

Federated Access Control in Heterogeneous Intercloud Environment: Basic Models and Architecture Patterns

Yuri Demchenko, Canh Ngo, Cees de Laat

System and Network Engineering
University of Amsterdam
Amsterdam, The Netherlands

{y.demchenko, c.t.ngo, delaat}@uva.nl

Craig Lee

The Aerospace Corporation
El Segundo, CA, USA
lee@aero.org

Abstract— This paper presents on-going research to define the basic models and architecture patterns for federated access control in heterogeneous (multi-provider) multi-cloud and inter-cloud environment. The proposed research contributes to the further definition of Intercloud Federation Framework (ICFF) which is a part of the general Intercloud Architecture Framework (ICAF) proposed by authors in earlier works. ICFF attempts to address the interoperability and integration issues in provisioning on-demand multi-provider multi-domain heterogeneous cloud infrastructure services. The paper describes the major inter-cloud federation scenarios that in general involve two types 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 federated access control model uses Federated Identity Management (FIDM) model that can be also supported by the trusted third party entities such as Cloud Service Broker (CSB) and/or trust broker to establish dynamic trust relations between entities without previously existing trust. The research analyses different federated identity management scenarios, defines the basic architecture patterns and the main components of the distributed federated multi-domain Authentication and Authorisation infrastructure.

Keywords- *Federated Intercloud Access Control Infrastructure, Intercloud Federations Framework, Intercloud Architecture Framework, Authorisation, Federated Identity Management, Cloud Security infrastructure.*

I. INTRODUCTION (HEADING 1)

Current development of the Cloud Computing [1, 2] technologies demonstrates movement to developing Intercloud models, architectures and integration tools that could allow integration of cloud based infrastructure services into existing enterprise and campus infrastructures, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualized cloud environment [3].

Clouds are increasingly used both by industry and by research community to outsource and/or extend their IT infrastructure as well as offload their computationally intensive tasks and storage of the large volumes of data that in clouds can be easily make globally reachable. Despite the

growth and service offering improvement by the major cloud mega-providers such as Amazon [3], Microsoft Azure [4], Google Cloud [5], Rackspace [6] and few others, a growing number of cloud-oriented applications and global services will require provisioning cloud based infrastructure services that may involve multi-provider and multi-domain resources, including required inter-connecting network infrastructure and necessary integration with the enterprise legacy services and infrastructure.

The federated model for services, resources and other infrastructure components integration, interoperability and access control is becoming a commonly accepted approach [7]. However, there is no currently available well-defined federation model that would provide a common basis for integration of resources and services from multiple providers and allow user identities federation between their home organization and multiple cloud based service domains.

In this research and paper, we refer to our ongoing research to define the general Intercloud Architecture Framework (ICAF) [8, 9, 10], being developed by the authors, that intends to address the multi-domain heterogeneous cloud based infrastructure services integration and interoperability including integration and interoperability with the campus/enterprise legacy IT infrastructure services. The short ICAF definition summary is provided below. The ICAF defines the Intercloud Federation Framework 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 to allow creating complex project and group oriented infrastructures provisioned on-demand and across multiple providers.

To ensure consistency in the proposed in this paper definitions and description, we needed to revisit some “intuitively” used terms and concepts. In particular, in this paper we distinguish between a cloud customer which can be an enterprise or organization and a user who is an end-user or service consumer. For example, a customer creates a web services on cloud but actual service users or consumers are external entities who in the context of this research need to provide their identity or authorization credentials in order to access cloud based services.

We also distinguish between simple multi-provider cloud services and federated cloud/intercloud services. Simple non-

federated cloud services provisioning may include cloud services and resources from multiple CSP but these services are composed as independent components either by customers themselves integrating them into their existing infrastructure or the service composition is done by the third party broker on behalf of the customer. In this scenario, the resources or services deployed in different clouds are not supposed to interact and don't require special federation mechanisms, even though the issues with distributed VM deployment/placement, VM and services scaling and services migration remain. Federated intercloud infrastructure and services, on the other hand, require interaction between services in different cloud/CSP domains and consequently user access of services from different administrative and security domains. Federated cloud infrastructure and consequently federated access control should allow smooth services interaction using common/single identity and access credentials.

