Open Cloud eXchange (OCX): Architecture and Functional Components

Yuri Demchenko, Jeroen van der Ham, Canh Ngo, Cees de Laat
University of Amsterdam
Amsterdam, The Netherlands
e-mail: {y.demchenko, jvdh, t.c.ngo, C.T.A.M.deLaat}@uva.nl

Eduard Escalona
I2CAT, Barcelona, Spain
e-mail: eduard.escalona@i2cat.net

Taras Matselyukh
Opt-Net BV, Amsterdam, The Netherlands
e-mail: tmatsely@opt-net.eu

Sonja Filiposka
Ss. Cyril and Methodius University in Skopje
Skopje, FYR Macedonia
e-mail: sonja.filiposka@finki.ukim.mk

***Abstract*— This paper presents the concept of Open Cloud eXchange (OCX) that has been proposed to bridge the gap between two major components of the cloud services provisioning infrastructure: Cloud Service Provider (CSP) infrastructure; and 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 interconnecting the CSP infrastructure and local access network infrastructure, in particular, to solve the "last mile" problem in delivering cloud services to customer locations and individual (end-)users. The OCX remains 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 GÉANT network, or jointly, and provides suggestions about OCX implementation. The proposed OCX concept will leverage the existing Internet eXchange (IX) and GLIF Open Lightpath Exchange (GOLE) solutions and practices, 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. The paper also describes trusted/secured topology exchange protocol and dynamic trust establishment protocol as a part of the OCX services.**

Keywords- Intercloud Architecture Framework (ICAF); Open Cloud eXchange (OCX), Intercloud Federations Framework, Dynamic Trust Establishment.

I. INTRODUCTION

The use of cloud based services and Cloud Computing [1, 2] technologies in general among universities and by research community 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.

The provisioned cloud based infrastructure services may involve multi-provider and multi-domain resources, including integration with legacy services and infrastructures. Current development of the cloud technologies demonstrates movement to developing Intercloud models, architectures and integration tools that could allow integrating cloud based infrastructure services into existing enterprise and campus infrastructures [3, 4], on one hand, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualised cloud environment [5], on the other hand.

Currently, National Research and Education Networks (NREN) 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. There is a clear need for technologies consolidation to address performance and manageability issues in combined cloud and service delivery infrastructure for project oriented collaborations.

In many cases large Cloud Service Providers (CSP) 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 NREN's at national level. This approach can be also used at the European Research and Education network GÉANT what would simplify cloud services delivery for European wide projects and communities.

This paper proposes a new concept and a new functional component of the general inter-cloud infrastructure, namely the Open Cloud eXchange (OCX). OCX intends to bridge the gap between the two major components of the cloud services infrastructure: (1) Cloud Service Provider (CSP) infrastructure that typically has a global footprint and is intended to serve the global customer 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 presented paper provides information for discussing 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 paper refers to the general Intercloud Architecture Framework (ICAF) proposed in the earlier authors' work as a result of cooperative efforts in a number of EU funded projects such as GÉANT3 [6] and GEYSERS [7] and currently being submitted as an Internet-Draft to IETF [8]. The proposed OCX

is positioned as an important infrastructure component of the Intercloud Federation Framework (ICFF) [9].

The remainder of the paper is organized as follows. Section II provides overview and analysis of the general use cases for cloud use by universities and NRENs. Section III defines the main OCX functionalities that combine both network connectivity and Trusted Third Party services: this section also specifies the general requirements to OCX. Section IV summarises requirements and defines the main components of the proposed Intercloud Architecture. Section V provides design suggestions for implementation and deployment of the OCX architecture components. Section VI provides suggestions for OCX design validation and modeling. Related works are discussed in section VII, and the paper concludes with the future developments in section VIII.

II. General Cloud Use Cases for Universities and NREN's

This section describes typical cloud use by universities and research community that motivates a need for the dedicated delivery infrastructure for cloud services to support advanced research at universities and other research organisations.

We also refer to the general use cases and usage scenarios defined by industry and documented by NIST [10], Open Data Center Alliance (ODCA) [11], and Global InterCloud Technology Forum (GICTF) [12], however focus on the specific uses of cloud based services by the education and research organisations.

