Defining Intercloud Federation Framework for Multi-provider Cloud Services Integration

Marc X. Makkes*†, Canh Ngo*, Yuri Demchenko*, Rudolf Strijkers*†, Robert Meijer*†, Cees de Laat*

* System and Network Engineering Group
University of Amsterdam
Amsterdam, the Netherlands
e-mail:{t.c.ngo,y.demchenko,delaat}@uva.nl

† Information and Communication Technology
TNO
Groningen, The Netherlands
{marc.makkes, rudolf.strijkers, robert.meijer}@tno.nl

***Abstract*—This paper presents the on-going research to define the Intercloud Federation Framework (ICFF) which is a part of the general Intercloud Architecture Framework (ICAF) proposed by the authors. ICFF attempts to address the interoperability and integration issues in provisioning on-demand multi-provider multi-domain heterogeneous cloud infrastructure services. The paper describe the major Intercloud federation scenarios that in general involves two type of federations: customer-side federation that includes federation between cloud based services and customer campus or enterprise infrastructure; and provider-side federation that is created by a group of cloud providers to outsource or broker their resources when provisioning services to customers. The proposed ICFF uses cloud resources brokering model as the main operational model in typically non-coordinated Intercloud and multi-cloud environment. The paper analyses federated identity management scenarios and related design patterns that actually creates a basis for operating federations and providing consistent federated access control infrastructure. The paper also refers to successful virtual organisation experience in Grids and attempts to re-use it in ICFF. The presented work attempts to provide an architectural model for developing Intercloud middle-ware and in the way will facilitate cloud interoperability and integration.**

***Index Terms*—Intercloud Federations Framework; Intercloud Architecture; Cloud Computing Reference Architecture; Multi-layer Cloud Services Model.**

I. INTRODUCTION

Clouds are increasingly used both by industry and by research community to outsource and/or extend their IT infrastructure. They are also used to offload the computationally intensive tasks and large data volumes, thus make them easily and globally reachable. Cloud Computing [1], [2] technologies are evolving as a common way to provide infrastructure services, resources virtualization and on-demand provisioning. In addition, they bring mobility and hardware independence to the existing distributed computing and networking applications. Despite the growth and improvement in services offered by the cloud mega-providers such as Amazon [3], Microsoft Azure [4], Google Cloud [5], Rackspace [6], an enlarging number of cloud-oriented applications and global services will require provisioning for cloud based infrastructure services involving multi-provider and multi-domain resources. They also need to inter-connect and integrate with legacy network infrastructures and enterprise services.

Current cloud technologies development demonstrates movement on developing Intercloud models, architectures and integration tools. They support the integration of cloud infrastructures into existing enterprise and campus infrastructures, and provide a common and interoperable environment to move existing infrastructures on the cloud environment [7].

A common approach here is to use different services, resources and identities federation models. However, there is no available well-defined work to provide a common federation model for resources and services integration from multiple providers, which also allows users identities federation between home organizations and cloud service domains.

We refer to our ongoing research to define the general Intercloud Architecture Framework (ICAF) [8]–[10], that intends to address the multi-domain heterogeneous cloud based infrastructure services integration and interoperability including: integration and interoperability with the legacy IT infrastructure services. The ICAF defines the Intercloud Federation Framework (ICFF) as a framework for federating independently managed cloud and non-cloud resources and service domains together with the customer and provider identity services federation.

In this paper we propose a further definition of the ICFF components supporting to create complex projects and group oriented infrastructures on-demand provisioned across multiple providers. The research presented in this paper is based on and attempts to leverage the experience from a number of cooperative projects where the authors actively participated such as EGEE [11], GEANT3 [12] and, GEYSERS [13], that have developed federated models for Virtual Organization (VO), federated Grid resources sharing, federated access to web and network services, and combined network and IT resources provisioning by telecom services providers.

The remainder of the paper is organized as follows. Section II provides analysis of the general use cases and basic scenarios for cloud and inter-cloud federation, including short reference to the VO based federation model in Grids. Section III presents the summary of the Intercloud Architecture framework, and section IV goes into further definitions and details

Copyright (c) IARIA, 2013. ISBN: 978-1-61208-271-4

of the proposed Intercloud federation framework. Section V provides information about our work to build a cloud-based test-bed for modeling and testing the proposed federation models. Section VI gives a short overview of the related works. And finally, Section VII contains conclusions and describes our further development plans.