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/GN3plus [12] and GEYSERS [13], that have developed federated models for Virtual Organization (VO) based federated Grid resources sharing, federated access to web and network services, and combined network and IT resources provisioning by telecom services provides.

The remainder of the paper is organized as follows. Section 2 provides a reference and a short summary of Intercloud Architecture Framework in context of which the proposed cloud federation models will be discussed. Section 3 provides an observation about paradigm change in the cloud security. Section 4 reviews the technologies that enable general and cloud services federation, refers to VO based federations in Grid. Section 5 provides analysis of the general use cases and basic scenarios for cloud and inter-cloud federation. Section 6 defines the main components and operational procedures in the Intercloud Federation Framework. Section 7 introduces the general model and define the main functional components of the federated access control infrastructure, and section 8 discusses federated identity management in clouds. Section 9 provides conclusions and describes our further development plans.

II. INTERCLOUD ARCHITECTURE FRAMEWORK

We provide here a short description of the Intercloud Architecture Framework proposed and being developed by the authors in the framework of the mentioned above cooperative projects [9]. The ICAF definition is using a general case of provisioning the cloud based infrastructure to support the enterprise or scientific workflow and operations related to the processes monitoring and data processing. Cloud technologies simplify building such infrastructure and provisioning it on-demand.

Figure 1 illustrates how an example enterprise or scientific workflow can be mapped to cloud based services and then deployed and operated as an instant inter-cloud infrastructure. It contains cloud infrastructure segments IaaS (VR3-VR5) and PaaS (VR6, VR7), separate virtualised

resources or services (VR1, VR2) that can be also enterprise none-cloud legacy applications, two interacting campuses A and B with existing campus facilities, and interconnecting them network infrastructure that in many cases may need to use dedicated network links for guaranteed performance.

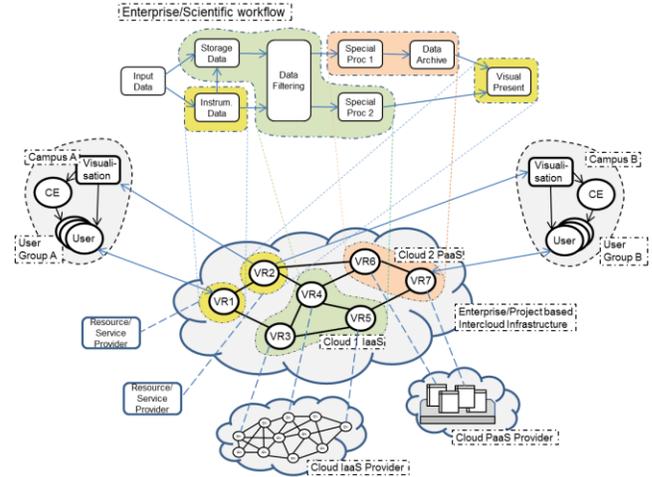


Figure 1. Enterprise or project oriented cloud based infrastructure to support enterprise or scientific workflow.

In the context of this paper, all involved entities and resources that generally may belong to different administrative and security domains may create federations for effective management and access control. Efficient operation of such infrastructure will require both overall infrastructure management and individual services and infrastructure segments to interact between themselves. This task is typically out of scope of existing cloud service models and is intended to be addressed by the proposed Intercloud Architecture.

