Open Cloud eXchange (OCX)

Draft proposal by GN3plus JRA1 Task 2 Network Architectures for Cloud Services

Draft version 0.8 (Public), 27 September 2013

Contributors:

Yuri Demchenko (UvA) (editor)
Migiel de Vos (SURFnet)
Damir Regvart (CARNET)
Sonja Filiposka (UKiM)
Tasos Karaliotas (GRNET)
Kurt Baumann (SWITCH)
Daniel Arbel (Technion)
Jeroen van der Ham (UvA)
Rudolf Strijkers (UvA)
Eduard Escalona (I2CAT)

Abstract

The concept of Open Cloud eXchange (OCX) has been proposed to bridge the gap between two major components of the cloud services provisioning infrastructure: (1) Cloud Service Provider (CSP) infrastructure which either has a global footprint, or is intended to serve global customer community, including those customers who target to deliver services to the global/worldwide community; and (2) cloud services delivery infrastructure which in many cases requires dedicated local infrastructure and quality of services that cannot be delivered by the public Internet infrastructure. In both cases there is a need for joining/combining CSP infrastructure and local access network infrastructure, in particular, for solving the "last mile" problem in delivering cloud services to customer locations and individual (end-)users. The OCX will remain neutral to actual cloud services provisioning and limit its services to Layer 0 through Layer 2 to remain transparent to current cloud services model. The proposed document identifies the initial set of requirements to OCX, that can be run by NRENs, as a part of the GEANT network, or jointly, and provides suggestions about OCX implementation. The proposed OCX concept will leverage the existing Internet eXchange (IX) by Internet community and GLIF Open Lightpath Exchange (GOLE) by GLIF community, adding specific functionality that will simplify inter-CSP and customer infrastructure integration when supporting basic cloud services provisioning models, in particular Trusted Third Party (TTP) services to allow federated infrastructure and access control, commonly used by NRENs.

Table of Contents

1 Background

The use of cloud based services and Cloud Computing technologies [1-4] in general among universities and by NRENs will increase in the near future. This will be stimulated also by increasing demand for computation power for the emerging Data Intensive Science applications that require both advanced computing and networking infrastructure and infrastructure to support collaborative groups. There is a need for another technologies consolidation to address both infrastructure performance and manageability for data/computing centric/driven tasks and for advanced user support for project oriented collaborations. Currently, NRENs are providing network access and advanced infrastructure services for their constituencies, and also the infrastructure for federated access control and cross-organisational collaborative groups support.

In many cases large Cloud Service Providers (CSP) can create/establish a Point of Presence (POP) for large customers. On the other hand, customers with distributed campuses are ready to extend their network to one of the CSP's POP. The latter approach is becoming popular among National Research and Education Network NREN's at national level. The approach can be also used at the European R&E network GEANT what would simplify cloud services delivery for European wide projects and communities.

The proposed document provides information for discussion how the above mentioned trends (and related problems) can be addressed with the new proposed idea of the Open Cloud eXchange (OCX) that should provide a framework and facilities for better services delivery from the Cloud Service Providers (CSP) to customers (organisations) and to end-users, on one hand, and simplify integration of cloud based applications between universities. The OCX will remain neutral to actual cloud services provisioning and limit its services (of the transport network) to Layer 0 through Layer 2 to remain transparent for current cloud services model.

The document provides background information motivating OCX development, summarises the general use cases and defines requirements to OCX. The document proposes an initial OCX architecture and design and also refers to other technologies that describe the background environment in which the proposed OCX will operate, including standardisation activities related to the inter-cloud technologies

1.1 GN3plus JRA1 Task 2 Network Architectures for Cloud Services

Open Cloud eXchange has been initially proposed by the GN3plus JRA1 Task 2 Network Architectures for Cloud Services activity.

JRA1 Task 2, Network Architectures for Cloud Services, will research which general architecture and network technologies are best suited for cloud-based services and how NRENs can design and build their networks to offer cloud-based services at scale to the full range of their users (also seen in a global perspective). The result will be a part of the basis for Task 1.

Network infrastructure plays important role in delivering cloud services and can be seen as three interdependent structures:

- The user access network, which connects users to applications.
- Extreme high-speed networks, which interconnect physical servers and the movement of their virtual machines (VMs).
- Mega pipe networks, interconnecting storage tiers.

JRA1 Task2 will, in cooperation with Task 1, investigate and propose the best architecture for supporting the three interdependent structures that support a cloud-based service, including the distribution of very large scientific data. In addition, the results and findings will be supported by test and/or demonstration cases.

JRA1 is focusing on the network elements and orchestration for supporting cloud-based services, whereas JRA2 will research true software-driven networking for cloud-based services, with automated resource orchestration and provisioning that yield reduced network capacity requirements, predictable service performance, and simpler operations. It is therefore expected that JRA1 and JRA2 will cooperate on topics such as network virtualisation and automation solutions that deliver Performance on Demand by automating the allocation of shared network resources among data centres on behalf of cloud operations. JRA2 will cooperate

on the Task 2 work and will focus on the software-driven elements and related control plane aspects; JRA1 will focus on the southbound elements of the management and related control plane matters when interworking with the software-driven network elements

1.2 Notes from the JRA1 kickoff meeting (4-5 April 2013, NORDUNET, Copenhagen)

Initial discussion of the Open Cloud eXchange idea took place at the GN3plus JRA1 kick-off meeting at NORDUNET Copenhagen offices on 4-5 April 2013. The Task 2 members discussed existing problems and challenge in delivering the cloud services to NREN members: universities and research organisations. SURFnet presented their project on providing dark fiber between cloud providers and universities that created a starting point for the initial definition of the Open Cloud eXchange.

2 Use cases and scenarios

This section will provide initial information about typical cloud use by universities and research community and analyse in more details few selected use cases that motivates need of the dedicated delivery infrastructure for cloud services to support advanced research at universities and other research organisations. Further use cases definition will require contribution from the GN3plus and GEANT community.

We refer to the general use case cases and usage scenarios defined by industry and documented by NIST [NIST Use cases], Open Data Center Alliance (ODCA) [10], and Global InterCloud Technology Forum (GICTF) [11], however define the specific of the cloud use by the education and research organisations.

2.1 Clouds use by universities

Detailed analysis of the cloud services use by universities is presented in the Appendix B. Here we provide a short summary of the typical cloud services use.

The following lists the typical/popular uses of cloud services by universities both at the level of departments and individually by the staff and the students:

- Outsourcing e-mail service to global providers where the most popular is the Gmail by Google. Gmail allows email accounts consolidation and has benefit of the global accessibility what is the important for mobile research community.
- Storage services are very popular both for backup purposes and for sharing documents and data. Documents and data sharing are important services to support intra- and inter-organisational collaboration. The popular shared storage services include Dropbox, SkyDrive, Box and others. Despite the existing security concerns these services are quite popular for regular and not security critical cases. TERENA community has being developing secure cloud storage sponsored by the TF-Storage [put reference here]
- CloudApps services which is the most popular representative is Google Apps are quite popular both among researchers and students. CloudApps allows easily construct a necessary computational task using available functionalities and obtain necessary modelling results.
- Many general and specialist software applications are provided as Software as a Service (SaaS). Examples of such services include scientific software and applications [need more specific example]
- Currently, increasing amount of scientific data is available to research community and collaborative groups as Grid and cloud storage resources. Examples are LHC experiment data and genome data that are provided to researchers worldwide. Other scientific data repositories such as satellite data may require more strict policy compliance.
- Using cloud Infrastructure as a Service (IaaS) services are popular for deploying multiple VMs that can be used for running user designed services and doing experimentation with new infrastructure services and protocols.

- National and organisational data centers are increasingly providing access to High Performance Computing (HPC) as cloud services.

In most cases the above use of cloud services is done over Internet and doesn't require any specific network services. However advanced research require access to large datasets, scientific instruments and HPC. Combining all these components into collaborative scientific infrastructure will require dedicated network infrastructure and related services to support researchers' collaboration.

Referring to the generic Cloud Services Model [2, 4, 15, 17] such functionality can be defined as Intercloud Access and Delivery Infrastructure (ICADI) which the main goal is to deliver cloud based services to organisational customers and end users. More details about ICADI is provided in Appendix C1.

2.2 Basic/Reference use cases requiring dedicated cloud services delivery infrastructure

At this moment we can identify the following use cases for delivering cloud services to campus based users:

- Streaming high speed high volume experimental or visualisation data to (and from) labs in campus location that may require dedicated links.
- Distributed scientific data processing with MPP tools on the facilities distributed among universities and research organisations.
- CSP and campus network peering over dedicated L0-L2 fiber link.

The goal of the references use cases collection is to identify the required functionality for the Cloud/Intercloud Access and Delivery Infrastructure (ICADI) that structurally includes all infrastructure components between the CSP, the final consumer and other entities involved into cloud services delivery and operation.

3 Open Cloud Exchange (OCX) definition and general requirements

This section provides the definition of the Open Cloud eXchange (OCX) that was proposed to address the currently existing problems in delivering cloud services to organisational/enterprise customers and end users. The OCX intends to bridge the gap between two major components of the cloud services provisioning infrastructure:

(1) CSP infrastructure which either has a global footprint, or is intended to serve global customer community, including whose customers who has global/international presence or deliver services to global/worldwide community; and

(2) Cloud services delivery infrastructure which is despite the cloud services concept is based on the ubiquitous Internet connectivity, in many case require dedicated local infrastructure.

In both cases, there is a need for joining/combining CSP infrastructure and local access network infrastructure, in particular for solving the "last mile" problem in delivering cloud services to customer locations and individual (end-)users.

3.1 OCX definition

The OCX concept is based on and extends the Internet eXchange (IX) and Optical eXchange model with additional facilities/functionality to allow ad hoc dynamic Intercloud federation establishment and non- restricted cloud providers, customers, and also local infrastructure providers peering in case when cloud services delivery requires involvement of such entity.

Besides providing physical location for interconnecting (network) of all main/involved actors, to simplify and facilitate services delivery the OCX declares two basic principles:

- **No third party services** (like service brokering, integration or operation) – OCX will not be involved into business relations related to the actual cloud services delivery;
- **Trusted Third Party (TTP)** services to facilitate ad-hoc/dynamic federations establishment – OCX may provide service of the trusted repository of the PKI certificates, provider and services directory. OCX may operate under supervision of the community (representatives) which will act as a policy authority for security and operational practices; in this case OCX may provide a clearinghouse service for SLA and PKI Certificates policies.

The proposed OCX role as a TTP will facilitate creation of dynamic federations, establishment of dynamic trust relation. As a part of membership service OCX, the member CSP's may establish trust relation, i.e. by means of cross-certification or just providing trusted certificates repository similar to TACAR (TERENA Academic CA Repository) [36].

The intended OCX functionality belongs to the general Intercloud Access and Delivery Infrastructure (ICADI) as defined by the Intercloud Architecture Framework (ICAF) [15, 17]. However, the OCX may limit its services to Layer 0 through Layer 2 to remain transparent to current cloud services model.

3.2 Requirements to OCX

This section will provide both general requirements to OCX functionality and its design followed from the basic use cases and scenarios analysis. Rationale for the requirements is provided where necessary.

1) Generally, the OCX should follow and leverage the Internet eXchange design and operational principle adopted to support specifics of the cloud services provisioning. In this respect, OCX can be similarly defined as a place for inter-connection and peering between providers and customers.

The big cloud providers are becoming global service and infrastructure providers with their own infrastructure spanning globally. They change the telecommunication landscape and can handle significant amount of their own and customers' traffic internally though internal network infrastructure which is not necessary need to be TCP/IP protocol based.

OCX may also benefits from been collocated with collocation service provider, NREN exchange points, regional data center servicing regional/national research community.

2) Primarily, the OCX should provide the Layer 0 through Layer 2 network services to interconnect CSP Points of Presence (PoP) to be fully transparent to current cloud services models that generally uses Layer 3 network infrastructure virtualisation when deploying VMs and their interconnection.

However, further performance optimisation for cloud infrastructure may require Layer 2 network virtualisation and performance optimisation. Consequently, this may require OCX services at the lower layers.

OCX should support topology information exchange between peering members of the OCX. Topology information exchange should be considered as an important component/requirement for effective services interconnection at different networking layers.

OCX interconnection network infrastructure must guarantee high QoS parameters such bandwidth, latency and jitter.

3) OCX should provide necessary services to support smooth services delivery and integration between CSP and Customer that besides network connectivity may include support for federated services integration and operation.

These services can be generally defined as Trusted Third Party Services (TTP) and may include but not limited to:

- Trusted introducer service that can be supported by the Trusted Certificates Repository (similarly to TACAR service by TERENA [37].

- CSP and Cloud Services Directory and Discovery Service
- SLA repository and clearinghouse

4) OCX architecture should allow flexible operational scenario where it may have hierarchical architecture and can be operated by NREN's and GEANT.

