Open Cloud eXchange (OCX): Bringing Cloud Services to NRENs and Universities

Yuri Demchenko, Jeroen van der Ham, Cees de Laat University of Amsterdam {y.demchenko, jvdh, t.c.ngo, strijkers, C.T.A.M.deLaat}@uva.nl Taras Matselyukh Opt-Net BV tmatsely@opt-net.eu

Eduard Escalona I2CAT e-mail: eduard.escalona@i2cat.net Migiel de Vos SURFnet migiel.devos@surfnet.nl Sonja Filiposka Ss. Cyril and Methodius University in Skopje sonja.filiposka@finki.ukim.mk Tasos Karaliotas GRNET karaliot@noc.grnet.gr Alex Mavrin Apteriks alex@apteriks.com Damir Regvart CARNET damir.regvart@carnet.hr Kurt Baumann SWITCH kurt.baumann@switch.ch Daniel Arbel IUCC dani@noc.ilan.net.il Tony Breach NORDUNET tony@nordu.net

Abstract— This paper presents the concept of Open Cloud eXchange (OCX) that has been proposed by the GN3plus JRA1 activity 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 limits its services to Layer 0 through Layer 2 to remain transparent to current cloud services model. 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. The presented paper describes the OCX concept, architecture, design and implementation options, and demo scenario being developed by the OCX development team.

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 technologies [1, 2] in general is expected to continue to increase among universities and research communities in the future. This rise will also be stimulated by the increasing demand for computational power of the emerging Data Intensive Science applications that require both advanced computing and networking infrastructure, as well as infrastructure to support collaborative groups [3].

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 wiling to extend their network to one of the CSP's POP. The

latter approach is becoming popular among National Research and Education Networks (NREN) at the national level. This approach can also be implemented at the European Research and Education network GÉANT and would simplify cloud services delivery for European wide projects and communities.

The Open Cloud eXchange (OCX) has been proposed by the GN3plus JRA1 activity as a new concept and a new functional component of the general inter-cloud infrastructure. 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 paper refers to the general Intercloud Architecture Framework (ICAF) [4, 5] 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 solution 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 summarizes 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 remarks on future development in section VIII.

II. CLOUD USE CASES FOR UNIVERSITIES AND NREN'S

Typical cloud use by universities and research community motivates the need for dedicated delivery infrastructure for cloud services in order to support advanced research and collaboration.

For the common cloud use cases we also refer to the general use cases and usage scenarios defined by the industry and documented by NIST [10]. The focus here is on the specific uses of cloud-based services by higher education and research organizations.

A. Clouds services in universities

The typical uses of cloud services by universities both at the level of departments and individually by the staff and students can be listed as follows:

- Outsourcing e-mail service to global providers (e.g. Gmail), which allows for email accounts consolidation and has benefit of global accessibility, which is of utter importance for the mobile research community.
- CloudApps services such as Google Apps are also very popular among researchers and students allowing transparent and intensified collaboration.
- Storage services (e.g. Box) for backup purposes, but also documents and data sharing, which are important services for intra- and inter-organizational collaboration support. Despite the existing security concerns these services are quite popular for common cases where data privacy is not critical. Also, the TERENA community has been developing secure cloud storage sponsored by the TF-Storage [11].
- Many general and specialized software applications are provided as Software as a Service (SaaS). Examples include scientific software and applications, such as innogetCloud, Cloudera, GenomeQuest. Most of these solutions are either migrated to the cloud or custom built upon the PaaS service model and allow a simplified construction of a necessary computational task using available functionalities in order to obtain necessary modelling results [12].
- The use of cloud Infrastructure as a Service (IaaS) services are prominently used by deploying multiple VMs that can be used for running user designed services and creating experimentation environments for newly developed infrastructure services and protocols.
- Increasing amount of scientific data is available to research community and collaborative groups in the form of Grid and cloud storage resources. Examples are LHC experiment data and genome data provided to researchers worldwide. Other scientific data repositories such as satellite data require more strict policy compliance.
- National and organizational data centers are increasingly providing access to High Performance Computing (HPC) as cloud services.

In most of the reviewed cases the cloud services are provided over the public Internet and do not require any specific network services. However, the advanced research activities require access to large datasets, specific scientific environments and HPC. Combining all these components into a collaborative scientific infrastructure requires a dedicated network infrastructure and related supporting services.