A. Clouds use by universities

The following lists the typical 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 Gmail by Google. Gmail allows email accounts consolidation and has benefit of the global accessibility which is the most important for mobile research community.
- Storage services are very popular both for backup purposes and for sharing documents and data, which 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 been developing secure cloud storage sponsored by the TF-Storage [13].
- CloudApps services such as Google Apps are quite popular both among researchers and students. CloudApps allow easy construct of a necessary computational task using available functionalities in order to obtain necessary modelling results [14].
- Many general and specialist software applications are provided as Software as a Service (SaaS). Examples of such services include scientific software and applications, such as innogetCloud, Cloudera, GenomeQuest. Most of the examples are either migrated to the cloud or custom built upon the PaaS service model.
- 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.
- 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.
- 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 does not require any specific network services. However advanced research requires 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.

B. Basic 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.

III. Open Cloud Exchange (OCX) definition and general requirements

The Open Cloud eXchange (OCX) is proposed to address the currently existing problems in delivering cloud services to organisational/enterprise customers and end users.

A. Basic OCX Functionality

The proposed OCX concept is based on and extends the Internet eXchange Points (IXP) [15] and GLIF Optical Lightpath Exchange (GOLE) [16] service models with additional functionalities to allow ad hoc dynamic Intercloud federation establishment and non- restricted peering between cloud providers, customers, and also local infrastructure providers, in case cloud services delivery requires involvement of such entity.

Besides providing physical location for interconnecting (network) of all 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 provisioning and 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 and establishment of dynamic trust relation. As a part of membership service, 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) [17].

Referring to the generic Cloud Services Model (CSM) defined in [3, 8] as a part of the Intercloud Architecture Framework (ICAF), the OCX functionality can be related to the Intercloud Access and Delivery Infrastructure (ICADI) layer where the main goal is to deliver cloud based services to organisational customers and end users. Structurally ACADI includes all infrastructure components between the CSP, the final consumer and other entities involved into cloud services delivery and operation. However, to allow easy integration into existing cloud infrastructures and remain transparent to current service models, the OCX may limit its services to Layer 0 through Layer 2 transport networks.

The introduction of the OCX TTP service intends to support the federated cloud and inter-cloud service provisioning that simplifies heterogeneous multi-provider services integration and operation. In this respect the OCX will provide important functionality related to the Intercloud Federation Framework (ICFF) [4, 9].

B. Requirements to OCX

The general requirements to OCX functionality and its design follow from the basic use cases and scenarios analysis:

1) Generally, the OCX should follow and leverage the Internet eXchange design and operational principle adopted to support the specifics of 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 handle significant amount of their own and customers' traffic through internal network infrastructure which is not necessarily TCP/IP protocol based.

OCX may also benefit from being collocated with the collocation service provider, NREN exchange points or regional data center servicing regional/national research community.

2) Primarily, the OCX should provide the Layer 0 through Layer 2 network services [18] to interconnect CSP Points of Presence (PoP) remaining 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 consequently OCX services at the lower networking 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 (cross/inter)connection network infrastructure must guarantee high QoS parameters such as 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 are not limited to:

- Trusted introducer service that can be supported by the Trusted Certificates Repository (similarly to TACAR service by TERENA [17] or formerly used Trust Anchor Repository (TAR) service for DNSSEC by ICANN [19].
- 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 GÉANT.

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

IV. THE PROPOSED OCX ARCHITECTURE AND COMPONENTS

Figure 1 below illustrates the general case of implementing an enterprise or scientific workflow which is mapped to the heterogeneous multi-provider infrastructure that includes cloud based services, specialist services/instruments, and network service providers. OCX placed between customers/campuses and cloud providers will provide facilities for interconnecting all members and entities of the federated cloud infrastructure.

As illustrated in Figure 1, the OCX services can be provided by the Cloud Carrier or Network Provider, in particular NREN or GÉANT.

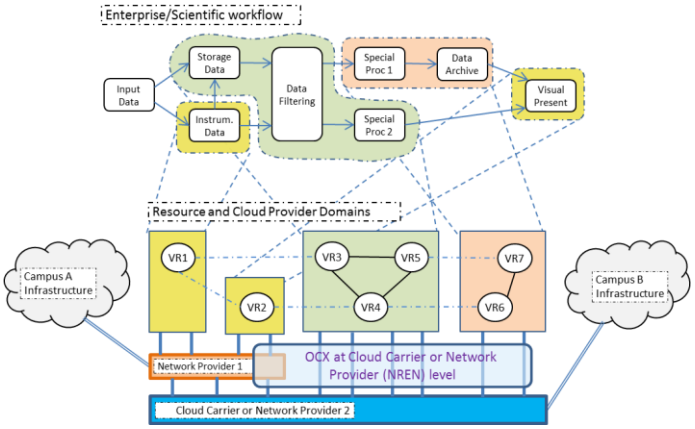

Figure 1. OCX at Cloud Carrier or Network Provider level.