When implemented with modern optical network technologies (e.g. Lambda and DWDM) the OCX can easily realise different distributed topological models: extended, collapsed, hierarchical

4 The proposed OCX Architecture and components

Figure 1 below illustrates the general case of implementing enterprise or scientific workflow on the heterogeneous multi-provider infrastructure. OCX that can be placed between customers/campuses and cloud providers will provide facilities for interconnecting all members and entities of the federated cloud infrastructure.

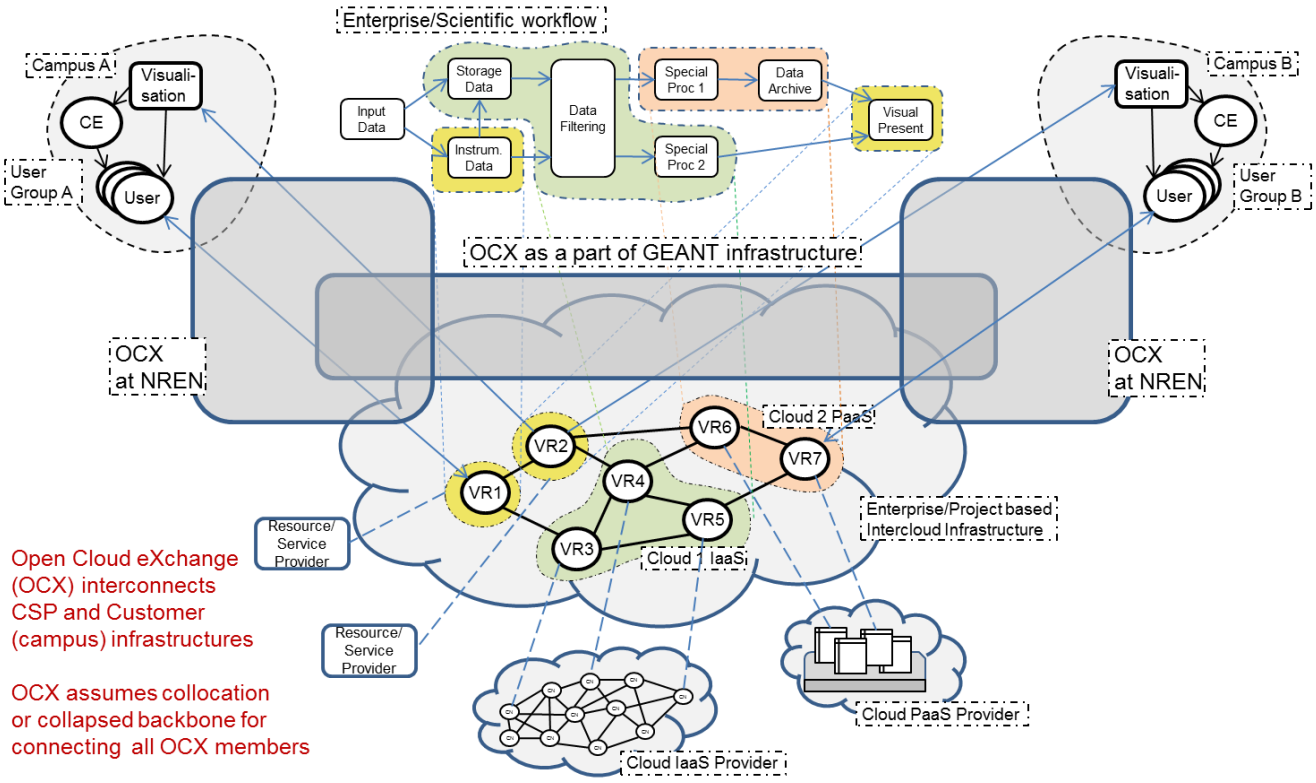

Figure 1. Enterprise or scientific workflow implemented on the heterogeneous multi-provider infrastructure.

Architecturally and functionally OCX functions and services are related to the ICADI layer in the multilayer Cloud Services Model (see details below in Appendix C.3).

Figure 2 provides another view for the OCX services where OCX services can be provided by the Cloud Carrier or Network Provider level, in particular NREN or GEANT.

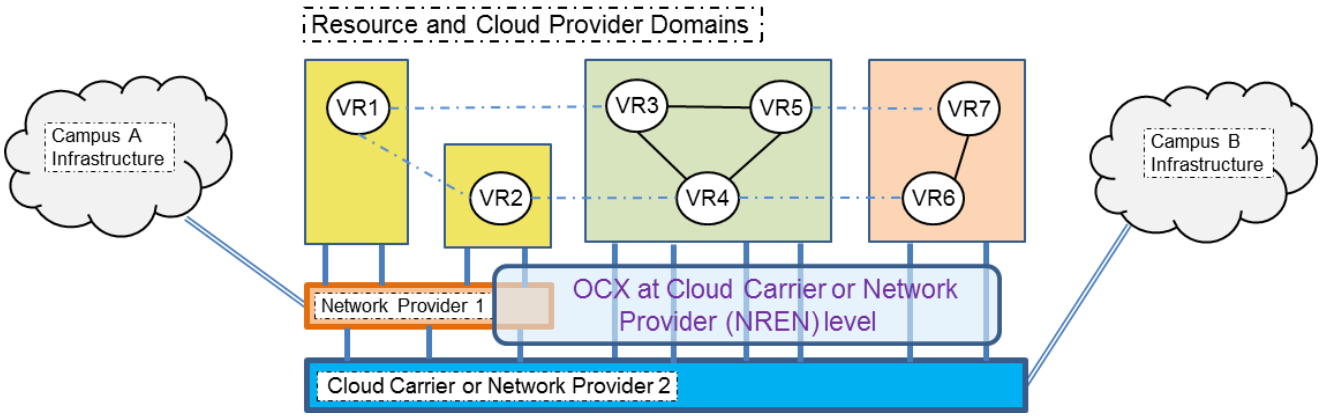

Figure 2. OCX at Cloud Carrier or Network Provider level.

Architecturally and functionally the OCX includes the following services and functional components (see Fig 3):

- Physical Point of Presence (PoP) for providers and customers
- L0-L2 network interconnection facility (optionally also connectivity with the dedicated optical links)
    - The associated service should allow topology information exchange between providers and customers in a secure and consistent way (note, topology information in most cases considered as commercial or restricted information)
- Trusted Third Party (TTP) services to support dynamic peering, business/service and trust relations establishment between OCX members; the specific services may include:
    - Trusted Certificates repository and associated Trusted Introducer service to allow dynamic trust associations and/or federations establishment
    - Additionally Trust Broker service can provided supported by either or both Trusted Introducer and privacy/data security policy Registry or clearinghouse.
- Publish/subscribe Services Directory and Discovery; additionally the SLA Clearinghouse service can be provided.
- Additionally, Cloud Service Broker to provide service advice and integration for contracted community.

Figure 3 provides a view of the core OCX components as a part of the federated Intecloud infrastructure that involves multiple Cloud Service Providers which use OCX for transparent exchange of traffic/communications between cloud services.

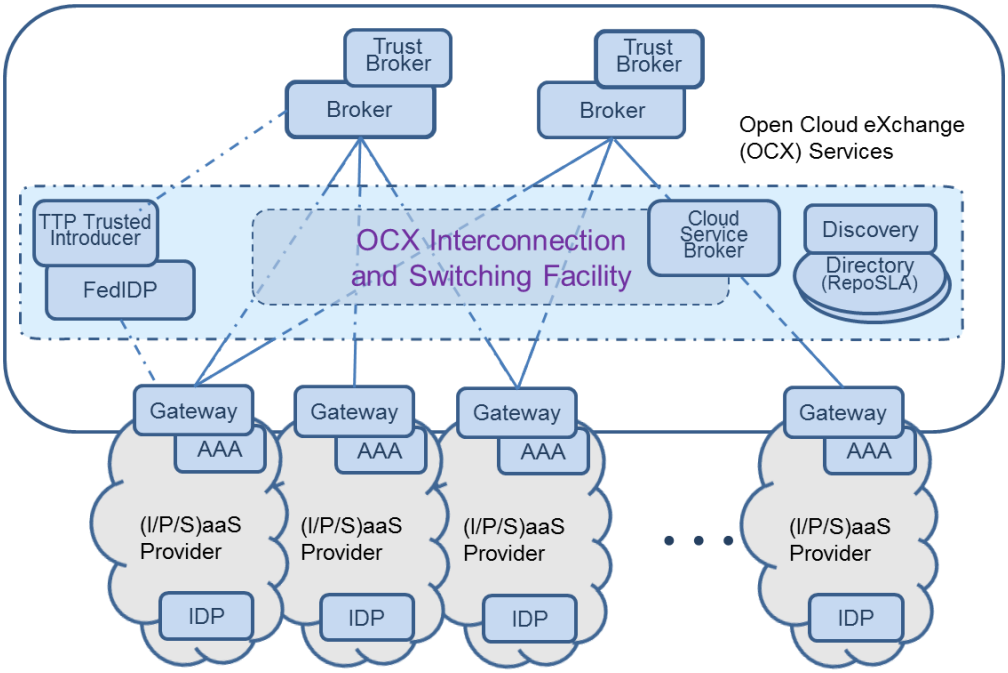

Figure 3. OCX functional component (core and optional)

5 OCX Design suggestions

This section will provide suggestion for design and implementation of the functionalities described in the Requirements and Architecture sections.

5.1 OCX interconnection network and peering design

Topologically OCX should allow any-to any interconnection at Layer 0, Layer 1 and Layer 2. OCX L0-L2 topology.

This can be implemented by using corresponding L0-L2 optical switches. Figure 4 illustrates the switching topology of OCX.

Note:

Design suggesting should be provided to support topology information exchange in a secure way.

Design suggesting should be provided how to achieve guaranteed QoS parameters such as bandwidth, latency and jitter.

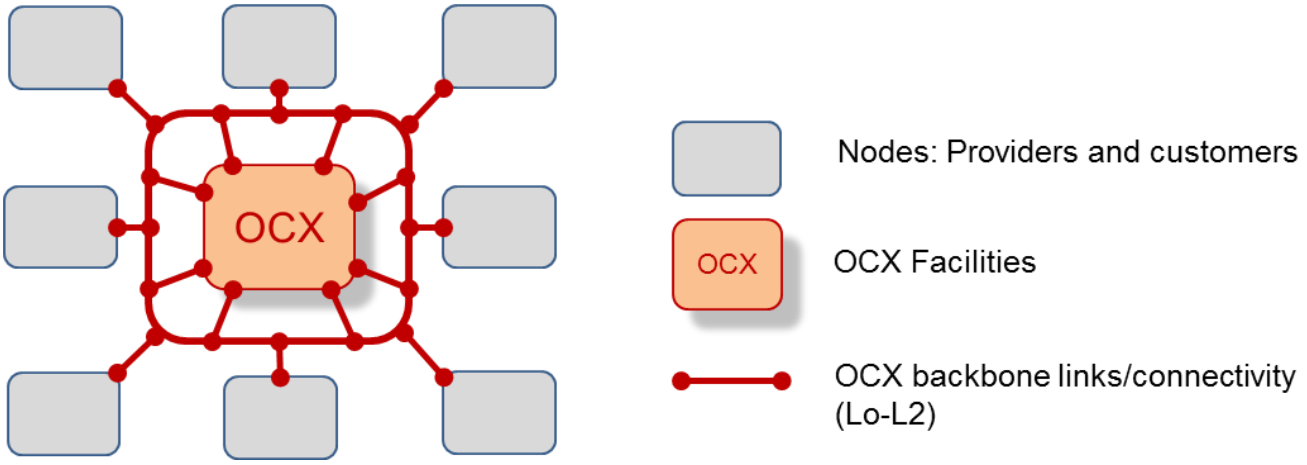

Figure 4. OCX topological model

5.2 OCX SDN-based Design

The characteristics of the OCX require fast decision making and policy enforcement mechanisms to coordinate transparently the traffic of the cloud service transactions. OCX can benefit from an SDN architecture by adopting its main design principle, the separation of the control and data planes. This way, the data plane can be optimized for applying forwarding rules efficiently at any layer (L0-L2) while the SDN controller will implement data forwarding, data filtering, policy enforcement, TTP services, etc. A modular implementation of this SDN controller such as the one offered by Floodlight [37] or even an implementation using the Network as a Service (NaaS) concepts developed by frameworks like OpenNaaS [38] provide the flexibility and extensibility that allow an easy adaptation of interconnectivity requirements.

5.3 OCX Trusted Third Party services

Figure 3 illustrates how OCX can operate as a Trusted Third Party to establish direct/dynamic trust relations between OCX members. These trust relationships can be used for establishing identity management federations among OCX members.

