deal with this matter[43].

For example, in relation to KIC InnoEnergy[44] (see deliverable D6.6 Dissemination and exploitation strategy), a public-private partnership on education, research and innovation in the energy field, consisting of several nodes across Europe involving universities, research institutes and companies, a idea has been proposed to create a KIC InnoEnergy IdP, that would issue accounts and email addresses, which users could then use to access "InnoEnergy-approved" applications throughout the InnoEnergy community. This would provide members of the InnoEnergy community with seamless access to all relevant applications and support the mobility of members across the InnoEnergy network. To minimize administration for staff and hassle for users, such an InnoEnergy IdP might reuse accounts from existing IdPs within the InnoEnergy community and add a virtual stamp "member of InnoEnergy" to these accounts. But various modes and models are possible in this.

The problem with the example from KIC InnoEnergy above remains of course the access of industry to the Géant infrastructure. Next to accepting them on the Géant infrastructure (possibly for a fee), another solution might be to create a so-called "open collaboration exchange", an idea proposed by SURFnet at TERENA VAMP 2013[45], a flexible setup to bridge different approaches to federated identity management. In principle, this could also allow individual users (i.e. not affiliated with an organization and thus also not present in an IdP) to participate in activities of such virtual organizations, e.g. by using their eID[46]. And other models may come up here as well.

Public-private partnerships such as KIC InnoEnergy may also contain small and medium enterprises (SMEs), which may not possess the resources to setup an IdP themselves. To still involve these collaboration partners in a fully fledged way, cloud services have emerged that can offer this kind of identity management services to these smaller companies. A good example is GARR (IT), which offers a so-called "IdP in the cloud" service to a number of smaller organizations among its members[47]. And there are also private companies able to provide such services.[48]

5.4 Unified communications across borders

The conclusion from VCH with respect to unified communications across borders was that the technology for unified communications hubs is too immature at present to be generally applicable for collaborations. However, as this kind of communication is essential for cross border collaborations, it would be good if pressure could be put on vendors to come up with standards for UC hub technology and to enable their products for federated identity management. And if the market will not solve this problem by itself, perhaps there are other ways to realize this.

[42] For example, see the pilot of SURFnet in the with NBIC-CTMM, a public-private partnership in Bioinformatics research: http://www.surfnet.nl/en/Thema/coin/indepraktijk/Pages/PilotNBIC,CTMMandNLeSC.aspx and http://www.surfnet.nl/en/Thema/coin/indepraktijk/Pages/Default.aspx
[43] See also the notes of the Open Session on Industry and eduGAIN at TERENA VAMP 2013: http://www.terena.org/activities/vamp/ws2/slides/OpenSpace_notes.pdf
[44] http://www.kic-innoenergy.com
[45] http://www.terena.org/activities/vamp/ws2/slides/OpenCollaborationExchange.pptx
[46] https://www.eid-stork.eu
[47] See http://www.terena.org/activities/vamp/ws2/slides/Lalla_Mantovani.pdf
[48] One example is iWelcome, http://www.iwelcome.com, but many others exist as well.

5.5 Service provision across borders (federation hubs)

The example of the DTU itslearning cloud service (see §3.2.1) has shown that different federations have different architectures, have different ways to connect a service, have different policies and are in a different stage of readiness to support (cross border) connection of service providers. For service providers that offer their services in many countries, this can be a costly affair and also one difficult to manage from a technical point of view, as many different interfaces to federations need to be maintained. And, as in the case of itslearning, the servers are located in one country (Norway), so there is basically no reason to connect to more than one federation once the adoption of services like eduGAIN takes off.

As a result, the development of the eduGAIN service may lead to a situation where (commercial) service providers choose one federation as their “hub” to provide their service via eduGAIN across Europe and other countries that are or will be member of eduGAIN. This, in turn, may lead to a competition between federations to become a service provision hub. What would determine a federation to be chosen as a hub is unclear yet, but it seems obvious that the presence of functionalities dealt with in the other sections in this chapter will play a role in this. As such, eduGAIN may have the potential to turn the traditional world of federation upside down if it is able to keep up with developments itself.

5.6 Presentation

Virtual organizations that deepen their collaboration efforts are likely to have more joint activities and will develop a higher need to get reliable information provision. As a result, the requirements to portals serving the collaboration will be more ambitious as well. Then again, however, the problem comes up that institutions are likely to be involved in more than one collaboration at the same time, which would imply that they would need to make their services available in different ways in different portals, if there were no possibilities to reuse the solution applied for the portal of one collaboration to that of another (see also §2.4). For some time, following Google’s OpenSocial standard seemed a way to realize this, as it is also well able to support federated identity management, but at the time of writing it is unclear if this standard will be supported in the long term. Therefore, promoting general (and reliable) standards to do this would be helpful to stimulate (cross border) collaboration.