The proposed Intercloud Architecture Framework [9] includes the following components that separate all functions related the cloud services design, control, management and operations into “orthogonal” groups:

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

(2) Intercloud Control and Management Plane (ICMP) 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 the sense of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF;

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

III. PARADIGMS CHANGE IN CLOUD SECURITY

Virtualisation, elasticity and on-demand provisioning of cloud infrastructure services drives paradigm change in security design and operation. Considering evolutionary relations between Grids and Clouds, it is important to compare their security models. It is also important from the point of view that future e-Science infrastructures will integrate both Grid based core e-Science infrastructure and Cloud based infrastructures provisioned on-demand, and eventually Grids based services will be migrated to clouds [11].

Grid security architecture is primarily based on the Virtual Organisations (VO) that are created by the cooperating organisations that share resources (which however remain in their ownership) based on mutual agreement between VO members and common VO security policy. In Grids, VO actually acts as a federation of the users and resources that enables federated access control based on the federated security and trust model [15, 16]. To state this another way, a VO is a security and collaboration context that can span multiple administrative domains.

Increasing move of enterprise and public sector services to clouds motivates refactoring of the traditional security services and tools to adopt/address the following “cloud factors”:

- Services virtualisation, what allows for VM processes isolation at host and at CPU level
- On-demand service provisioning
- Dynamic services composition and lifecycle management
- Services migration across machines, hosts and locations
- Services and resources scalability and global reachability

If applied to security services, these factors will also require federation lifecycle support and scalability, including support for dynamic membership granting and terminating.

In this paper we discuss the security aspects of the cloud federations management and federated access control, while for the general security challenges and models we refer to the earlier authors’ papers [17, 18].

IV. RELATED WORKS AND STATE OF THE ART

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:

A. *Federated Identity Management and Access Control*

The following are the successful community initiatives and popular products

- Shibboleth Attribute Authority Service [19] and OpenSAML [20] are the two projects that actually laid down the foundation for wide adoption of the federated identity management and federated access control.
- OpenID [21] is an open standard that allows users to be authenticated by certain co-operating sites, has growing acceptance among cloud providers.
- CILogon [22] service enables use of federated identities for access to research services. CILogon provides a federated X.509 certification authority and relies on the InCommon Federation and currently also used for accessing federated cloud infrastructures.
- OASIS Identity in the Cloud TC [23] that develops profiles of open standards for identity deployment, provisioning and management in cloud computing
- Moonshot Project [24] 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) [25]
- OpenStack KeyStone project [26] that provides Identity, Token, Catalog and Policy services for use specifically by projects in the OpenStack family.

We investigate closer the VO based federations management in Grids and a new concept of the Open Cloud eXchange proposed in the large European project GEANT/GN3plus [12, 13] representing European research community needs in cross-border research infrastructure services.

B. *VO based Federations 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 [16]. Developing Intercloud Federation Framework we intend to re-use Grid community experience in building robust inter-organisational services, in particular using VO for managing dynamic security associations [27, 28, 29].

In contrast to clouds, all VO services may be provided by member organizations on behalf of the VO. Services provisioning in clouds typically also includes identity provisioning.

V. GENERAL USE CASES AND BASIC SCENARIOS

A. Roles and Actors

We define the following main actors and roles adopting the Resource-Ownership-Role-Action (RORA) model proposed in [30]:

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

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

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

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

B. Customer side and Provider side Federations

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

Figure 2 illustrates two cases when (a) cloud based services and/or infrastructure needs to be federated with the existing user accounts and enterprise infrastructure, or (b) cloud based public services can use external IdP and in this way already existing user accounts with the single or multiple 3rd party IDP (such as Google+/GooglePlay, Facebook, Microsoft, or other open IDP).

Figure 3 illustrates the major actors and their relation in the provider side federation to share and outsource cloud resources when providing a final service to the customer.