This section will provide design suggestion how to achieve the required TTP services such as

- Trusted Certificates repository (similarly to TACAR, TERENA Academic CA Repository) and associated Trusted Introducer service to allow dynamic trust associations and/or federations establishment
- Trust Broker service can provide supported by either or both Trusted Introducer and privacy/data security policy registry or clearinghouse.

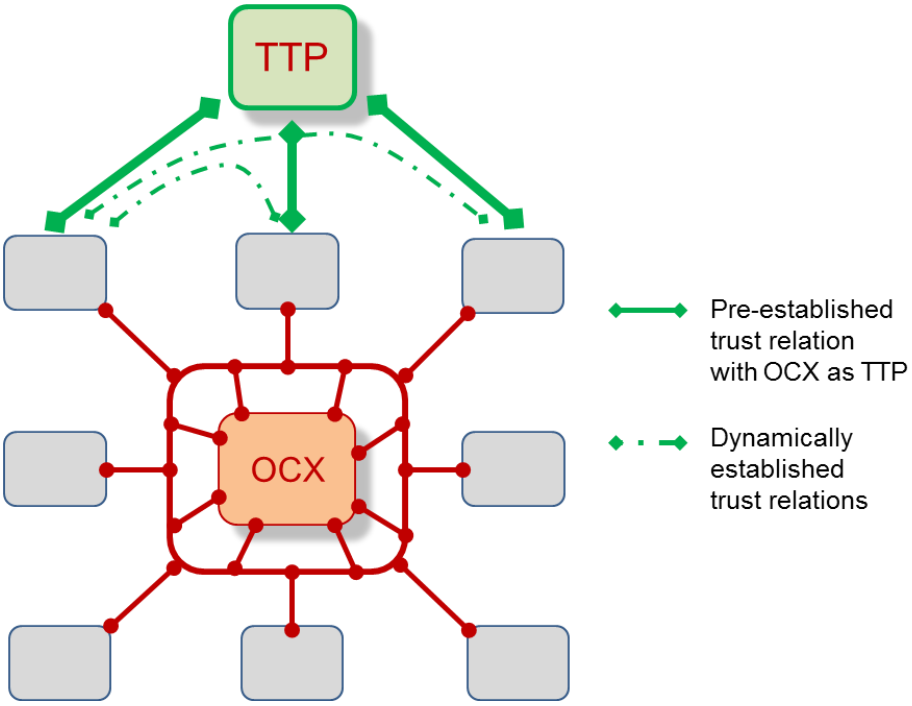

Figure 5. OCX TTP role in establishing dynamic trust relations between OCX members

We refer to research works in [20] and [21] that provide a solution and mechanisms for trust relations establishment in the federated cloud environment. It is recommended that members need to have trust policies to define such criteria.

5.4 Trusted Introduction Protocol for Dynamic Secure Federations Establishment

This section will provide suggestions for defining and implementing the Trusted Introduction Protocol for the Dynamic Secure Federations establishment using OCX TTP services. The proposed solution will evalluate solutions developed by the ABFAB WG at IETF[25, 26] , works by the University of Kent [20] and the University of Amsterdam [21].

5.5 OCX API's definition

The OCX design will define the major API's to access OCX services. This will be typically required when changing the CSP and customer setup and relations. OCX is intended to be transparent for cloud services protocols and communications.

The following API will/may need to be defined:

- OCX interconnection API that will include the following functions:
  - interconnection topology, presumably "many-to-many"
  - Links bandwidth QoS parameters
  - VPN/virtual circuits setup, etc.
- Access (publish-subscribe) to OCX CSP, Customer and Service Directory
  - Presumably Web Services SOAP or REST interface
- Access SLA and security policy repository and clearinghouse
  - Presumably Web Services SOAP or REST interface

- Access OCX Trusted Anchors Repository that will collect and store certificates of the OCX members
  - Presumably Web Services SOAP or REST interface
- *(Optionally)* Secure Token Service (STS) and Federated Identity Provider (FIDP) that can be provided by GEANT network or local NREN – *To be discussed.*

6 OCX implementation models

We consider different options for OCX location: at NREN's, at GEANT premises and combined versions with hierarchical OCX infrastructure and extended OCX backplane/backbone. Figure 6 illustrates the basic options with single OCX located at GEANT or NREN premises.

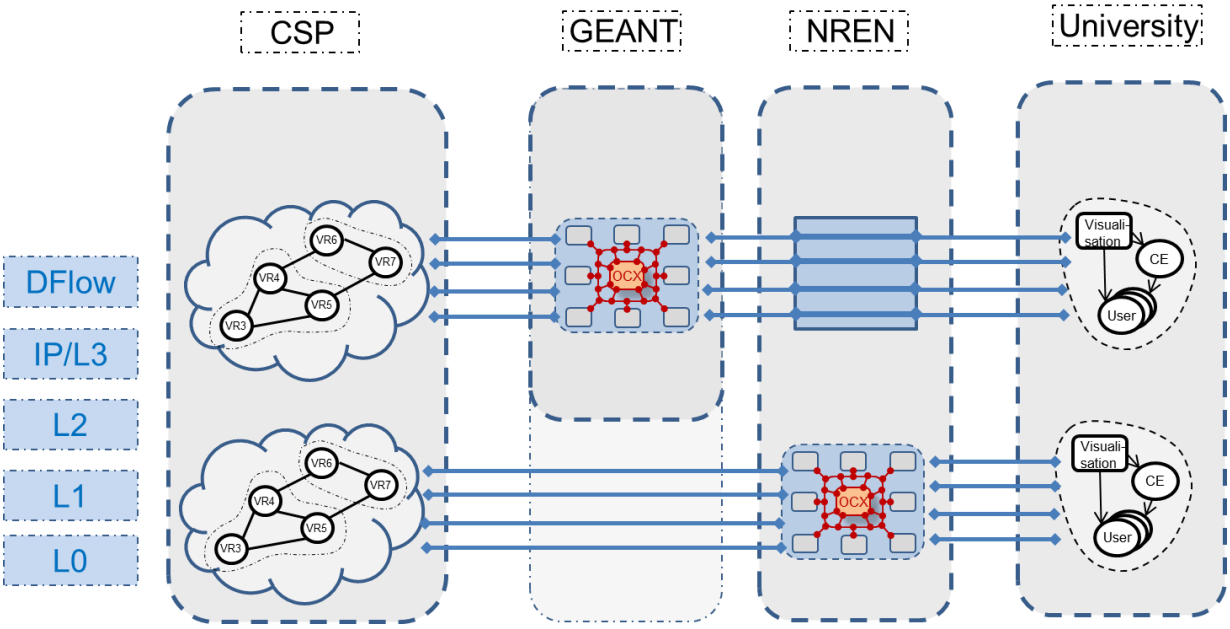

Figure 6 Single OCX located at GEANT or NREN premises: single OCX on L0-L3 (IP) and DFlow.

Figure 7 illustrates hierarchical OCX architecture there OCX at the Trans-European/GEANT level are interconnected with the national OCX run by NRENs to create cross-border cooperative access infrastructure to cloud services. OCX's operates independently but use dedicated links to interconnect between them.

Figure 8 illustrates distributed OCX topology that uses extended backplane approach where the OCX switching backplane is extended to remote location.

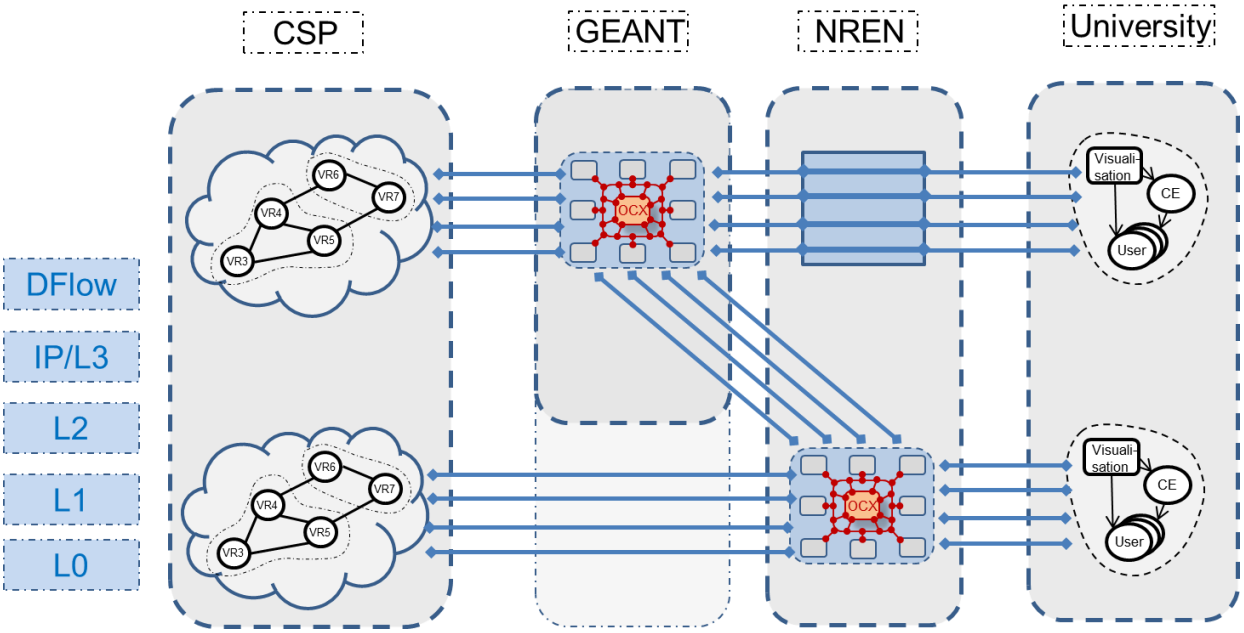

Figure 7 Single OCX located at GEANT or NREN premises: hierarchical.

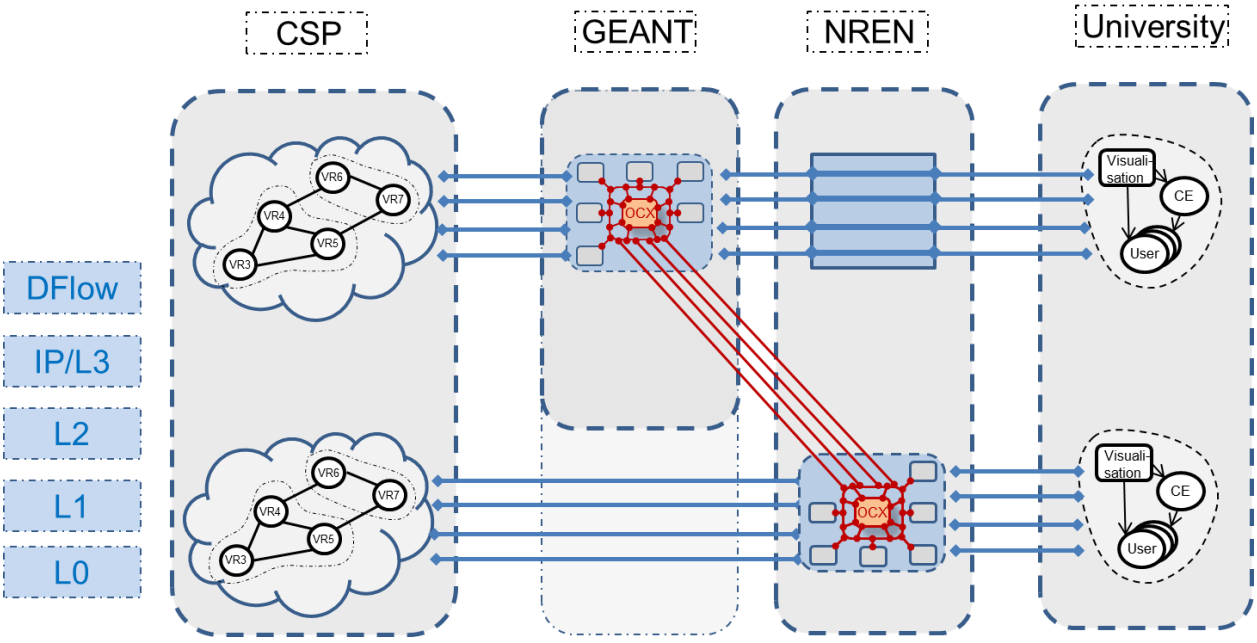

Figure 8 Single OCX located at GEANT or NREN premises: extended backplane.

7 Related Projects by GEANT community and NREN's

7.1 Prototype OCX Services Implementation by SURFnet

7.1.1 NetherLight Open Lightpath Exchange to offer Open Cloud eXchange services

As of 2002, NetherLight in Amsterdam is one of the Open Lightpath Exchanges (OLE) operated by SURFnet. An OLE allows any party to connected and does not have limitations on the possible cross connects. These cross connects are always transparently made on L2 or below. In the past 10 years many international connections and cross connects have been made and the OLE infrastructure has been growing. Nowadays almost the whole world can be reached via the OLEs and its connectors.