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 via a dedicated infrastructure:

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

III. OPEN CLOUD EXCHANGE (OCX) DEFINITION AND GENERAL REQUIREMENTS

In order to address the currently existing problems in delivering cloud services to organizational/enterprise customers and end users, in this paper we propose the Open Cloud eXchange (OCX).

A. Basic OCX Functionality

The proposed OCX concept is based on and extends the Internet eXchange Points (IXP) [13] and GLIF Optical Lightpath Exchange (GOLE) [14] 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 entities.

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

- No third party services (i.e. service brokering, integration or operation). In this way, OCX will not be involved in the business dealings related to the actual cloud services provisioning and delivery;
- Trusted Third Party (TTP) services for ad-hoc/dynamic federations establishment: OCX may provide the service of trusted repository, certificate provider and services directory operating under supervision of the community (representatives), which will act as policy authority for security and operational practices.

The proposed OCX role as a TTP will facilitate creation of dynamic federations and establishment of dynamic trust relation.

Referring to the generic Cloud Services Model (CSM) defined in [4, 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 organizational customers and end users. Structurally ICADI

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 limits 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 OCX will provide important functionality related to the Intercloud Federation Framework (ICFF) [4, 9].

B. OCX requirements

The general OCX functional requirements and its design are derived from the basic use cases and scenarios analysis:

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

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

2) Primarily, OCX should provide Layer 0 through Layer 2 network services [16] to interconnect CSP PoPs remaining fully transparent to current cloud services models that generally use Layer 3 network infrastructure virtualization for VM deployment and interconnection.

The OCX (cross/inter)connection network infrastructure must guarantee high QoS parameters. However, further performance optimization for cloud infrastructure may require Layer 2 network virtualisation and consequently OCX services at the lower networking layers.

The topology information exchange between the OCX peering members should be considered as an important component/requirement in order to provide effective services interconnection at different networking layers.

3) OCX should support smooth service delivery and integration between CSP and customers, which apart from the high QoS network connectivity may also include support for federated services integration and operation. These services can be generally defined as Trusted Third Party Services (TTP).

4) OCX architecture should provide a flexible operational scenario operated by NREN's and GÉANT. When implemented using modern optical network technologies (e.g. Lambda and DWDM), OCX can be realized using different distributed topological models: extended, collapsed, or hierarchical.

IV. OCX ARCHITECTURE AND COMPONENTS

Figure 1 given below illustrates the general case of implementing an enterprise or scientific workflow mapped over heterogeneous multi-provider infrastructure that includes: cloud infrastructure segments IaaS (VR3-VR5) as well as PaaS (VR6, VR7), separate virtualized resources or services (VR1, VR2), two interacting campuses A and B, and a network infrastructure that in many cases may need to use

dedicated network links for guaranteed QoS. The OCX placed between customers/campuses and cloud providers will provide facilities for interconnecting all members and entities of the federated cloud infrastructure.



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

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



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

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 dedicated optical links)
 - The associated service should allow topology information exchange between providers and customers in a secure and consistent way (this is of extreme importance since topology information in most cases is considered as commercial or restricted information)
- Trusted Third Party (TTP) services for support of 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.
- Optionally, Cloud Service Broker to provide service advice and integration for contracted community.

V. OCX DESIGN AND IMPLEMENTATION

OCX is currently entering the stage of network interconnection design. As a conceptually new component of the inter-cloud infrastructure, OCX will require definition of new service, control and management interfaces that should be integrated with the current cloud management services. This opens a possibility to use the basic SDN (Software Defined Network) design principles [17]. The data plane can be optimized for applying forwarding rules efficiently at any layer (L0-L2) while the SDN controller will implement features like routing, data filtering, policy enforcement, etc.

The OCX design team will also look into a possibility to use the Network Service Interface (NSI) [18] to control OCX connectivity services that is already used in the GEANT network. On the other hand, OCX management capabilities should allow their interaction with the emerging industry standard for cloud infrastructure services interoperability such as OASIS TOSCA (Topology and Orchestration Specification for Cloud Applications) [19].

The following provides suggestions 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 using corresponding L0-L2 optical switches. Figure 3 illustrates the switching topology of OCX, together with the TTP services operation model.



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 TTP 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, storing their trust anchors like a trusted certificated repository in TACAR [15]. 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 have trust policies that define such criteria.

C. OCX implementation Models

We consider different possibilities for the 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.