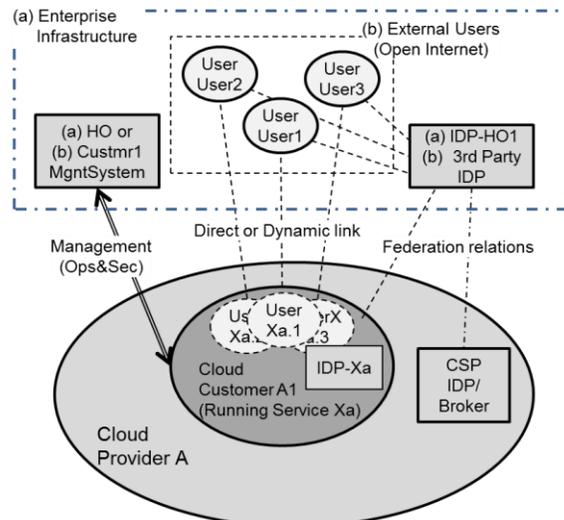


Figure 2. Customer/user side federation for delivery of the federated cloud services to enterprise customers.

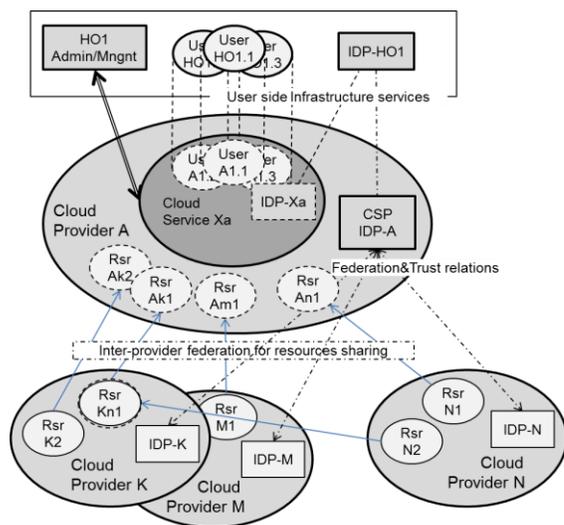


Figure 3. Provider side federation for resources sharing and outsourcing.

VI. ICFE COMPONENTS AND OPERATION

ICFE defined in [9] and introduced in section 2 allows clouds from different administrative domains to form a federation. The federation allows for end-users to access cloud services from multiple domains without need to obtain a separate identity, while services remain under control of their original operator or home provider.

The Intercloud Federation Framework is responsible for coordinating allocation of resources in a unified way. Figure 4 illustrates the main components of the federated Intercloud Architecture, specifically underlying the Intercloud gateway function (GW) that provides translation of the requests, protocols and data formats between cloud domains. At the same time the federated Intercloud infrastructure requires a number of functionalities, protocols and interfaces to support its operation:

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

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

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

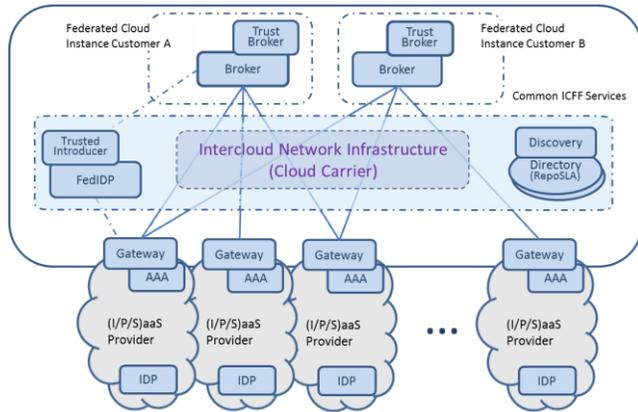


Figure 4. Intercloud federation infrastructure.

A. Cloud 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 defined as: "allocation of resources across the multiple cloud resources such as computational clusters, parallel supercomputers, storage clusters that belong to different administrative domains".

The service broker has interaction with both customers and providers 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. Service broker brings benefits of having a unified interface to all cloud providers in the federation what facilitates also interoperability between different participating clouds.

B. Service registry

The service registry is a directory where cloud providers can publish information about available services IaaS, SaaS and PaaS, that includes details about services, their interfaces

and availability as well as Service Level Agreements and associated policies. The broker can query service registry information and negotiate SLA and policy with the clients, including allocation in a specific cloud provider.