II. General Use Cases and Basic Scenarios

A. Customer side and Provider side Federation

We define two general use cases for (1) federating cloud resources on the provider side, or (2) creating federated multi-provider infrastructures and services to deliver federated cloud services to the customer. We define the following main actors and roles adopting the Resource-Ownership-Role-Action (RORA) model proposed in [14]:

- **Cloud Service Provider** (CSP) as 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). We need to admit specifies 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.
- **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 (e.g. enterprise or university) requesting 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.

Note, we do not define the broker at this stage because for the basic scenarios discussed here the broker functions can be substituted with either CSP or Identity provider (IdP) role. We will provide definition of the cloud broker role in section IV for the multi-provider Intercloud environment. Figure 1 illustrates two cases when (1) the cloud based services and/or infrastructure needs to be integrated/federated with the existing user accounts and enterprise infrastructure, or (2) cloud based public services can use external IDP and in this way already existing user accounts with the single or multiple 3rd party IDPs (such as Google+/GooglePlay, Facebook, Microsoft, or other OpenID providers).

Figure 2 illustrates the major actors and their relation in the provider side federation that is typically created between cloud service providers to share and/or outsource their cloud resources when providing a final service to the customer

B. Federated Access Control and Identity Management

Federated Identity Management (FIDM) is the main component of the federated cloud infrastructure. This issue has been recognized by industry and addressed by the OASIS Cloud TC

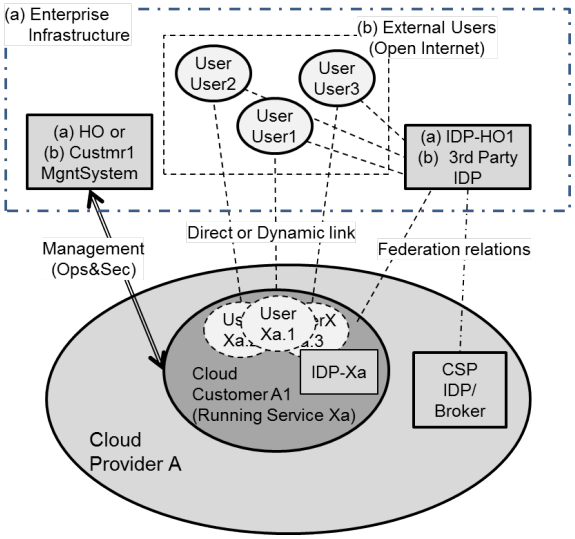

Fig. 1. Customer/user side federation for delivery of the federated cloud services to (a) enterprise customers running their own IDP and (b) for user access federation for public cloud based services.

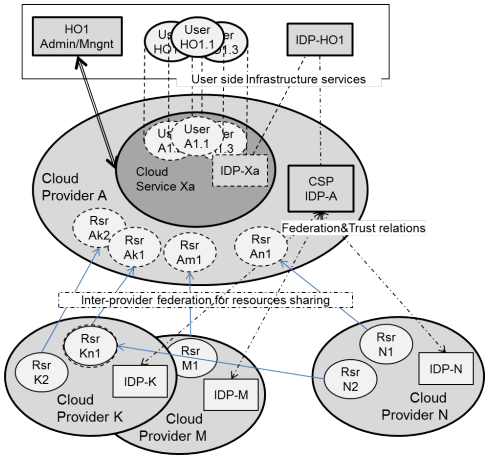

Fig. 2. Provider side federation for resources sharing and outsourcing

[15]. In the typical distributed inter-cloud infrastructure, the broker outsources the authentication and attribute management to a 3rd party IDP, either regular or cloud-aware which we will refer to as Federated IDP (FIDP). Similar to the general federation scenarios, we identify two scenarios for FIDP: a single user (actually representing individual users of the public services) and users of a customer organization (that can also be referred to as "Home Organization (HO)") that have their accounts at their HO in which their identities are confirmed by the HO-IDP.

1) A single-end user scenario: In this scenario, the FIDM at broker site needs to support standardized IDP protocols such as OpenID, SAML, OAuth to interoperate with public IDP, as in Figure 3.