NetherLight, and some of the other OLEs, intend to innovate and keep ahead. This means that new technologies are tested and if successful implemented. Currently NetherLight is working on innovation topics such as Bandwidth on Demand, Virtual Networking, 100G transatlantic trials and the Open Cloud eXchange (OCX) concept.

In the second half of 2012, SURFnet and NetherLight have been performing pilots with cloud providers that want to offer their services with lightpath characteristics to SURFnet connected institutions. This meant that the concept of NetherLight as OLE would remain similar, but the function would grow. Next to an innovator and international hub NetherLight can now also be identified as marketplace. Via this marketplace cloud providers can offer their services to the SURFnet connected institutions, via connected OLEs to other R&E institutions and to other cloud providers.

7.1.2 GreenQloud

Researchers, teachers, students and ICT departments of institutions are interested in using the advantages of cloud computing. They would like to save costs, not worry about running out of storage and easily extend or run additional machines and/or jobs. Most of these people would like to use dedicated paths to the cloud provider, to ensure protection from the internet and make it possible to incorporate cloud machines into their own network.

GreenQloud is a company from Iceland that provides storage and compute in the cloud using 100% renewable geothermal and hydro energy. Connecting the services of GreenQloud with lightpaths via NetherLight gives our connected institutions some advantages above the regular IP services:

- Guaranteed bandwidth and latency
- Protected from the regular internet
- Possibility of domain extension (VM's appear as if inside campus network)
- Cost reduction due to offloading of traffic

In this case the lightpaths between GreenQloud and our connected institutes are dedicated and redundant[1] Ethernet services through NetherLight.

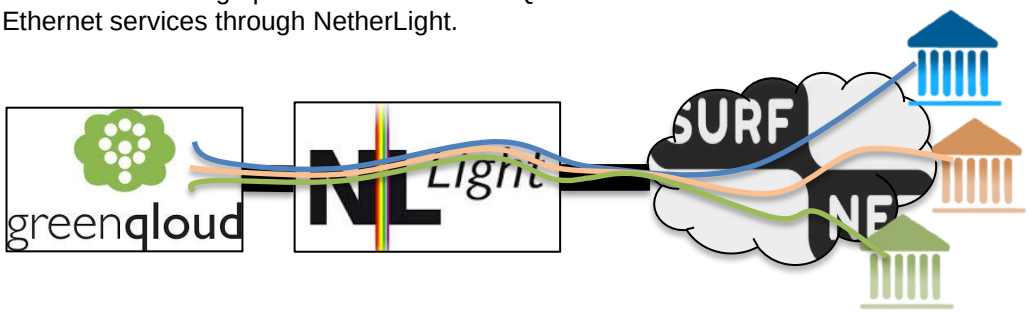

Figure 7.1: NetherLight setup; VLANs from GreenQloud to three SURFnet connected institution

[1] Redundant path is work in progress, expected in Q4 2013.

In addition GreenQloud was also connected to the SURFconext platform. Providing all researchers, students, teachers and ICT staff safe and easy access.

7.1.3 OneXS

Institutions would like to benefit from the use of unified communications. Unified communications provides a combination of voice, chat, audio- and videoconferencing. These services can be used via the regular Internet. However, this does not provide enough certainty and therefore a dedicated path between the institution and the cloud provider is required.

OneXS is a service provider for communication and data solutions. Their core business is fixed and mobile telephony. In 2012 a pilot was started between OneXS and Windesheim University of Applied Sciences. In a successful pilot OneXS provided unified communications. A few months later another SURFnet-connected institution requested to use the services of OneXS via NetherLight. Using the services of OneXS via lightpaths through NetherLight give our connected institutions some advantages above regular IP connectivity:

- Guaranteed bandwidth and latency
- Protected from the regular internet
- Protected from DDOS attacks

In this case the lightpaths between OneXS and our connected institutes are dedicated Ethernet services through NetherLight.

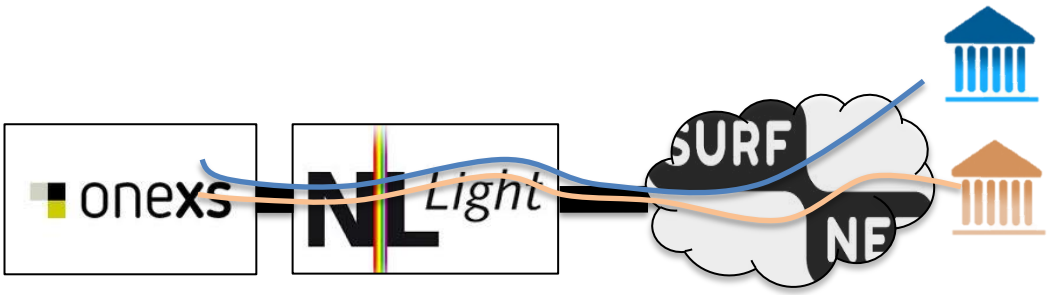

Figure 7.2: NetherLight setup; VLANs from OneXS to two SURFnet connected institution

7.2 SURFConext [29]

The SURFconext infrastructure for online collaboration gives users access to services provided by various different providers, which they can apply within a single environment. This opens up new opportunities for collaboration within and between institutions.

SURFconext is a collaboration infrastructure that connects a number of basic building blocks for online collaboration:

- Federated authentication and authorisation, so that users can securely access all kinds of available services via the same account that they use at their own institution;
- Group management making it possible for access to content and functionalities, for example for a project team, to be managed centrally. These may be internal groups of the institution or groups from SURFconext group management application;
- Standard data interface for exchanging activities, reports, and group information (OpenSocial) with cloud applications;
- Cloud applications of various providers (for example Google Apps, Edugroepen, Sharespace, Liferay Social Office).

SURFconext allows institutions to integrate internal and external online services, thus enabling them to offer users a collaboration environment within which they can access the online services that they require.

SURFconext is part of the SURFworks innovation program. SURFconext has been developed for and in collaboration with the higher education and research sector in The Netherlands. For institutions, the launch of SURFconext offers an occasion to join forces and to draw a common strategy for online collaboration. At the same time it facilitates lightweight integration of self-hosted institutional services with (commercial) cloud services.

7.3 The GLIF "Automated GOLE Pilot" Project [30]

GLIF stands for the Global Lambda Integrated Facility, a cooperation between NRENs and research institutes launched in 2001. GLIF has a two-fold goal: to create a forum for engineers and researchers to exchange experiences, and to cooperate to make lambdas available for researchers and projects involved in data intensive research.

In order to make global optical networking possible, GLIF exchange points have been created where long connections can be connected together to create multi-domain lightpaths. These exchange points typically work on a lower layer than common Internet Exchanges, since they typically connect users on layers lower than 2.

During the history of GLIF the policy applied at exchange points was not always clear, so several years ago the concept of a GLIF Open Lightpath Exchange (GOLE) has been defined. This mandated that GOLEs have an open character, i.e. treat everyone the same, and be open about any policy that may be applied [GOLE].

Since the start of GLIF inter-domain lightpath provisioning has involved much manual processing and actions. Typically a user requests a lightpath at his home institution, which is then forwarded to an NREN. The lightpath will cross several GOLEs, after which again an institution and end-user is involved in terminating the lightpath request. Each of these has to play an active role in the process of creating the lightpath, ranging from approving the request to changing the configuration of the network to accommodate the request. Often these are distributed over several timezones, which means that a lightpath request often takes about two weeks to be implemented.

In 2009 GLIF started with a taskforce to implement automation in several of its GOLEs using early implementations of the Network Services Interface [NSI]. Several GLIF participated to jointly create an Automated GOLE testbed. The evolution of this testbed has been demonstrated at SC10,SC11 and SC12.

The tesbed is created by thirteen different GOLEs, spanning over a dozen timezones, using five different implementations of the NSI Connection Service. This has made it possible that lightpaths can now be created and destroyed within seconds, during SC12 we demonstrated hundreds of requests daily. With this much smaller response time it has become much easier and attractive for users to request multi-domain lightpaths.

The early experiments with the Automated GOLE testbed have also helped to improve the NSI protocol. NSI Connection Service version 2 is now submitted as a draft standard, and will be demonstrated at SC13. Many participants are currently working to implement this version also, and they have also indicated to move this service into production as soon as possible.

7.4 Federated Access to Web resources: eduGAIN [35]

GEANT community has long time experience in federated network and services access. Federation are typically created at the national level and run by NREN's. To allow federated access at trans-European level, the community has challenged the following level of services federation by enabling by inter-federation, the possibility for users from one federation to access services provided by another federation. This process is made possible through an infrastructure that supports the exchange of information between different countries, by technologies that enable for the process to take place in a secure fashion and by legal obligations (such as data protection laws or a contractual agreement) that ensure that users data are securely handled.

eduGAIN is an infrastructure that enables trustworthy exchange of information about authentication and authorisation among GÉANT partners and possibly beyond. eduGAIN can provide a good model for OCX TTP trust management and services federation.

7.5 GRNET Okeanos Project [31]

7.5.1 General Description

GRNET Oceanos project aims to built a Cloud Infrastructure in order to provide

- IaaS service similar to Amazon AWS (Cyclades)
- Storage Service (Pithos+)
- Virtual Networks
- Virtual Firewalls (not available yet)

Figure 9 Okeanos Components bellow describes the complete toolset provided by okeanos and how they could be incorporated together in order to build a private in-cloud infrastructure.

The service is based solely on Open Source Software and in more details

1. KVM hypervisor
2. GANETI Cluster-based virtualization management software
3. Open Source Cloud Components built in-house like
    a. Synnefo (provides Cyclades Service)
    b. Kalamari
    c. Archipelago (storage backend)

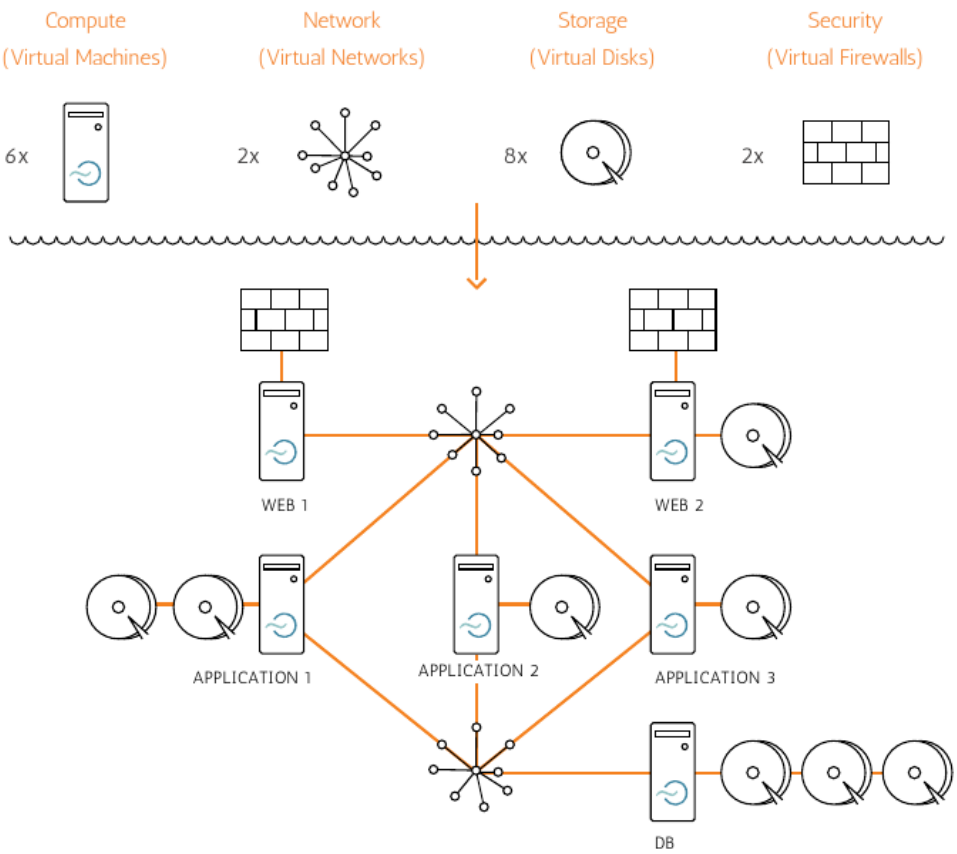

Figure 9 Okeanos Components

Okeanos supports KVM-based VMs, managed by Google Ganeti. .KVM does full system virtualization, and supports Microsoft Windows, Linux, and BSD deployments inside its VMs. So far, server Images for Red Hat Enterprise Linux / CentOS, Fedora, Debian Linux, Ubuntu/Kubuntu, and Microsoft Windows Server 2008R2 have been tested extensively inside ~okeanos deployments, using virtio-based storage and network drivers for minimal virtualization overhead.