C. 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.

Current relationships between cloud entities often rely on SLAs what is suitable for direct relationships between parties. ICFF scenarios require a cloud provider or cloud consumer can connect to other entities, through a chain of direct SLA/trust relations by establishing dynamic trust relationship [18]. The dynamic resource provisioning in the collaboration scenario of cloud providers requires the dynamic trust establishments between them and support the following functionality:

- Be compatible, interoperate and extend standardized mechanisms on multi-domain identity management and trust management, such as SAML [31], OAuth2 [32].
- Support a fine-grained trust management policy language.
- Interoperate with the on-demand resource provisioning system and access control services to manage cloud resources during the whole their life cycle.

VII. FEDERATED ACCESS CONTROL COMPONENTS

This section will provide details how to build federated access control in cloud and inter-cloud environment, including using OpenStack Keystone identity management and authorisation service.

This section will refer to DACI model and GAAA-TK library [17] developed as part of GEYSERS project for virtualized infrastructures.

Figure 5 illustrates the main components of the Federates Access Control infrastructure (FACI) that typically uses Authentication and Authorisation services provided by the service domain but may use Home IDP either directly or relayed via local to the service IDP0 federated with the Home IDP.

Once the User's identity has been authenticated and user attributes have been obtained from the Home IDP and federated local IDP, the Policy Enforcement (PEP) requests a Policy Decision Point (PDP) to authorize the User's request, i.e., verify that they are allowed to make the request. Here, the PDP uses the User's Identity Attributes, and the Access Attributes of the requested Resource, to make a decision concerning the request. This can be done based on the policy provided by the Policy Authority Point (PAP). The PDP applies a set of rules to the attributes sets to make the authorization decision. XACML policy format and SAML assertion expression language can provide a flexible platform for managing complex authorization decisions in multidomain environment [33].

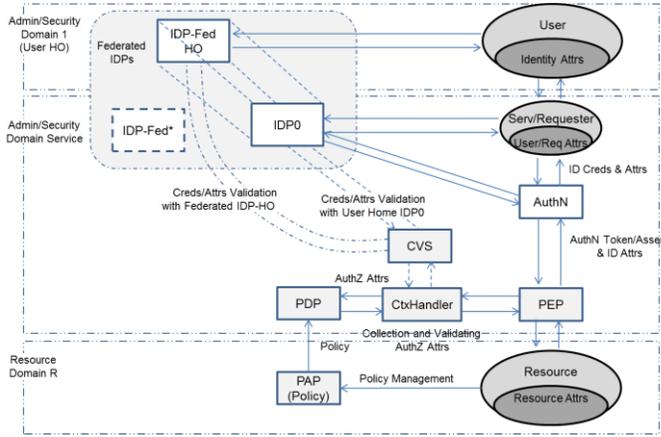


Figure 5. The Access Control Infrastructure components interaction when managing access control in a federated multi-provider environment

VIII. FEDERATED IDENTITY MANAGEMENT IN CLOUDS

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 In the typically distributed inter-cloud infrastructure, the broker outsources the authentication and attribute management to the 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 public services users) and users of a customer organization.

A. A single end-user scenario

ICFF at broker side needs to support standardized IDP protocols/scenarios: OpenID, SAML, OAuth, KeyStone protocol, CILogon, Account Chooser.

When the customer is an organization or a company, there are possible different IDP deployments. First, due to sensitive IDP information, some organizations choose to deploy their own private IDP onsite, which needs to collaborate with the ICFF Broker as in Figure 6. The vital requirement here is for the broker to have a mechanism to discover the customer's IDP to connect for retrieving end-users' attributes and logon statuses.

Preliminary work is already being done in this regard. The University of Kent has a prototype federated identity management design and implementation for the OpenStack Keystone service [25, 34]. The Kent design provides a Directory service of known and trusted IdPs, enabling Keystone to identify and use the proper authentication protocol. Very importantly, it also provides an Attribute Mapping service that maps all returned identity and authorization attributes into attributes that are locally understood. A simplified version of this design is being considered by the OpenStack Keystone team.