2) Company/organization scenarios: When the customer is an organization or a company, there are possible IDP deployments. First, due to sensitive IdP information, some

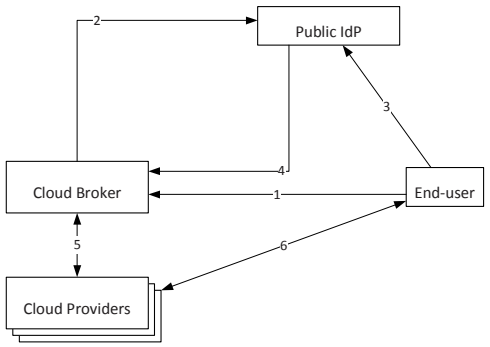

Fig. 3. Multi-provider federation with a Public IDP

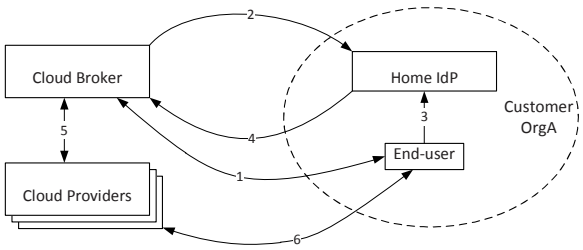

Fig. 4. Corporate customer running an on-site IDP service

organizations choose to deploy their own private IdP on-site, which need to collaborate with the FIDM Broker as in Figure 4. The vital requirement here is broker need mechanisms to discover the customer's IDP to connect for retrieving end-users' attributes and logon statuses.

In other scenario, a "light-weight" customer may want to out-source their identity management service to a cloud provider (i.e. IDP as a Service – IdPaaS). In this case, the IDP services are provisioned and collaborate with the FIDM cloud broker. The on-demand IDP service should support followings:

- Support service provisioning life-cycles.
- Manageable by the cloud customer for their own organization.
- Integrate with access control services for the cloud resources.

C. Policy and Security Context Management

Policy and security context management are important components of creating, operating and managing federated access control infrastructure. Authors' previous works the XACML (eXtensible Access Control Markup Language) policy format provides all necessary functionality for multi-domain policy expression and attributes definition [16], [17]. XACML policy identification and attributes format allow for using different namespaces and attributes semantics. The proposed Generic AAA Authorisation framework [18] allows multi-domain attributes validation and mapping when evaluating access control request. Another important component in managing federated access control infrastructure is authorization session security context management what can be achieved with using tickets and tokens as session credentials. Proposed in [19], [20] authorization tickets and pilot tokens can support inter-domain security context communication, delegation and federation management.

D. VO based Federation in Grids

The problem, which underlies the Computational Grid concept, is coordinated resource sharing and problem solving in dynamic, multi-institutional Virtual Organizations (VO). VO are defined as a collection of individuals, institutions and resources that access and share resources within the Grid [21]. Developing Intercloud federation framework we intend to re-use Grid community experience in building robust inter-organisational services, in particular using VO and a federation mechanism for managing dynamic security associations [22] The following security services and related functionalities are identified for the VO [22]:

1) Identity management service, normally provided by IDP.
2) Attribute management service that issues attributes bound to user or resource identity that primary can be used for authorization decision when accessing VO resources or services.
3) Authorization service to enforce access control to the resource or service based on entity's attributes/roles and authorisation policies.
4) Policy management service to provide VO-wide policies related to authorisation, trust management, identity federation, mapping of identities, attributes and policies.
5) Trust management service that may include CA and associate PKI management services that allows establishing and managing trust relations inside VO.

In contrast to clouds, all VO services may be provided (and managed) by member organizations on behalf of the VO. Services provisioning in clouds typically includes also identity provisioning that may be linked to (or federated with) the existing user identity.

III. INTERCLOUD ARCHITECTURE FRAMEWORK

The Intercloud Architecture Framework, introduced in [8], 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. The ICAF consist of the flowing components:

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;
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 and 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.

The ICFF is the main framework which creates the Intercloud it self. The primary focus in the paper lies on the ICFF.

IV. ICFF Definition and Requirements

As defined in [9], [23] the ICFF allows clouds from different administrative domains to from a federation. The federation allows for end-users to view the cloud as one, while the individual cloud providers can differentiate based on location, infrastructure and network connections to the outside world.

A. Intercloud Federation Framework.

The Intercloud federation framework is responsible for coordinating allocation of resources in a unified way. Figure 5 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 brokers,
- Service Registry
- Service Discovery
- Identity provider (IdP)
- Trust manager

B. Service Broker

To overcome these shortcomings of decentralized non-coordinated allocation of resources with in multi-provider multi-domain heterogeneous cloud services, we introduce a service broker to solve allocation of resources. We identify the broker as the key component for federation, which does not have to be exclusive. The role and responsibility of the service broker is to solve the resource brokering problem. We defined as the problem as follows: ”Allocation of resources and services across the multiple cloud resources such as computational clusters, parallel supercomputers, storage clusters that belong to different administrative domains”.