Architecturally and functionally, the OCX includes the following services and functional components (see Fig 2):

- 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 is 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 be provided and 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.

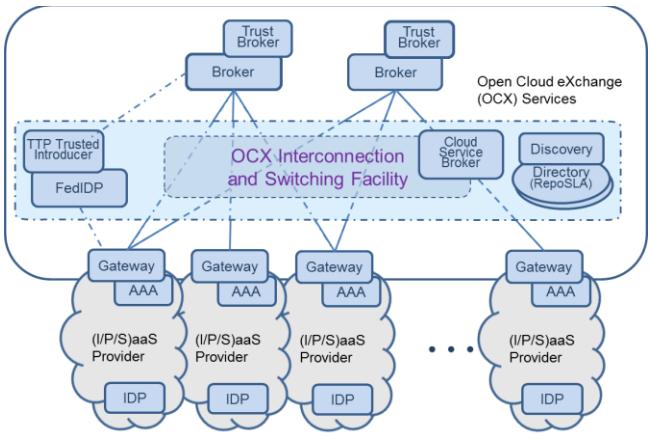

Figure 2. OCX functional component (as part of the Intercloud federation infrastructure)

V. OCX Design and Implementation

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

A. OCX interconnection network and peering design

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

This can be implemented by using corresponding L0-L2 optical switches. Figure 3 illustrates the switching topology of OCX.

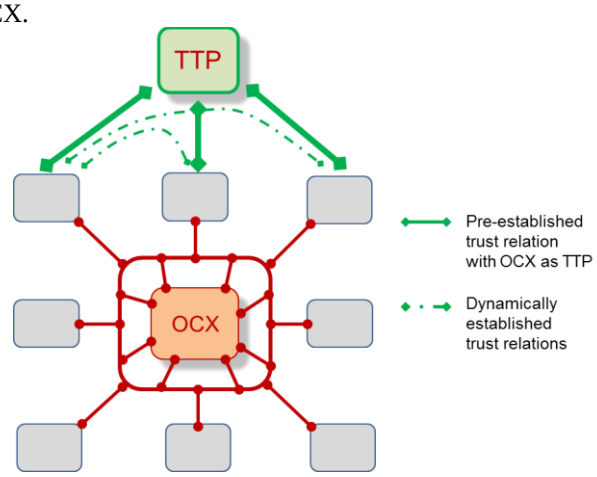

Figure 3. OCX interconnection capability and TTP role in establishing dynamic trust relations between OCX members

B. 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.

The OCX trust model can contain a TTP for all members, which stores their trust anchors like a trusted certificated repository in TACAR [17]. Relationships between unknown members can depend on the trust threshold values determined from other existing relationships as proposed in [20]. It is recommended that members need to have trust policies to define such criteria.

C. OCX implementation Models

We consider different options for OCX location: at NREN's, at GÉANT premises and combined versions with hierarchical OCX infrastructure and extended OCX backplane/backbone. Figure 4 illustrates the basic options with single OCX located at GÉANT or NREN premises, also showing a possibility of building extended OCX switching capability by direct interconnection of two OCX in different locations.

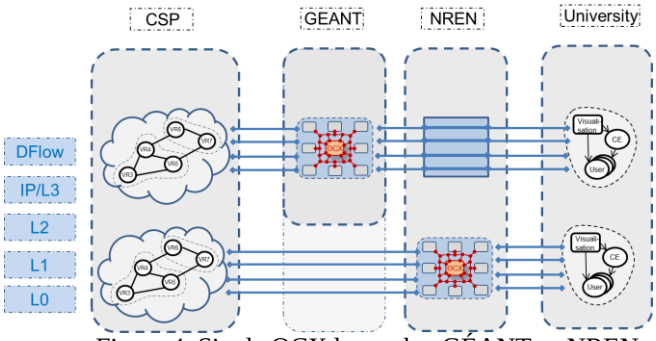

Figure 4. Single OCX located at GÉANT or NREN premises: single OCX.

On the other hand, Figure 5 illustrates hierarchical OCX architecture where OCXs located at the Trans-European/ GÉANT 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.