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 for cloud services. The OCXs operate independently using dedicated links for interconnection.



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

D. OCX SDN-based Design

The OCX characteristics require fast decision-making and policy enforcement mechanisms for transparent coordination of the cloud service transactions traffic. 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 efficiently applying forwarding rules 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

A. OCX 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 resilience of the service in the case of network and equipment outages,
- Separation (segmentation) of the traffic,
- Assured traffic delivery with the required service level guarantees,
- Service levels sustainability in the peak use scenarios (scalability),
- Security and protection of the data as it traverses the network (confidentiality),
- Transmission reliability and resistance to and protection from Denial of Service attacks (resilience).

Preliminary assessment of the functionalities provided by the popular network simulation tool OMNET++ [23] revealed that it can be successfully used during the design stage for the OCX simulated testing instead of building a dedicated network prototype solution test-bed. This approach balances the fidelity of the simulation tests against the cost and duration of the testing. The 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 foundation 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 using a 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 intent to use open-source based network modelling tools that would allow both integrating new component models and use improved models for creating necessary SDN software modules.

B. OCX Demonstration

In order to create a proof of concept demo that will highlight the benefits of using OCX, a simple test scenario has been defined. The aim of the proof of concept is to present how the OCX solution can provide a reusable network infrastructure that will deliver guaranteed QoS compared to the public Internet connection alternative.

The scenario is based on one of the main use cases that would benefit from dedicated connections to CSPs discussed earlier, in this particular case: HD video streaming and editing. The demo scenario is defined as follows: two institutions (A and B) would like to combine and edit several locally available HD video streams. The video combining is to be done on a cloud IaaS and storage provider (Okeanos) where a single HD video stream based on the separate videos will be created. The single combined stream is to be edited using image manipulation software available on a different cloud provider (Cloud Sigma). The result of the video combining and manipulation is to be sent to one of the participating institutions.

In a traditional approach using the public Internet for interconnecting to the cloud providers, after both of the institutions send the videos to the cloud storage, the resulting combined video has to be sent back over the Internet to one of the institutions that will subsequently send the video to the other provider that is to be used for video editing purposes, and receive it back again after it is done. All of the data transfers are done over the public Internet using the best effort approach without any QoS guarantees or special traffic isolation.

In the case of using OCX to implement the same scenario, as it is presented in Figure 6, the task can be solved much more efficiently. There are OCX boxes placed at the network providers (NRENs) for all interested parties (SURFnet, GRNET, and SWITCH), which are in turn directly connected to the customers and to the cloud providers. As illustrated, the interconnection between the customers and cloud providers is provided using multi-domain layer 2 services, which are established on demand between the OCX boxes using the underlying services offered by the GEANT network (e.g. bandwidth on demand). This means that, on network level, customers will gain dedicated access to a cloud service by establishing a layer 2 connection to their local OCX box, which will in turn connect them to the respective cloud provider via the GEANT network.



Figure 6. OCX demo scenario

The major benefit of the OCX infrastructure is the use of dedicated links towards the cloud providers that will substantially improve the data transfer performances between the institutions and the CSPs by completely mitigating the public Internet. The use of multi-domain L2 services ensures traffic isolation. Also, all already available layer 2 connections can be reused for future cloud service delivery. After the initial setup, the customers can use the provided cloud service transparently. Furthermore, since the connection to the cloud providers are done on layer 2 (or lower), the available cloud services can be easily expanded with more advanced features (e.g. extending the customer network into the cloud).

VII. RELATED WORK

The proposed OCX architecture and service model is built upon successful services like Internet Exchange (IX) [13] for general Internet traffic exchange and GOLE (GLIF Open Lightpath Exchange) [14] that provides 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 dozen time zones, 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 and unlike OCX uses layer 3 connectivity with BGP routing. Its price model is based on virtual port usages and volume of data transfer.

The Moonshot Project [26] develops 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 like mail, file store, remote access and instant messaging. The 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, 30] and trust bootstrapping protocol [31].

VIII. CONCLUSION AND FUTURE DEVELOPMENT

This paper presents an on-going research and development 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.

The current stage of development concludes the OCX architecture and functionalities definition, specification of requirements and design suggestions. The next steps will include design validation (in particular, modeling the OCX network infrastructure and operational model), API definition (including new required protocols) and creation of a testbed between participating NRENs and universities. OCX's role in facilitating integration of (multi-) provider and campus cloud infrastructures poses a number of security challenges, which

will also be analyzed at the next stage. These activities are planned in the framework of the GN3plus project for the period until September 2014.