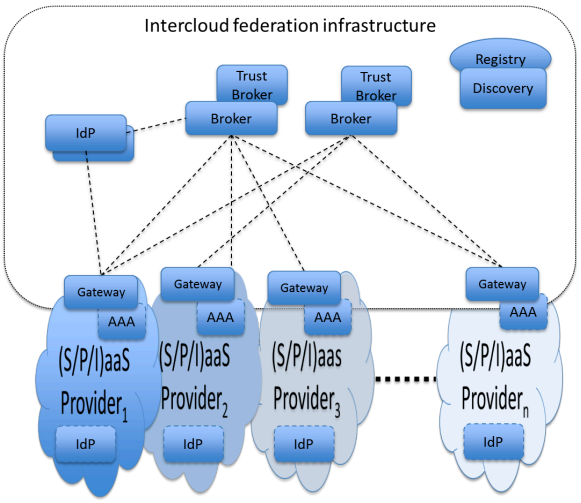

Fig. 5. Intercloud Federation Framework, where the broker has a central role for connecting to multi-cloud providers and presenting this as one Interface to the end-user. In addition, it has support for dynamical trust and IdP.

To solve the brokering problem, the service broker has interaction with both customers to allocate and de-allocation resources across multiple cloud providers on behave of the customers. Having a broker allocate resources on behave will simplify administration for cloud providers, as cloud provider only have to do accounting for service brokers, instead for every customer.

To have a service broker as opposed to having no brokers (such as a root directory [24]) in the federation, is to have a unified interface to all cloud providers as opposed to have different interfaces to each cloud provider in the federation. In that sense, the broker together with the cloud provider’s gateway provides and ensures the interoperability between different participating clouds. Thus, the brokers provide interface for allocation of resources for their costumers.

To provide identity management over moreover the brokers have interfaces to service registry, service discovery, identity provider (IdP), and trust manager, see Figure (5) for details.

C. Service registry

The service registry is a directory where cloud providers can provide information regarding IaaS, SaaS and PaaS services, which includes details of allocation of resources as well as service level agreements and policies. The broker can query Service registry information about services, and can negotiate SLA and policy with the clients. In addition, this information can be used to allocate resources in a specific cloud provider.

D. Identity Provider

ICFF operates across security domains, which are involving different cloud entities, from cloud providers to cloud consumers [2]. In this context, ICFF needs to support and integrate with the identity and trust management for these entities for both provider and customer sides.

The dynamic resource provisioning in the collaboration scenarios of cloud providers require the trust management to carry

Copyright (c) IARIA, 2013. ISBN: 978-1-61208-271-4

out trust establishments between them. The trust management in the ICFF needs to support following requirements:

- Dynamic trust establishment between indirect cloud entities: Current relationships between cloud entities often rely on SLAs, which are mostly suitable for direct relationships. ICFF scenarios require a cloud provider or cloud consumer could connect to other unknown entities, through a chain of direct SLA relationships, which is known as dynamic trust relationship [25].
- Interoperate and extend standardized mechanisms on multi-domain identity management and trust management, which are SAML [26], OAuth [27] to support on-demand provisioned clouds.
- A fine-grained trust management policy language.

ICFF should take into account federated identity management in its operation management:

- Compatible with existing public identity management systems.
- Interoperate between identity management with the on-demand access control services to manage cloud resources.

E. Grid vs Cloud Federation

The main idea behind cloud computing is that infrastructure that is not used, is rented to third parties. This includes storage, computational, and services in an on-demand and pay-as-you-go model. Except for the on-demand and pay-as-you-go model, the ideas of grids grid are not quite different. Grid federation is based on institutions that want to cooperate, such that users, can access computational resources quicker. The hierarchy is mostly flat, with a 'super scheduler' to schedule all jobs on the combined resources using queue's. To scale vertically, i.e. creating hierarchy can only be done with software such as [28]. Clouds on the other hand, are mostly providing services to their customers, and have competition on the market. Horizontal scaling and federation can both be done with brokering. In addition, brokering allows for hierarchical scaling as a broker of broker can be created. Clouds provide a services oriented model, such as IaaS, PaaS and SaaS. Together with brokering, this 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.

The vital difference between grids and clouds is that the amount of computation is mostly unknown with clouds, hence it is manly used for running services while grids are to run predefined computational jobs with budgets. While grids can be run on clouds using grid software [22] the other way around is not trivial task. In addition, clouds are mostly used workloads that are not pre-defined, such as services, while grids run mostly budget or time constrained computation jobs.