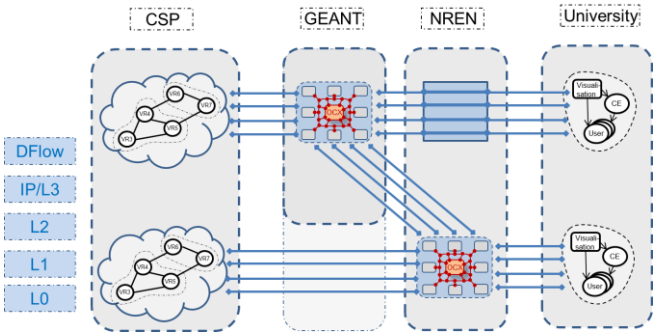

Figure 5. Single OCX located at GÉANT or NREN premises: hierarchical.

D. 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 features such as routing, data filtering, policy enforcement, TTP

services, etc. A modular implementation of this SDN controller such as the one offered by Floodlight [21] or even an implementation using the Network as a Service (NaaS) concepts developed by frameworks like OpenNaaS [22] provide the flexibility and extensibility that allow an easy adaptation of interconnectivity requirements.

VI. OCX Design Validation and Modelling

Design validation and functionality modeling is an important stage in the new infrastructure service development and future roll-out. This should allow for checking the effectiveness of the proposed solutions and selecting the optimal characteristics of selected functional components and hardware.

The minimum set of requirements for the OCX validation testing are:

- Availability and resiliency of the service in the case of network and equipment outages,
- Separation (segmentation) of the traffic,
- Assured delivery of the traffic with required service level guarantees,
- Sustainability of the service levels in the peak use scenarios (scalability),
- Security and protection of the data as it traverses the network (confidentiality),
- Protection from the denial of service attacks (resiliency),
- Reliability of the transmissions and resistance to Denial of Service attacks.

Preliminary assessment of the functionality provided by the popular network simulation tool OMNET++ [23] revealed that it can be successfully used at the design stage for the OCX simulated testing instead of building dedicated network prototype solution test-bed. This approach allows balancing the fidelity of the simulation tests against the cost and duration of the testing. Main reasons behind this decision are the costs of the required networking equipment and long delivery times for such equipment, as well as lack of our ability to influence the software road-map development from the leading telecommunication equipment vendors in the required period of time. The consistent OCX simulation model will also provide a basis for future SDN components implementation.

The following steps need to be performed before starting the validation testing:

1) Identify, describe and categorize the needs of the most likely applications which are going to be used by the NREN users and universities, in terms of technical key performance indicators (KPIs);

2) Define the realistic all-encompassing use cases for each application;

3) Define the OCX functional architecture and functional requirements;

4) Identify the L1 and L2 networking technology, which is best suited to deliver the user traffic in a compatible manner with the OCX delivery models that will be compliant with the functional requirements;

5) Build the simulation test-bed environment and develop the new software models and components for the OCX system, which will perform functions defined in the functional architecture and existing standards;

6) Performance or scalability testing in computer simulated test bed.

The software tools may have limitations and hidden quality issues which might delay or prevent the full execution of the project plan. In order to mitigate such risks, we propose to make use of the open-source based network modelling tools that would allow both integrating new component models and use improved models for creating necessary SDN software modules.

VII. Related works

The proposed OCX architecture and service model is built upon such successful services as Internet Exchange (IX) [15] for general Internet traffic exchange and GOLE (GLIF Open Lightpath Exchange) [16] providing lightpath interconnection service. In the following we provide a short reference to the GOLE and review some works related to other OCX functionality.

A. The GLIF Automated GOLE Pilot Project

GLIF exchange points have been proposed to make global optical networking possible and allow multi-domain lightpaths connections. These exchange points typically work on a lower layer than common Internet Exchanges, since they typically connect users on layers lower than L2.

Since the start of GLIF, inter-domain lightpath provisioning has involved much manual processing and actions. Current automated GOLE implementation makes use of the Network Services Interface [24] developed by Open Grid Forum (OGF).

The Automated GOLE test bed interconnects thirteen different GOLEs, spanning over a dozen timezones, using five different implementations of the NSI Connection Service. The end-to-end/multi-domain lightpath is created and destroyed within seconds.

B. Related research

In this section we provide reference to the related works and technologies that can be used to support security federations and federated access control in clouds.

Amazon Direct Connect [25] provides dedicated network connectivity from customers sites to Amazon web services (e.g. EC2, S3, VPC, DynamoDB) to replace regular public internet access and VPN connections, which could handle large data sets and real-time data feeds. It is available directly at AWS Direct Connect Locations or via other network partners. The service can be provisioned on-demand without setup charges. Its price model is based on virtual port usages and volume of data transfer.