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 organizations that should support data intensive research domains and applications like: particle physics LHC (Large Hadron Collider) experiments, SKA (Square Kilometer Array) astronomy observations, genomics, climate research, etc.

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

ACKNOWLEDGEMENT

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 238875 (GÉANT).

REFERENCES

- 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-cloudcomputing/pub/CloudComputing/ReferenceArchitectureTaxonomy/N IST_SP_500-292_-090611.pdf
- [3] The Adoption of Cloud Services. TERENA. ASPIRE Report, September 2012. http://www.terena.org/publications/files/ASPIRE %20-%20The%20Adoption%20of%20Cloud%20Services.pdf
- [4] 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
- [5] Demchenko, Y., C.Ngo, C. de Laat, J.A.Garcia-Espin, S.Figuerola, J.Rodriguez, L.Contreras, G.Landi, N.Ciulli, Intercloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand. The 2nd Intl Workshop on inter-Clouds and Collective Intelligence (iCCI-2013). The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA2013). 25-28 March 2013. ISBN-13: 978-0-7695-4953-8.
- [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 0.6, January 4, 2013. [online] http://www.ietf.org/id/draft-khasnabish-cloudreference-framework-06.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/wpcontent/uploads/2012/05/sp800-146.pdf
- [11] TERENA TF Storage. [online] http://www.terena.org/activities/tfstorage/

- [12] Google Apps. [online] http://www.google.com/apps/intl/en-GB/edu/
- [13] 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-internetexchange-points-guide-policy-management-and-technical-issues
- [14] The GLIF "Automated GOLE Pilot" Project. http://staff.science.uva.nl/~delaat/sc/sc10/GLIFAutomatedGOLEPilot .SC.pdf
- [15] TERENA Academic Certification Authority Repository. [online] https://www.tacar.org/
- [16] Advanced Network Services [online] http://internet2.edu/network/services
- [17] OFELIA and GÉANT Cooperation on OpenFlow Experimental Facilities. Posted 22 August 2013. [online] http://www.fp7ofelia.eu/news-and-events/press-releases/ofelia-and-gEantcooperation-on-openflow-experimental-facilities/
- [18] GFD.173 Network Services Framework v1.0, OGF Standard [online] http://www.gridforum.org/documents/GFD.173.pdf
- [19] Topology and Orchestration Specification for Cloud Applications, Version 1.0. Candidate OASIS Standard. 11 June 2013. [online] http://docs.oasis-open.org/tosca/TOSCA/v1.0/TOSCA-v1.0.html
- [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] Demchenko, Y., C.Ngo, C. de Laat, T.Wlodarczyk, C.Rong, W.Ziegler, Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services, Proc. 3rd IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2011), 29 November - 1 December 2011, Athens, Greece. ISBN: 978-0-7695-4622-3
- [30] 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
- [31] 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.
- [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

VITAE

Yuri Demchenko received his M.Sc. degree and later Ph.D. from the Kiev Polytechnic Institute, National Technical University of Ukraine. He is a Senior Researcher with the System and Network Engineering (SNE) Research group at the University of Amsterdam. His main research areas include Cloud and Big Data technologies, security distributed authorization service architectures and complex infrastructure, resource provisioning and manageable security services. He is involved in two European projects GN3plus and EuroBrazil where he develops OCX and federated Intercloud infrastructure. Yuri is actively contributing to standardization activity at RDA, NIST, OGF, IETF on cloud and Big Data related topics.

Migiel de Vos received his M.Sc. degree in Computer Science and Engineering from the Technical University of Eindhoven in the Netherlands in 2009. Since 2010 he is working on Research and Development at the department network services of SURFnet. He is involved in the operations and development of the SURFnet network and the NetherLight exchange point. This includes dedicated international connectivity, OnDemand networking and connecting cloud service providers. As of 2013 Migiel is also participating in the GN3plus project where he actively contributes to the concept of the Open Cloud eXchange.

Damir Regvart is a CARNet (Croatian Academic and Research Network) employee working as Head of Network Operation Center. Damir received his master's degree in Electrical Engineering from the University of Zagreb, Faculty of Electrical Engineering and Computing in 2002. His research interests are in the field of secure network communication, implementation of new network protocols, architectures and WAN technology. Currently he is involved in GN3plus JRA1 project as task leader for Network Architectures for Cloud Services for Horizon 2020.