VM storage volumes are physically stored as objects in a distributed, redundant, object-based storage backend. he storage backend is deployed in commodity physical nodes, with no need for proprietary hardware or custom interconnects; it is a distributed, shared-nothing architecture, with no SPOFs. Storage bandwidth and capacity scales with the number of storage nodes. Nodes are added and removed in a live system, with dynamic object replication and automatic rebalancing. Having a shared-storage backend allows for seamless VM migrations among physical nodes.

7.5.2 Okeanos interfaces

All Okeanos functionality is exported to end users via a clean RESTful Okeanos API that is a superset of OpenStack Compute API v1.1. Following an open standard ensures compatibility with a multitude of third-party cloud management tools and lowers the barrier to entry for migration of existing software deployments on the cloud.

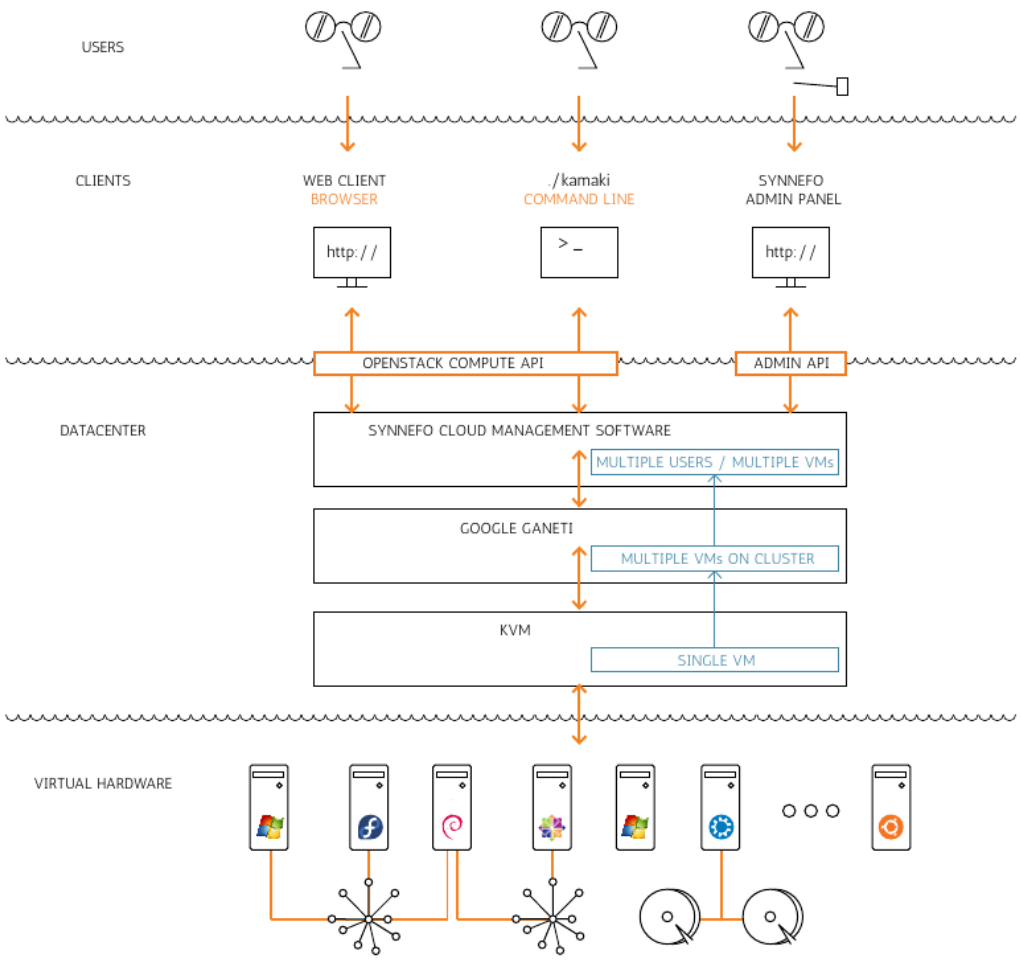

Figure 10. Okeanos layered architecture.

~okeanos comes with a clear, simple Web UI through which the user may quickly provision new and manage existing compute, network and storage resources. The Web UI is a client-side Javascript/jQuery application using the ~okeanos API behind the scenes, which means two things: (a) the Web UI runs on the client side, eliminating unnecessary server roundtrips, (b) The API implementation is always up-to-date, with all functionality available both programmatically and over the UI.

When the need arises to provision and manage resources automatically and in bulk, the ./kamaki command-line tool can be used to perform low-level administrative tasks. ./kamaki is just another client to the ~okeanos API, targeted to advanced end users and developers.

7.5.3 Networking in Okeanos

~okeanos supports full IPv4 and IPv6 connectivity to the public Internet for its VMs. The network implementation is deployment- specific, behind Ganeti, and may be customized extensively to the customer's individual needs. A reference ~okeanos implementation supports host-based routing for multiple IP address pools, with minimal overhead, and no Network Address Translation. Eliminating the need for NAT allows VMs to migrate freely between physical hosts, without introducing SPOFs.

~okeanos provides virtual Ethernets as a separate resource, giving the user freedom to create arbitrary network topologies of interconnected VMs, e.g., for multi-tiered deployments of enterprise software. Private networks are supported by the API and are exposed all theway to the UI. Each private network is an isolated Ethernet segment, carrying raw L2 Ethernet frames. This gives unrestricted choice of IP addressing schemes, allows running own DHCP services, and supports non-IP traffic as well. VMs see a separate virtual Ethernet NIC for each private LAN they are part of.

The user may protect each public IPv4/IPv6 interface with a virtual firewall, choosing from a number of predefined firewall configurations. Firewalling is provided as a virtual appliance by the infrastructure and works independently from the guest OS running inside a VM. Bridging of cloud-based with physical resources One cannot expect a complete deployment of physical resources to be migrated overnight to the cloud. ~okeanos exploits private networking functionality to form secure bridges between virtual networks and your existing physical network in your server room or datacenter, essentially bringing cloud-based resources right next to your physical servers. Need your virtual resources to allocate IP addresses from your physical DHCP server? Now that's possible.

8 Future developments

The proposed document is a product of the GN3plus JRA1 Task 2 activity in cooperation with other activities.

The document provides an information to other project activities, to GEANT community and to other cooperating parties and seeks for comments and contribution.

The further efforts will be put to better defining the OCX components, detailing use cases and requirements, to moving to pilot implementation and design at selected number of NRENs and GEANT network itself.

The project recognizes importance of receiving feedback from wider community and will propose the OCX architecture and operational model to such standardisaion bodies as IETF and Open Grid Forum (OGF) Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [28].

9 Acknowledgement

This work is supported by the FP7 EU funded Integrated project GN3plus. The authors express acknowledgement to all project and research partners who contributed to the OCX functionality discussion and provided valuable advices regarding use cases, suggested technology use, and basic operational models, in particularly, we acknowledge contribution by Taras Matselyukh (Opt/Net BV) and Martin Pels (MS-IX).

10 References

Cloud Computing standards and BCP documents by industry associations

[1] NIST SP 800-145, "A NIST definition of cloud computing", [online] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] NIST SP 500-292, Cloud Computing Reference Architecture, v1.0. [Online] http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

[3] NIST SP 800-146, Cloud Computing Synopsis and Recommendations. May 2012 [online] Available: http://www.thecre.com/fisma/wp-content/uploads/2012/05/sp800-146.pdf

[4] Cloud Reference Framework. Internet-Draft, version 0.5, July 3, 2013. [online] http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-05.txt

[5] FG Cloud Technical Report (Part 1 to 7). [online] http://www.itu.int/en/ITU-T/focusgroups/cloud/Documents/FG-coud-technical-report.zip

[6] IEEE P2302 - Standard for Intercloud Interoperability and Federation (SIIF). [online] http://standards.ieee.org/develop/project/2302.html

[7] Trust Router. Internet-Draft, March 25, 2012. [online] http://www.ietf.org/id/draft-howlett-abfab-trust-router-ps-02.txt

[8] OASIS IDCloud TC, "OASIS Identity in the Cloud TC." [Online]. Available: http://wiki.oasis-open.org/id-cloud/.

[9] On-Demand Infrastructure Services Provisioning Best Practices. ISOD-RG Draft Version 04 [online] draft-isod-bcp-infrastructure-v04.docx
[10] Open Data Center Alliance (ODCA) [online] http://www.opendatacenteralliance.org/
[11] Global Inter-Cloud Technology Forum (GICTF), Use Cases and Functional Requirements for Inter-Cloud Computing, GICTF White Paper. August 9, 2010 [online] http://www.gictf.jp/doc/GICTF_Whitepaper_20100809.pdf
[12] SNIA Cloud Data Management Interface (CDMI) v1.0 [online] http://www.snia.org/tech_activities/standards/curr_standards/cdmi/ CDMI_SNIA_Architecture_v1.0.pdf

Major Cloud and Intercloud Architecture papers and reports

[13] Rajkumar Buyya, Rajiv Ranjan, Rodrigo N. Calheiros, InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2010, Busan, South Korea, May 21-23, 2010), LNCS, Springer, Germany, 2010.
[14] Bosch, P., A.Duminuco, F.Pianese,T.L.Wood, Telco Clouds and Virtual Telco: Consolidation, Convergance, and Beyond, Proc. Symposium on Integrated Network Management, 2011 IFIP/IEEE, 23-27 May 2011.
[15] Intercloud Architecture for Interoperability and Integration, Release 2, Draft Version 0.7. SNE Technical Report 2012-03-02, 1 July 2013. [Online] http://www.uazone.org/demch/worksinprogress/sne2012-techreport-12-05-intercloud-architecture-draft07.pdf
[16] Demchenko, Y., C.Ngo, M.Makkes, R.Strijkers, C. de Laat, Intercloud Architecture for Interoperability and Integration. Proc. The 4th IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2012), 3 - 6 December 2012, Taipei, Taiwan. IEEE Catalog Number: CFP12CLU-USB. ISBN: 978-1-4673-4509-5
[17] Demchenko, Y., C.Ngo, M.Makkes, R.Strijkers, C. de Laat, Intercloud Architecture Framework for Heterogeneous Multi-Provider Cloud based Infrastructure Services Provisioning. IJNGC Journal, July 2013.
[18] Makkes, M., C.Ngo, Y.Demchenko, R.Strijkers, R.Meijer, C. de Laat, Defining Intercloud Federation Framework for Multi-provider Cloud Services Integration, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2013), May 27 - June 1, 2013,Valencia, Spain.
[19] García-Espín, J. A., J. Ferrer Riera, S. Figuerola and Ester LópezA Multi-tenancy Model Based on Resource Capabilities and Ownership for Infrastructure Management. Proc. The 4th IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2012), 3 - 6 December 2012, Taipei, Taiwan. IEEE Catalog Number: CFP12CLU-USB. ISBN: 978-1-4673-4509-5
[20] Chadwick, D., M.Hibbert, Towards Automated Trust Establishment in Federated Identity Management. Proc. The 7th IFIP WG 11 International Conference on Trust Management (2013), Malaga, Spain.
[21] Ngo, C., Y.Demchenko, C. de Laat, Toward a Dynamic Trust Establishment Approach for Multi-provider Intercloud EnvironmentThe 4th IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2012), 3 - 6 December 2012, Taipei, Taiwan
[22] Promoting the Use of Internet Exchange Points: A Guide to Policy, Management, and Technical Issues, FInternet Society Report. 14 May 2009 [online] http://www.internetsociety.org/promoting-use-internet-exchange-points-guide-policy-management-and-technical-issues
[23] GFD.173 Network Services Framework v1.0, OGF Standard [online] http://www.gridforum.org/documents/GFD.173.pdf
[24] Amazon Direct Connect service [online] http://aws.amazon.com/directconnect
[25] IETF Application Bridging for Federated Access Beyond web (Active WG) [online] http://tools.ietf.org/wg/abfab/
[26] Trust Router. Internet Draft, March 25, 2012. [online] http://www.ietf.org/id/draft-howlett-abfab-trust-router-ps-02.txt
[27] Keystone, the OpenStack Identity Service! [online] http://docs.openstack.org/developer/keystone/
[28] Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG). [Online]. http://www.gridforum.org/gf/group_info/view.php?group=ISOD-RG

[29] SURFconext collaboration infrastructure http://www.surfnet.nl/en/Samenwerkingsomgeving/SURFconext/Pages/ProjectCOIN.aspx
[30] The GLIF "Automated GOLE Pilot" Project. http://staff.science.uva.nl/~delaat/sc/sc10/GLIFAutomatedGOLEPilot.SC.pdf
[31] Okeanos Infrastructure as a Service, GRNET Cloud service [online] https://okeanos.grnet.gr/home/
[32] GEANT Project. [Online] http://www.geant.net/pages/home.aspx
[33] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project). [Online] http://www.geysers.eu/
[34] GEYSERS Project Deliverable D2.2 (update). GEYSERS overall architecture & interfaces specification and service provisioning workflow. [online] http://wiki.geysers.eu/images/5/55/Geysers-deliverable_2.2_update_final.pdf
[35] eduGAIN [onlne] http://www.GÉANT.net/service/edugain/pages/home.aspx
[36] TERENA TF Storage. [online] http://www.terena.org/activities/tf-storage/
[37] TERENA Academic Certification Authority Repository. [online] https://www.tacar.org/
[38] Floofligh OpenFlow SDN Controller [online] http://www.projectfloodlight.org/floodlight/
[39] OpenNaaS: Open platform for Network as a Service resources [online] http://www.opennaas.org/
[40] Moonshot Project [online] https://community.ja.net/groups/moonshot

Appendix A Basic Cloud related terms definition

A.1 NIST SP 800-145 The NIST Definition of Cloud Computing

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing is defined as having five characteristics:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured Service

three service models:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

and four deployment models:

- Private clouds
- Public clouds
- Community clouds
- Hybrid clouds

Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

A.2 The major cloud stakeholders and actors

Cloud Service Provider (CSP) is an entity providing cloud based services to customers, on their request and based on the business agreement that is expressed as Service Level Agreement (SLA). It is important to admit specifics of business relations in clouds due to the fact that majority of cloud services are self-serviced and are governed under general or individualized SLA.