V. Cloud Federation Modeling

This section provides short overview of the test-bed that we used for modeling overlay network and which we are redesigning to support modeling of the basic federation models in provisioning federated cloud resources. The test-bed consists of a Broker, which connects users and Different cloud providers, which includes Amazon AWS and Brightbox, with each other and is such a way that users can create VM (IaaS) over multiple provide. The broker provides an interface to OpenID IdP provided by google [27] to provide accounting, authentication, and authentication. The test-bed provides an interface to the end- users such that they can instantiate a layer 2 overlay network using VPN's. The interface provides also addressing IPv4 and IPv6 for created IaaS nodes in an automated fashion. After the overlay network is created and addressing is assigned, the interface provides an option to enable IPv4 or IPv6 routing based on Quagga [29]. This allows uses to create on-demand overlay network in multi provider cloud environments. The authors believe that at the time of conference the proposed test-bed will collect valuable information to estimate performance of the basic federation use-cases when realized with the AWS infrastructure.

VI. Related Work

Federations of computational resources come in different forms, but one federation that's on large scale is grid computing. The problems of federation in Grid computing shows many resemblance with cloud computing.

The main idea behind grid computing is to use computation and storage resources for other computational goals if they are not used. This idea was then fully extended to multiple locations, multiple administrative domains, different architectures, etc., and link together with software. In Grid computing, the federation problem The Grid resource brokering, also know as super-scheduling, problem is defined as: " scheduling jobs across the grid resources such as computational clusters, parallel supercomputers, desktop machines that belong to different administrative domains". Brokering in computational grids is facilitated by specialized application schedulers such as Nimrod-G [30], Condor-G [31], AppLeS [32], APST [33] Legion and WorkFlow Engines. Grid Brokering activity involves:

- Querying grid resource information services (GRIS) for locating resources that match the job requirements,
- Coordinating and negotiating Service Level Agreements;
- and job scheduling.

The grid resources are managed by their local resource management systems such as Condor. These systems manage job queues, initiate and monitor their execution.

VII. Future Development

The paper presents an on-going research at the University of Amsterdam to develop the Intercloud Architecture (ICA) addresses the problem of multi-domain heterogeneous Cloud based applications integration and inter-provider and inter-platform interoperability. The presented research is planned

Copyright (c) IARIA, 2013. ISBN: 978-1-61208-271-4

to be contributed to the Open Grid Forum Research Group on Infrastructure services On-Demand provisioning (ISOD-RG) [27], where the authors play active role. In addition, we planned to extent our test-bed, in such away that it enables dynamic provisioning of federation infrastructure.

VIII. ACKNOWLEDGMENTS

This project is supported by the Dutch national research program COMMIT and the FP7 EU funded Integrated projects The Generalized Architecture for Dynamic Infrastructure Services (GEYSERS, FP7-ICT-248657), GEANT3 (FP7-ICT-238875).

REFERENCES

[1] "NIST SP 800-145, "A NIST definition of cloud computing"." http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed February 2013.

[2] "NIST SP 500-292, Cloud Computing Reference Architecture, v1.0.." http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505, accessed February 2013.

[3] "Amazone Web Services." http://aws.amazon.com/products/, accessed February 2013.

[4] "Microsoft Windows Azure." http://www.windowsazure.com/, accessed February 2013.

[5] "Google Cloud Platform." https://cloud.google.com/, accessed February 2013.

[6] "Rackspace Cloud." http://www.rackspace.com/cloud/, accessed February 2013.

[7] R. Buyya, R. Ranjan, and R. Calheiros, "Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services," *Algorithms and architectures for parallel processing*, pp. 13–31, 2010.

[8] Y. Demchenko, C. Ngo, M. Makkes, R. Strijkers, and C. de Laat, "Defining inter-cloud architecture for interoperability and integration," in *CLOUD COMPUTING 2012, The Third International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 174–180, 2012.

[9] Y. Demchenko, C. Ngo, C. de Laat, J. Garcia-Espin, S. Figuerola, J. Rodriguez, L. Contreras, G. Landi, and N. Ciulli, "Intercloud architecture framework for heterogeneous cloud based infrastructure services provisioning on-demand.," 2013.

[10] B. Khasnabish, "Cloud reference framework." draft-khasnabish-cloud-reference-framework-04.txt, 2012.

[11] "European Grid Infrastructure (EGI)." http://www.egi.eu/about/EGI.eu/, accessed February 2013.

[12] "Geant project." http://www.geant.net/pages/home.aspx, accessed February 2013.