Sonja Filiposka received her Ph.D. at the Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University in Skopje. Currently, she is an assistant professor at the Faculty of Computer Science and Engineering at the university. Her main research areas and interests include network design and performances, network science and complex networks theory, simulation methodologies and analysis. She is a co-author of over 80 scientific papers and is involved in a number of research and applicative projects on international and national level.

Taras Matselyukh has been playing senior technical and managerial roles such as senior architect, principal consultant, programme director, and ICT manager in networking & telecom industry for more than 20 years. His primary responsibility was to create high-quality IP and MPLS network & telecom solutions while leading groups of employees, engineers and external consultants. Currently he holds a position of Chief Technology Officer and Principal Consultant at Opt/Net Consulting B.V. He provides professional services and business consulting to telecom and internet service providers worldwide.

Eduard Escalona is the Infrastructure Control and Management research line manager within the Distributed Applications and Networks Area of the i2CAT Foundation. Before, he worked for 5 years (2007-2012) as a senior research officer at the University of Essex (UK) involved in several EU funded projects. He obtained his MSc and PhD degrees in telecommunications engineering at Universitat Politècnica de Catalunya (UPC). His main research interests are related to future internet architectures, with special focus in SDN and control and management of future internet infrastructures. He is co-author of over 60 scientific papers among international conferences and journals.

Alex Mavrin is Cisco CCIE #7846, founder at Apteriks and solutions architect. He specializes in enterprise networking, with current focus on Wireless and BYOD.

Kurt Baumann received a Master Degree in Mathematics of the University of Zurich (UZH) in 2001. In 2002 he passed the IBM trainee program. Afterwards he worked in a position of a security officer and customer engineer for IT-Infrastructures projects in the strategy-outsourcing department at IBM Switzerland. In 2005 he joined SWITCH as a member of the middle ware group in a position of the Project leader of SWITCHconnect. Today he is a member of the Peta Solutions Department at SWITCH with focus of network support research. He is actively participating in R&D projects in Wireless Mesh Networks, FEDERICA, cloud computing (Swiss Academic Cloud) and is task leader of the JRA2T5, Network Factory.

Daniel Arbel received his M.Sc. degree and later Ph.D. from the Technion - Israel Institute of Technology. Daniel is currently a member of IUCC (Inter University Computational Center) network group and NOC. He has 20 years of experience in design and management of campus and WAN networks. Daniel is involved in GN3plus as a member of jra1 task - Network Architectures for Cloud Services for Horizon 2020.

Jeroen van der Ham received his MSc in Artificial Intelligence from Utrecht University in 2002, his MSc in System and Network Engineering in 2004, and his PhD in 2010 at the University of Amsterdam on the topic of "Semantic descriptions of complex computer networks". He currently works as a researcher at the System and Network Engineering research group at the University of Amsterdam. His research interests are in semantic descriptions of multilayer and multi-domain networks and (virtualized) resources, as well as associated algorithms and architectures. He is editor of the NML Schema document and currently involved in various EU-funded projects. **Tony Breach** is a Research and Project officer at NORDUnet. He joined NORDUnet in the beginning of 2006 and has been evolved in the selection and deployment of a dark fibre based versatile infrastructure that enables NORDUnet's Optical Private Network (OPN) and NorthernLight Optical Exchange (NOX). Currently, Tony leads the Joint Research Activity 1 (JRA1) Future Network Architecture under the GÉANT 3 Plus project. Tony has significant experience within design, installation and maintenance of transmissions and broadband aggregations systems, design and deployment of operational and support systems for large telecommunications providers. Tony holds a M.Sc. degree in electromagnetic engineering from Aalborg University. **Cees de Laat** is a Professor and chair of the System and Network Engineering Research (SNE) group at the University of Amsterdam. SNE research topics includes optical/switched networking for Internet transport of massive amounts of data in TeraScale eScience applications, semantic resources description and modelling, distributed cross organization authorization infrastructures, systems security and privacy protection in distributed information systems. In cooperation with SURFnet he developed and implemented a number of projects in the GigaPort Research on Networks programme. He is a co-founder of the Global Lambda Integrated Facility (GLIF) and a founding member of CineGrid.org.