Cloud Service Broker (CSB) is an entity that may play a role of the third party in offering cloud service adding value of negotiating with many CSPs or customer groups and in some cases managing complex multi-provider services.

Cloud Service Operator is a new emerging role of the company that provides a value added service of integrating services from multiple cloud providers, delivering them to the customer and operating the resulting infrastructure.

Cloud Service Integrator is a role provided by the third party IT company to design and deploy the cloud services infrastructure that matches the customer requirements; this role includes detailed customer needs and requirements study and proposal of the optimized cloud based infrastructure, including also need for customer IT infrastructure redesign.

Cloud Auditor is a party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

Cloud Carrier is an intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers; Cloud Carrier services is typically provided by a telecom company.

Customer (like enterprise or university) is entity that request service from and has contractual relations with the CSP; customer does cloud services management themselves or outsource it to the third party.

Customer is an entity that requests cloud services. In a simple case, customer may be an end-user of the requested services, or in more general case, may be an organization (enterprise or university) that requests cloud based services for the members of their organisations and manages these services.

User is an end-user consuming cloud based services; in cloud services provisioning model an end-user may be also a customer.

Appendix B Cloud services use by universities and basic scenarios

B.1 Use cases and scenarios

The cloud services provided by GEANT and the NRENs are targeted for the Universities and Research Institutes/Centres as service users with the academic (teaching/research) staff, and students as end-users of all provided services. Thus, the potential number of users is measured well within tens of millions of end-users. The cloud services can make usability, administrative processes, research and scholarly collaboration more efficient and effective on a local, national, regional and overall scale of the academic network. However, another issue that must be considered for embracing cloud services is the reduced cost of operation. This is especially connected to the possible decentralized nature of the universities, in which situation a certain degree of services duplication and effort are imminent. One (obvious) way of reducing costs in these situations is leveraging internal cloud-like services by migrating to institutional solutions and/or virtual server solutions.

Since universities can be thought of as types of large enterprises, then the same recommendations and strategies should also apply maybe even more rigorously: they should generally avoid placing sensitive information in public clouds, but concentrate on building internal cloud and hybrid cloud capabilities in the near term. One such example is the IU Intelligent Infrastructure provided by the Enterprise Infrastructure division of University Information Technology Services at the Indiana University (http://kb.iu.edu/data/awwo.html) used to deliver mission-critical university applications and services. This service model offers two principal components: virtual systems, which supply the infrastructure and network capacity necessary to host applications, with optional disk storage on an enterprise-class storage area networks ensuring security and availability of files; backup solutions, which provide on-site and off-site storage, isolating from potential disasters by storing backup data within the provided hardened data centres. The general benefits obtained from the model are: reduced overall cost of hardware to the university, protection of environment with greener solution; improved security of university data and IT assets, etc.

In the case of a great number of end-users, it is essential that all of the supported cloud (and non-cloud) based systems can be accessed via a Central Authentication Service (CAS) using a single sign-on. The SSO can also be stacked with Federated authentication allowing members of one organization to use their authentication credentials to access a web application (i.e. cloud service) in another institution. Also, trust relationships that allow different entities to accept each other's assertions are needed. The eduGAIN service is the perfect candidate for providing Web SSO.

Universities need to consider which institutional services they wish to leave to consumer choice, which ones they wish to source and administer "somewhere else," and which services they should operate centrally or locally on campus. Cloud computing allows the flexibility for some enterprise activities to move above campus to providers that are faster, cheaper, or safer and for some activities to move off the institution's responsibility list to the "consumer" cloud (below campus), while still other activities can remain in-house, including those that differentiate and provide competitive advantage to an institution. An important option is the development of collaborative service offerings among universities. The cloud computing services are seen as a solution for the greedy demands of researchers for bandwidth and computing power and of students for sound and video-intensive applications.

There are a number of cloud services that are foreseen to be utilized by Universities:

- E-mail

E-mail is usually among the first services to move to the public cloud environment from the on-premises data centre thus eliminating the needs for upgrades, installing add-ons, or patching software done by the network administrators. Also, the cloud solution provides one consolidated place for all distributed entities inside the organization, while applying less limitations (especially inbox size) using scalable and well-distributed resources. This is especially the case for universities that don't have the capital to provide for the vast amount of users, and, even worse, the constant changeover. Migrating email to the cloud offers campuses substantial financial savings and eliminates on-site mail system infrastructure.

- Storage services

- Shared storage
- Backup storage

The cloud storage options allow organizations to choose one or more cloud locations to store files. Once the files are saved in one of several available cloud locations, they are accessible via nearly any computer or handheld device with Internet access and a web browser, reducing the need for multiple copies or additional disk space on the computer or mobile device. The shared storage options may include different solutions like Box, SharePoint, file shares in the local Data Center, Dropbox, GoogleDrive, SkyDrive etc. All of the supported locations are accessed using a single point of entry via the CAS system. However, before putting University information in the cloud, it is essential to determine whether the information will be adequately protected.

The tedious and costly work of IT staff to maintain an off-site backup location is the main reason for institutions turning to cloud backup providers for remote data protection. The amount of backup data often amounts tens of TB on a weekly basis. The use of VPN connections to an online backup cloud service with possible disaster recovery mechanisms, provide universities with the means for long-term protection of sensitive data. In the case of a university private cloud, a two site operation is usually favoured in order to provide a failover location.

- Scientific data access - Big Data
  - Genome data
  - LHC experiment data

Although SaaS are usually mostly interactive applications, there are opportunities for batch-processing and analytic jobs that analyse terabytes of data and can take hours to finish. The cloud computing model is a perfect match for big data related research since cloud computing provides unlimited resources on demand. If there is enough data parallelism in the application, users can take advantage of the cloud's new "cost associativity": using hundreds of computers for a short time costs the same as using a few computers for a long time. Programming abstractions such as Google's MapReduce and its open-source counterpart Hadoop allow programmers to express such tasks while hiding the operational complexity of the parallel execution across hundreds of servers. Integrating data from a widely spread network of sensors is another example of applications applicable in many different fields, while business intelligence and data analytics are the leading research problem driven by large enterprises. Also, the latest versions of the mathematics software packages Matlab and Mathematica are capable of using cloud computing to perform expensive evaluations. An interesting alternative model might be to keep the data in the cloud and rely on having sufficient bandwidth to enable suitable visualization and a responsive GUI back to the human user.

- Computational power
  - HPC access
  - VMs
  - Virtual computing labs

Members of the academic community (i.e. faculty, staff, and/or departments) can rent/use on-demand computational and storage services through a "Cluster as a Service" offered by: (i) a public vendor or (ii) another organization inside the NRENs national network or (iii) academic organization that is reachable directly via the Geant network. The cloud service can be provided using a real high-performance supercomputer cluster, or virtual machines, depending on the needs of the researchers. The IaaS clouds provided can be setup in different varieties: as Nimbus clouds – open source service package that allows users to run VMs by uploading or customizing provided image; OpenStack clouds – open source IaaS cloud-computing platform that supports an Amazon Web Services compliant EC2-based web service interface for interaction; Eucalyptus clouds - open-source software platform that additionally provides services such as the AWS-compliant Walrus and an interface for managing users and images; Virtual appliances (grid, Condor tasks, MPI tasks, Hadoop tasks, OpenStack etc) that can be used for training and education or creation of virtual computing labs for students use. Also, note that write-ups of science experiments performed in the cloud can contain reference to cloud applications like a virtual machine, making the experiment easier to replicate.

The PaaS model allows universities to be able to access other services and more advanced and more dedicated applications. As a matter of fact, PaaS does not merely allow one to access advanced services, it also allows creation of unique services, allowing universities to use cloud computing as a jump off point where they can access other services, create that application or service, or both.

- SaaS - CloudApps

The advantages of SaaS to both end users and service providers are well understood. Service providers enjoy greatly simplified software installation and maintenance and centralized control over versioning; end users can access the service “anytime, anywhere”, share data and collaborate more easily, and keep their data stored safely in the infrastructure. Basically, SaaS allows universities and students in those universities to utilize a wide range of applications and software online. It is evident that cloud computing remarkably boosts the learning ability of the students. SaaS can be employed for implementing new learning approaches and strategies. Universities can use CloudApps to effectively implement collaborative learning approaches where the students are able to work alongside students from other locations in order to achieve a common goal. Also, CloudApps greatly enhance the e-learning capability, making distant learning more effective and more efficient. Cloud computing and collaboration technologies can improve educational services, giving students access to low-cost content, online instructors, and communities of fellow learners.

At each university, there are a number of services (usually provided as a part of the university web portal) that are ready to be put in the cloud like: centralized publication database, private database, curricula and exam calendars, library system, CRM, e-learning portals, document creation/editing suits like GoogleApps, collaboration suits, e-tests and e-labs, etc.). Also, the integration of cloud technologies into computing curricula with the possibility of developing real applications used by other students can help in building a competence centre. Thus, in the field of SaaS universities are expected not just to have a huge basis of end-users, but also generate different academic CloudApps solutions. From the researchers point of view, SaaS applications are providing seamless collaboration on joint international projects and means of utilization of e-Infrastructure resources available. Special attention should be given to mobile interactive applications that respond in real time to information provided by users or sensors that combine two or more data sources.

- CaaS

Communication as a Service (CaaS), enables universities to utilize Enterprise level VoIP, VPNs, PBX and Unified Communications without the costly investment of purchasing, hosting and managing the infrastructure. CaaS has evolved along the same lines as Software as a Service (SaaS). Such communications that mostly interest the research community can include VoIP, instant messaging (IM), collaboration and videoconference applications using fixed and mobile devices. The CaaS vendor is responsible for all hardware and software management and offers guaranteed QoS. CaaS offers flexibility and expandability, with the network capacity and feature set changing from day to day if necessary so that functionality keeps pace with demand and resources are not wasted. In this sense, the Geant’s eduCONF in its cloud version can be seen as a CaaS testbed.

B.2 Benefits of using OCXs

- Other NRENs can also benefit from an already established private link (to Microsoft's Windows Azure service, for example) at a given NREN by enabling their universities to reuse the separate fast, stable and secure Geant network. What this means is students and academics alike can begin to take advantage of the outsourced cloud service for data crunching, storage and other cloud-based IT services over a high bandwidth connection.
- In order to provide risk mitigation integration with multiple cloud providers, as well as integrating cloud services with internally offered services are needed. One of the benefits in the proposed model is the integration of user credentials for different cloud services provides, based on federated identities. Federation identities can help institutions while bypassing expensive and exhausting point-to-point integrations.
- OCXs can serve as a type of an academic aggregator or broker. Cloud brokers, on the other hand, facilitate relationships directly between cloud service providers and their customers to negotiate better services, access, security, costs, and so forth.
- Using OCX a consortium sourcing model can be implemented. This model implies use of a not-for-profit means of aggregating demand to then either self-operate services or contract with a commercial or institutional provider to do so. Such a model allows for flexible group change, it avoids one-on-one

negotiations, and it leverages resources to improve economies of scale. One clear advantage of a consortium is the aggregation of demand that would allow institutions to better control their risk and cost. In this way, known entities at the national level leverage their resources and serve as cloud aggregators of institutional demand in multiple capacities.

- Aggregation of the academia's demand would help keep providers accountable and focused on addressing client needs. By aggregating the demand, the universities can preserve negotiating leverage. From the point of view of cloud providers, they would like the idea of not having to negotiate with each organization, but get a bigger deal with the OCXs being a sort of single point of contract.
- Cloud computing shared services environment can force a degree of standardization. Best practices approach can also ensure that providers are meeting "reasonable standards" expectations.