[13] "Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project)." http://www.geysers.eu/, accessed February 2013.

[14] J. Garcia-Espin, J. Riera, S. Figuerola, and E. Lopez, "A multi-tenancy model based on resource capabilities and ownership for infrastructure management," 2012.

[15] "OASIS IDCloud TC: OASIS Identity in the Cloud TC.." http://wiki.oasis-open.org/id-cloud/, accessed February 2013.

[16] Y. Demchenko, M. Cristea, and C. de Laat, "XACML policy profile for multidomain network resource provisioning and supporting authorisation infrastructure," in *Policies for Distributed Systems and Networks, 2009. POLICY 2009. IEEE International Symposium on*, pp. 98–101, IEEE, 2009.

[17] G. Garzoglio, I. Alderman, M. Altunay, R. Ananthakrishnan, J. Bester, K. Chadwick, V. Ciaschini, Y. Demchenko, A. Ferraro, A. Forti, *et al.*, "Definition and implementation of a saml-xacml profile for authorization interoperability across grid middleware in osg and egee," *Journal of Grid Computing*, vol. 7, no. 3, pp. 297–307, 2009.

[18] Y. Demchenko, A. Wan, M. Cristea, and C. De Laat, "Authorisation infrastructure for on-demand network resource provisioning," in *Grid Computing, 2008 9th IEEE/ACM International Conference on*, pp. 95–103, IEEE, 2008.

[19] L. Gommans, L. Xu, Y. Demchenko, A. Wan, M. Cristea, R. Meijer, and C. De Laat, "Multi-domain lightpath authorization, using tokens," *Future Generation Computer Systems*, vol. 25, no. 2, pp. 153–160, 2009.

[20] Y. Demchenko, O. Koeroo, C. de Laat, and H. Sagehaug, "Extending XACML authorisation model to support policy obligations handling in distributed application," in *Proceedings of the 6th international workshop on Middleware for grid computing*, p. 5, ACM, 2008.

[21] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *International journal of high performance computing applications*, vol. 15, no. 3, pp. 200–222, 2001.

[22] Y. Demchenko, "Virtual organisations in computer grids and identity management," *Information Security Technical Report*, vol. 9, no. 1, pp. 59–76, 2004.

[23] Y. Demchenko, M. Makkes, R. Strijkers, and C. de Laat, "Intercloud architecture for interoperability and integration," in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pp. 666–674, Dec. 2012.

[24] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud - protocols and formats for cloud computing interoperability," in *ICIW* (M. Perry, H. Sasaki, M. Ehmann, G. O. Bellot, and O. Dini, eds.), pp. 328–336, IEEE Computer Society, 2009.

[25] C. Ngo, Y. Demchenko, and C. de Laat, "Toward a dynamic trust establishment approach for multi-provider intercloud environment," in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pp. 532–538, IEEE, 2012.

[26] S. Cantor, J. Kemp, R. Philpott, and E. Maler, "Assertions and protocols for the oasis security assertion markup language," *OASIS Standard (March 2005)*, 2005.

[27] "Using OAuth 2.0 to Access Google APIs." https://developers.google.com/accounts/docs/OAuth2, accessed February 2013.

[28] P. Andreetto, S. Borgia, A. Dorigo, A. Gianelle, M. Marzolla, M. Mordacchini, M. Sgaravatto, F. Dvorák, D. Kouril, A. Krenek, *et al.*, "CREAM: a simple, grid-accessible, job management system for local computational resources," *CHEP 2006, Mumbay, India*, 2006.

[29] "GNU quagga routing software." http://www.quagga.net/, accessed February 2013.

[30] A. Natrajan, M. Humphrey, and A. Grimshaw, "Grid resource management in legion," *INTERNATIONAL SERIES IN OPERATIONS RESEARCH AND MANAGEMENT SCIENCE*, pp. 145–160, 2003.

[31] J. Frey, T. Tannenbaum, M. Livny, I. Foster, and S. Tuecke, "Condor-g: A computation management agent for multi-institutional grids," *Cluster Computing*, vol. 5, no. 3, pp. 237–246, 2002.

[32] F. Berman, "High-performance schedulers," *The grid: blueprint for a new computing infrastructure*, vol. 67, pp. 279–309, 1999.

[33] Y. Yang, K. van der Raadt, and H. Casanova, "Multiround algorithms for scheduling divisible loads," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 16, no. 11, pp. 1092–1102, 2005.

Copyright (c) IARIA, 2013. ISBN: 978-1-61208-271-4