Moonshot Project [26] that develop a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures and other commonly deployed services including mail, file store, remote access and instant messaging. Moonshot project implements the technology developed by the IETF Working Group Application Bridging for Federated Access Beyond web (ABFAB) [27].

The OpenStack KeyStone project [28] provides Identity, Token, Catalog and Policy services for use specifically by projects in the OpenStack family. We consider it as candidate

platform for OCX TTP implementation that can also integrate solutions proposed in the research work by the University of Kent [20] and also integrate the authors' earlier works on trust establishment trust based policy evaluation [29] and trust bootstrapping protocol [30].

VIII. Conlusion and Future Developments

This paper presents an on-going research and development as a part of the Joint Research Activity JRA1 in the GN3plus project conducted by a group of cooperating universities and NRENs to develop the Open Cloud eXchange (OCX) – a new service and component of the Intercloud Architecture that addresses problems with multi-domain heterogeneous cloud based applications integration and inter-provider and inter-platform interoperability.

Current stage of development concludes the OCX architecture and functionalities definition, specification of requirements and design suggestions. Further steps will include design validation, definition of APIs (including required new protocols) and creation of the test bed between participating NRENs and universities.

The future research will be focused on defining the Trusted Introduction Protocol for the Dynamic Secure Federations establishment using OCX TTP services. The intended solution will review the solutions being developed by the ABFAB WG at IETF [27, 31], works by the University of Kent [20] and the University of Amsterdam [29, 30].

OCX intends to provide a basis to support cloud based collaborative infrastructure for emerging new applications, in particular Big Data infrastructure for universities and research organisations.

The proposed approach and definitions are intended to provide an input to standardisation activities in the area of Intercloud architecture and services. The authors are actively contributing to a number of standardisation bodies, in particular, the Open Grid Forum NSI-WG, NML-WG and Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [32].

Acknowledgements

This work is supported by the FP7 EU funded Integrated project GN3plus.

References

[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] 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

[4] 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.

[5] 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.

[6] GEANT Project. [Online] http://www.geant.net/pages/home.aspx

[7] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project). [Online] http://www.geysers.eu/

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

[9] 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.

[10] 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

[11] Open Data Center Alliance (ODCA) http://www.opendatacenteralliance.org/

[12] Global Inter-Cloud Technology Forum (GICTF), Use Cases and Functional Requirements for Inter-Cloud Computing, GICTF White Paper. August 9, 2010 - http://www.gictf.jp/doc/GICTF_Whitepaper_20100809.pdf

[13] TERENA TF Storage. [online] http://www.terena.org/activities/tf-storage/

[14] Google Apps. [online] http://www.google.com/apps/intl/en-GB/edu/

[15] 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

[16] The GLIF "Automated GOLE Pilot" Project. http://staff.science.uva.nl/~delaat/sc/sc10/GLIFAutomatedGOLEPilot.SC.pdf

[17] TERENA Academic Certification Authority Repository. [online] https://www.tacar.org/

[18] Advanced Network Services [online] http://internet2.edu/network/services

[19] DNSSEC Trust Anchor Repositories (TAR), Update, by Russ Mundy http://dakar42.icann.org/node/21557

[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] Floofligh OpenFlow SDN Controller [online] http://www.projectfloodlight.org/floodlight/

[22] OpenNaaS: Open platform for Network as a Service resources [online] http://www.opennaas.org/

[23] OMNeT++ Network Simulation Framework [online] http://www.omnetpp.org/

[24] GFD.173 Network Services Framework v1.0, OGF Standard [online] http://www.gridforum.org/documents/GFD.173.pdf

[25] Amazon Direct Connect service [online] http://aws.amazon.com/directconnect

[26] Moonshot Project [online] https://community.ja.net/groups/moonshot

[27] IETF Application Bridging for Federated Access Beyond web (Active WG) [online] http://tools.ietf.org/wg/abfab/

[28] Keystone, the OpenStack Identity Service! [online] http://docs.openstack.org/developer/keystone/

[29] 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

[30] Membrey, P., K.C.C.Chan, C.Ngo, Y.Demchenko, C. de Laat, Trusted Virtual Infrastructure Bootstrapping for On Demand Services. The 7th International Conference on Availability, Reliability and Security (AReS 2012), 20-24 August 2012, Prague.

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

[32] 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