Appendix C Related developments and standardisation

This section provides overview of the related developments that can be used for OCX definition and design.

C.1 Intercloud Architecture Framework

C.1.1 General use cases for ICAF

The three basic use cases for Intercloud Architecture can be considered: (1) Enterprise IT infrastructure migration to cloud and evolution that will require both integration of the legacy infrastructure and cloud based components, and move from general cloud infrastructure services to specialised private cloud platform services; (2) large project-oriented scientific infrastructures including dedicated transport network infrastructure that need to be provisioned on-demand [15, 17, 18]; (3) IT infrastructure disaster recovery that requires not only data backup but also the whole supporting infrastructure restoration/setup on possibly new computer/cloud software or hardware platform. The networking research area itself introduces another use case for wide spread “cloud + network” infrastructure to support small and medium scientific experiments for testing new protocols and network dynamics that are too small for super computers but too big for desktop systems. All use cases should allow the whole infrastructure of computers, storage, network and other utilities to be provisioned on-demand, physical platform independent and allow integration with local persistent utilities and legacy services and applications.

Figures C.1 illustrates the typical example of building e-Science or enterprise collaborative infrastructure based on the defined scientific or enterprise workflow that includes campus/enterprise proprietary infrastructure and cloud based computing and storage resources, instruments, visualization system, interconnecting network infrastructure, and users represented by user clients. Figure C.2 introduces the Cloud Carrier role that provides the interconnectivity services between multiple cloud service providers, customer/campus locations and other components of the Intercloud infrastructure.

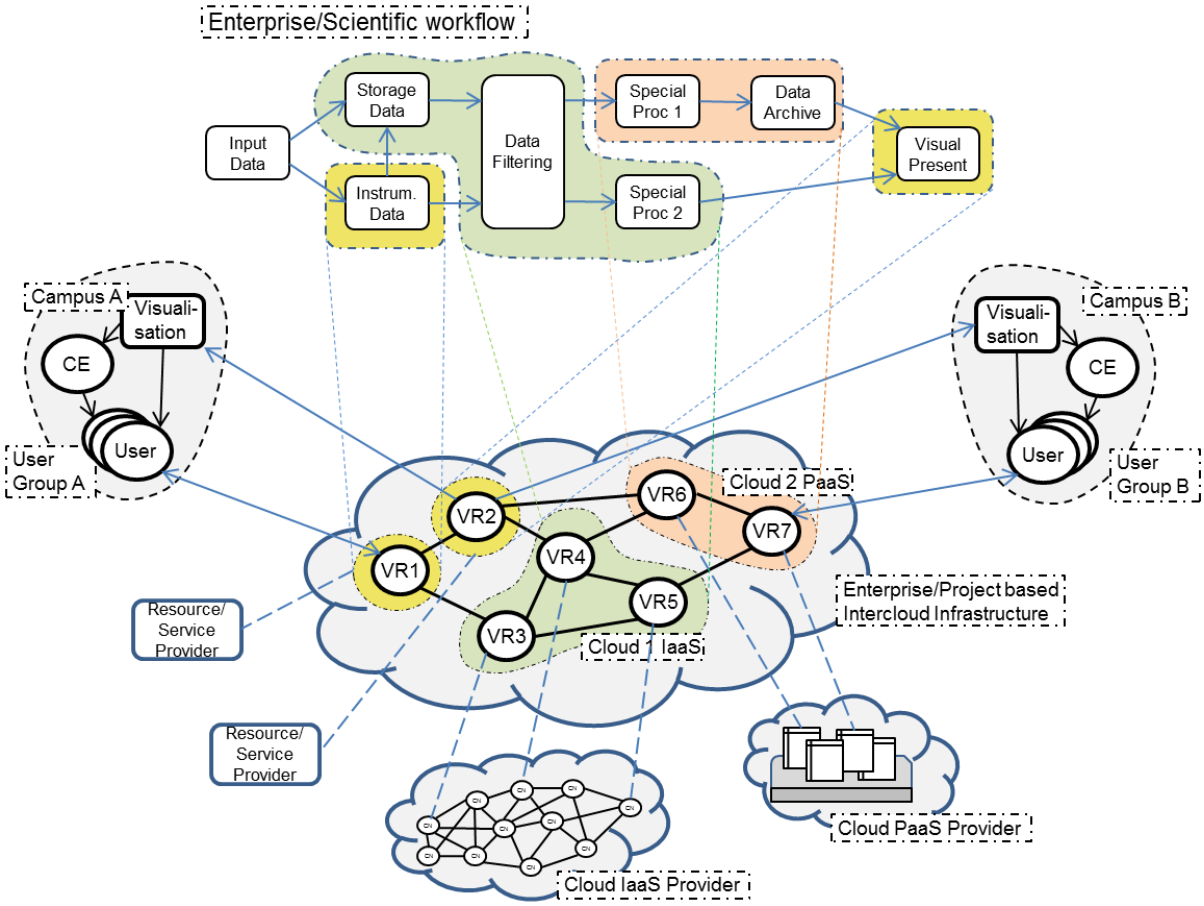

Figure C.1. Enterprise or project oriented collaborative cloud based infrastructure including IaaS (VR3-VR5) and PaaS (VR6, VR7) cloud infrastructure segments, separate virtualised resources or services (VR1, VR2) and two interacting campuses A and B.

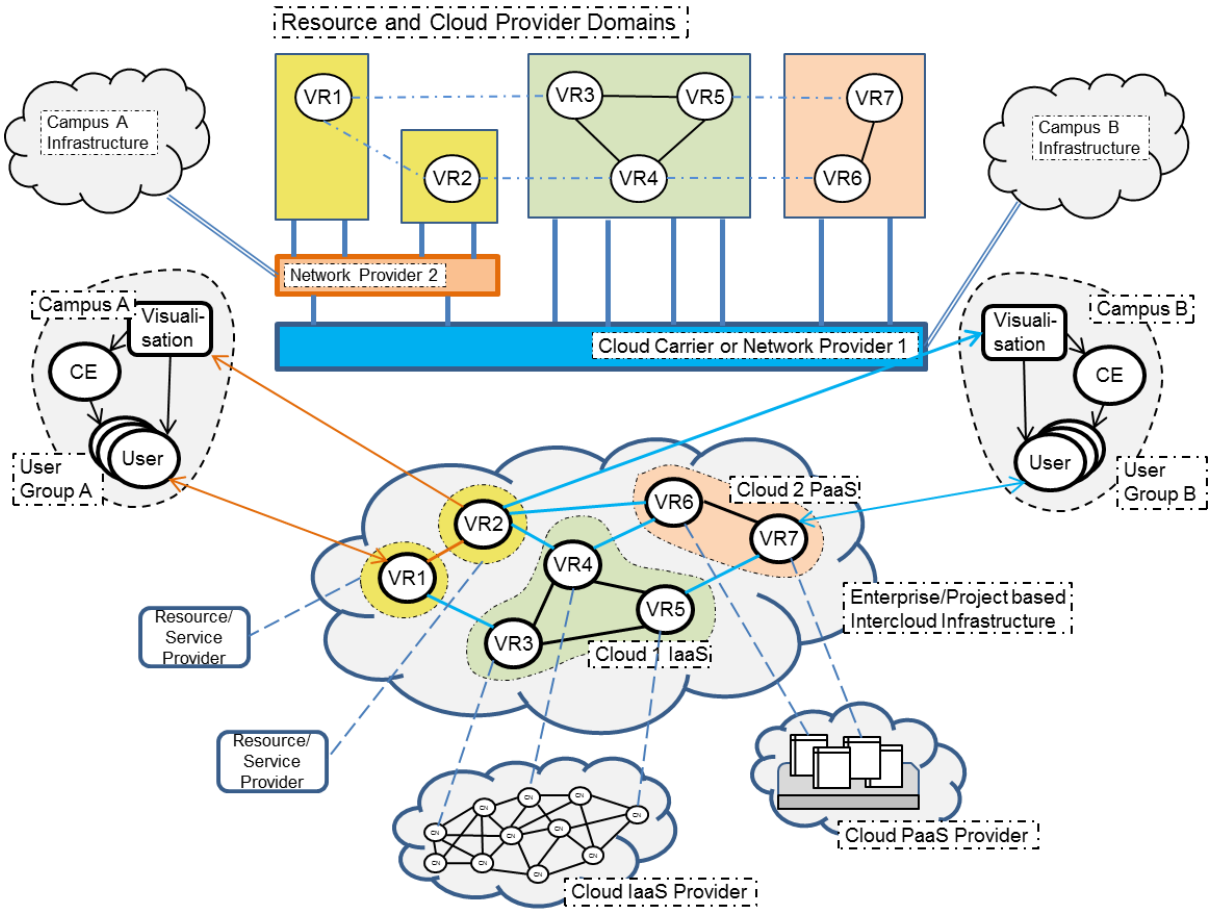

Figure C.2. Required network interconnecting infrastructure that can be provided either single Cloud Carrier or together with the regular network provider.

The figures also illustrates a typical case when two different types of cloud services such as IaaS and PaaS based need to interoperate to allow consistent hybrid cloud infrastructure control and management.

C.1.2 ICAF Definition

The proposed Intercloud Architecture should address the interoperability and integration issues in the current and emerging heterogeneous multi-domain and multi-provider clouds that could host modern and future critical enterprise and e-Science infrastructures and applications, including integration and interoperability with legacy campus/enterprise infrastructure.

Following the above requirements, we define the following complimentary components of the proposed Intercloud Architecture:

(1) Multilayer Cloud Services Model (CSM) for vertical cloud services interaction, integration and compatibility that defines both relations between cloud service models (such as IaaS, PaaS, SaaS) and other required functional layers and components of the general cloud based services infrastructure. It is important to admit that CSM defines a dedicated Layer 6 “Access and Delivery Infrastructure” that interconnects cloud provider datacenter or Point of Presence (POP) and customer/user location and infrastructure including also federated infrastructure components.

(2) Intercloud Control and Management Plane (ICCMP) for Intercloud applications/infrastructure control and management, including inter-applications signaling, synchronization and session management, configuration,

monitoring, run time infrastructure optimization including VM migration, resources scaling, and jobs/objects routing.

(3) Intercloud Federation Framework (ICFF) to allow independent clouds and related infrastructure components federation of independently managed cloud based infrastructure components belonging to different cloud providers and/or administrative domains; this should support federation at the level of services, business applications, semantics, and namespaces, assuming necessary gateway or federation services.

(4) Intercloud Operation Framework (ICOF) which includes functionalities to support multi-provider infrastructure operation including business workflow, SLA management, accounting. ICOF defines the basic roles, actors and their relations in sense of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF.

(5) Intercloud Security Framework (ICSF) that provides a basis for secure operation of all components of the Intercloud infrastructure. In this respect ICSF should provide a basis for integration of the security services between different CSM layers and all participating cloud service providers.

The following sections provide more information about the Cloud Services Model and Intercloud Federation Framework definition. ICCMP definition have been done and implemented as a part of the GEYSERS project [21, 26] that ??? The ICOF definition will include analysis of the TeleManagement Forum (TMF) documents related to eTOM and Operational Support Systems [22], Service Delivery Framework (SDF) [23].ICOF will also incorporate and leverage existing technologies related to SLA management and SLA based services provisioning [24], including also Web Services Agreement (WSAG) negotiation protocol [25].

C.1.3 Multilayer Cloud Services Model (CSM)

Figure C.3 illustrates the CSM layer definition and related functional components in a typical cloud infrastructure. It shows that the basic cloud service models IaaS, PaaS, SaaS that expose in most cases standard based interface to user services or applications but actually use a proprietary interface to the physical provider platform. In this respect the proposed model can be used for the inter-layer interfaces definition.

In the proposed Intercloud layered service model the following layers are defined including user client or application at the top (numbering from bottom up, see Fig. C.3):

(C6) User/customer side resources and services

(C5) Access/Delivery infrastructure hosting components and functions to provide access to cloud services/resources and interconnect multiple cloud domains

(C4) Cloud services layer that may include different type of cloud services IaaS, PaaS, SaaS

(C3) Cloud virtual resources composition and orchestration layer that is represented by the Cloud Management Software (such as OpenNebula, OpenStack, or others)

(C2) Cloud virtualisation layer (e.g. represented by VMware, Xen or KVM as virtualisation platforms)

(C1) Physical platform (PC hardware, network, and network infrastructure).

Note. Layer acronyms use prefix “C” to denote their relation to clouds.

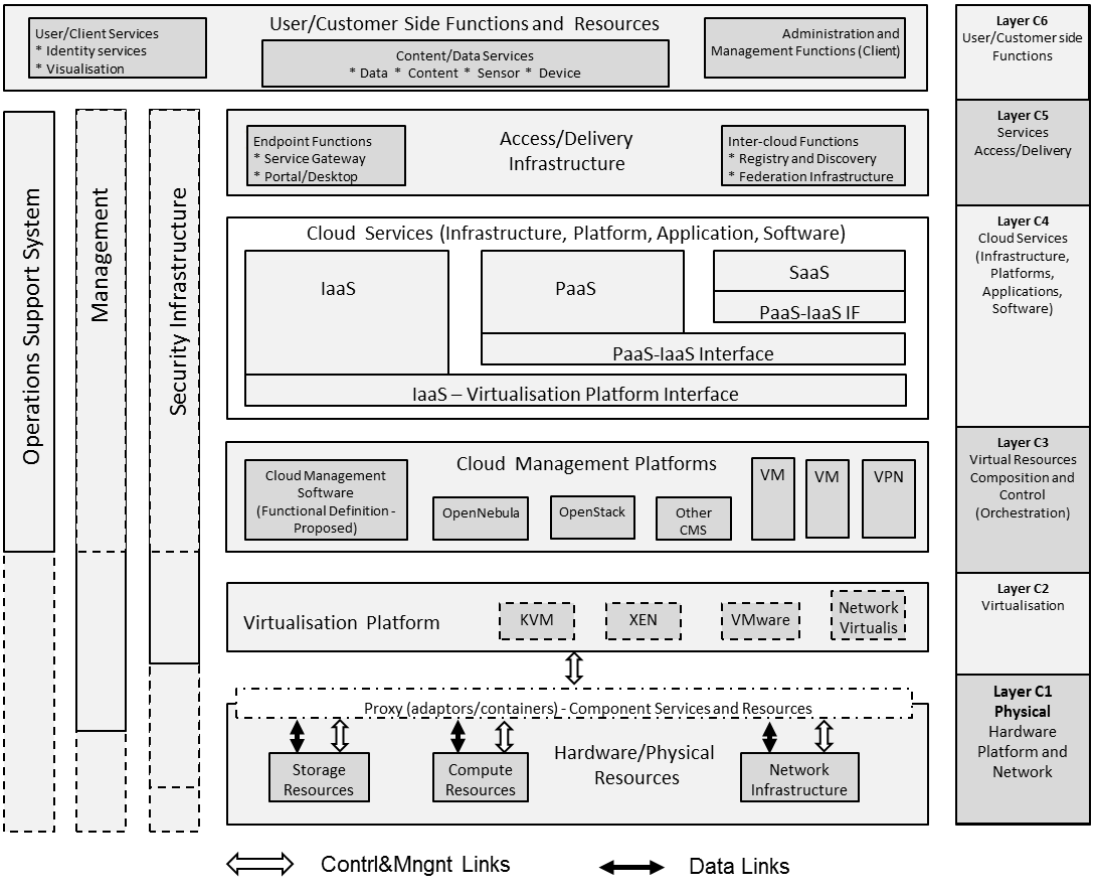

Figure C.3. Reference Multilayer Cloud Services Model (CSM).

The OCX introduction contributes to the definition of and justifies the need for well-defined Intercloud Access and Delivery Infrastructure (ICADI) positioned as is a functional Layer 5 Services Access and Delivery. The main ICADI functionality includes:

- Services to support connectivity between potentially multiple Cloud Service Providers/locations and also potentially multiple Customer locations.
- Dedicated network infrastructure that may be required to be transparent to generic cloud services and protocols
- Infrastructure and services for federated services operation and access control, including Federated Identity Management
- ICADI may delivered as a Cloud Carrier service which typically fits the traditional telecom operators business model. This can be also a business and operational domain for NRENs (what is presumed in this document)
- Presumably can be implemented as the Open Cloud eXchange (OCX) discussed in this document. Actually OCX can provide collapsed ICADI functions as a place for interconnection between cloud providers and customers.

C.1.4 Intercloud Federations Framework (ICFF)

C.1.4.1 *Roles and Actors*

We define the following main actors and roles adopting the Resource-Ownership-Role-Action (RORA) model proposed in [19]:

- Cloud Service Provider (CSP) as entity providing cloud based services to customers, on their request and based on the business agreement that is expressed as Service Level Agreement (SLA). We need to admit specifics of business relation in clouds due to the fact that majority of cloud services are self-services and they are governed under general or individualized SLA.
- Cloud Broker is an entity that may play a role of the third party in offering cloud service adding value of negotiating with many CSPs or customer groups and in some cases managing complex multi-provider services.
- Cloud Service Operator and/or Integrator is a new emerging role of the company that provides a value added service of integrating services from multiple cloud providers and delivering them to the customer.
- Customer is an entity that requests cloud services. In a simple case, customer may be an end-user of the requested services, or in more general case, may be an organization (enterprise or university) that requests cloud based services for the members of their organisations and manages these services.
- User is an end-user consuming cloud based services; in cloud services provisioning model an end-user may be also a customer.

Other roles such as Cloud Carrier and Cloud Auditor are defined in the NIST standards [1].

Typically, federation membership is managed by IDP hosted by customer or user home organization. In case of the dynamic federation that can be initiated by the user, a new IDP will be created as a part of the provisioned cloud based infrastructure. The following are assumption about what basic services and mechanism the new dynamically created IDP will possess or inherit:

- Instantiated from the CSP IDP and by creation is federated with the other user IDP's where user is a member;
- The created dynamic trust federation will use the dynamic IDP as a trust proxy or a broker in case if user processes run across multiple CSP resources or services.

C.1.4.2 *Customer side and Provider side Federations*

We define the two general use cases for federating cloud resources on the provider side or creating federated multi-provider infrastructures and services to deliver federated cloud services to the customer.

Figure C.4 illustrates two cases when (a) cloud based services and/or infrastructure needs to be integrated/federated with the existing user accounts and enterprise infrastructure, or (b) or cloud based public services can use external IdP and in this way already existing user accounts with the single or multiple 3rd party IDP (such as Google+/GooglePlay, Facebook, Microsoft, or other open IDP).

Figure C.5 illustrates the major actors and their relation in the provider side federation to share and outsource cloud resources when providing a final service to the customer.

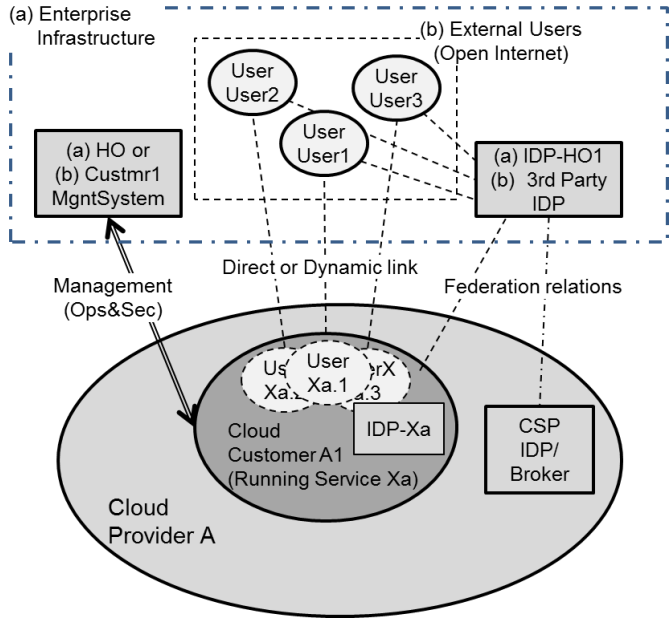

Figure C.4. Customer/user side federation for delivery of the federated cloud services to enterprise customers.

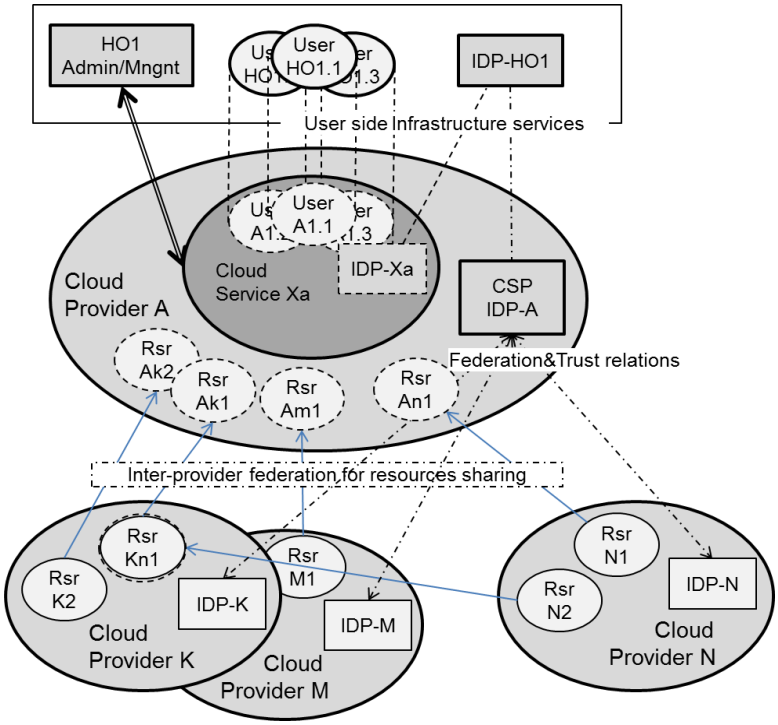

Figure C.5. Provider side federation for resources sharing and outsourcing

C.1.4.3 *ICFF Components and Operation*

ICFF defined in [18] allows clouds from different administrative domains to from a federation. The federation allows for end-users to access cloud services from multiple domains without need to obtain a separate identity, while services remain under control of their original operator or home provider.

The Intercloud Federation Framework is responsible for coordinating allocation of resources in a unified way. Figure C.6 illustrates the main components of the federated Intercloud Architecture, specifically underlying the Intercloud gateway function (GW) that provides translation of the requests, protocols and data formats between cloud domains. At the same time the federated Intercloud infrastructure requires a number of functionalities, protocols and interfaces to support its operation:

- Trust and service broker
- Service Registry
- Service Discovery
- Identity provider (IDP)
- Trust broker manager

The following federation related issues must be addressed in the further ICFF definition:

- Federation, delegation and trust management
- Single Sign On (SSO) and session credentials management
- Attributes management in federations, attributes validation , mapping and translation
- Federation governance, including federation lifecycle management.

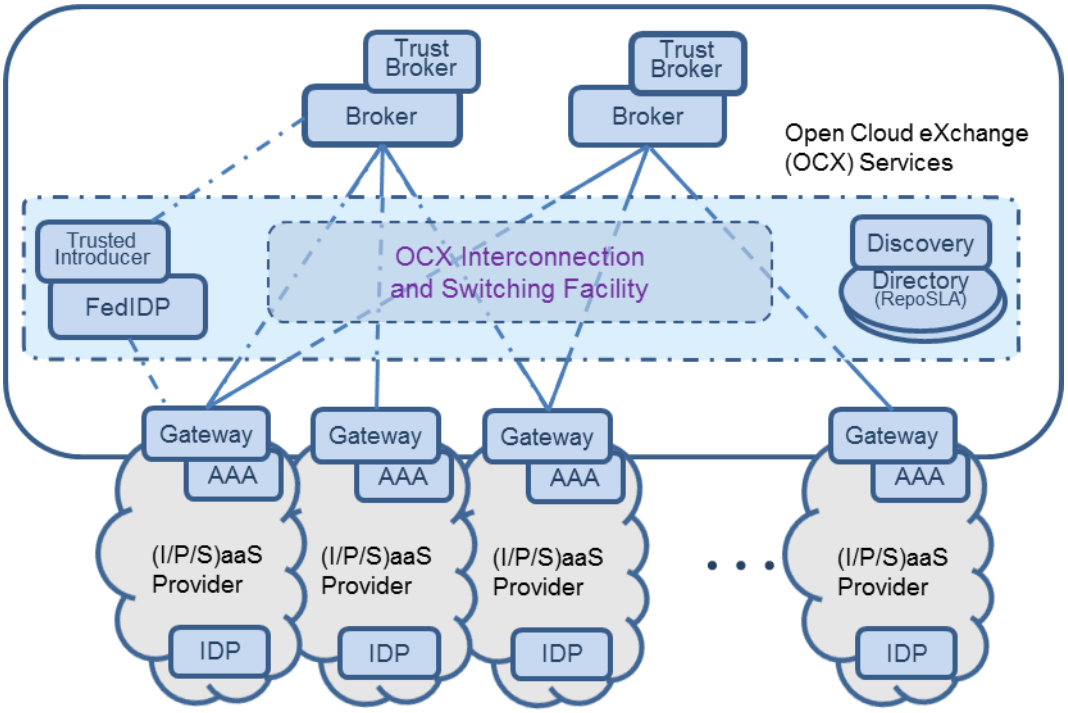

Figure C.6. Intercloud federation infrastructure.

C.2 IEEE P2302 Intercloud Interoperability and Federation Working Group and Intercloud Testbed Initiative

Information to be provided

C.3 ITU-T JCA-Cloud

Include if information available