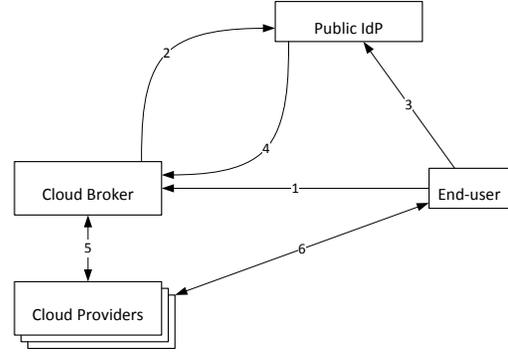


Figure 6. Multi-provider federation with a public IDP

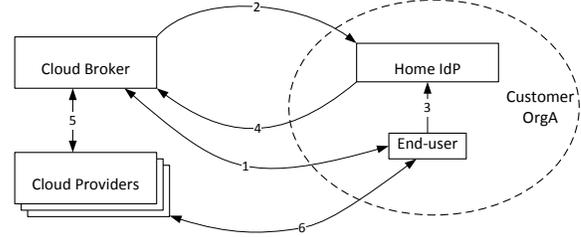


Figure 7. Corporate customer running an onsite IDP service

B. Company/organization scenarios

When the customer is an organization or a company, there are possible IDP deployments. First, due to sensitive IDP information, some organizations choose to deploy their own private IDP onsite, which need to collaborate with the Broker ICFF as in Figure 7. 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 (a.k.a. IDP as a Service – IDPaaS). In this case, the IdP services are provisioned and collaborate with the inter-cloud broker. The on-demand IDP service should support the following:

- Support service provisioning lifecycle, i.e. be provisioning session aware [35]
- Be manageable by the cloud customers for their own organization
- Integrate with access control services for the cloud resources.

IX. SUMMARY AND FUTURE RESEARCH

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

The paper defines the basic scenarios in federated cloud services provisioning and access control that include both user side federation model and provider side federation model. The paper defines the main roles and actors in the cloud federations. The proposed analysis and solutions are

targeted to address a number of practical problems in smooth multi-provider services integration and delivery to enterprise or campus users, in particular using NREN and campus based identity management services as a trusted third party what expectedly will facilitate creation of dynamic federations between multiple cloud service providers and university /customer organisations.

Further research will include modelling of the proposed Intercloud federation models to evaluate effective methods for the identity provisioning and access control policy evaluation in heterogeneous inter-cloud environment.

The presented research is planned to be contributed to the Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [36], where the authors play active role.

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] Amazon Web Services. <http://aws.amazon.com/products/>
- [4] Microsoft Windows Azure. <http://www.windowsazure.com/>
- [5] Google Cloud Platform. [online] <https://cloud.google.com/>
- [6] RackSpace Cloud. [online] <http://www.rackspace.com/cloud/>
- [7] Buyya, R., R.Ranjan, R.N.Calheiros, InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. Proc. 10th Intern Conf. on Algorithms and Architectures for Parallel Processing (ICA3PP 2010, Busan, South Korea, May 21-23, 2010), LNCS, Springer, Germany, 2010.
- [8] Demchenko, Y., C.Ngo, M.Makkes, R.Strijkers, C. de Laat, Defining Inter-Cloud Architecture for Interoperability and Integration. The Third Intern Conf on Cloud Computing, GRIDS, and Virtualization (CLOUD COMPUTING 2012), July 22-27, 2012, Nice, France.
- [9] Demchenko, Y., et al, Intercloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand. The 27th IEEE Intl Conf. on Advanced Information Networking and Applications (AINA2013), 25-28 March 2013
- [10] Cloud Reference Framework. Internet Draft, 6 January 2014. [online] <draft-khasnabish-cloud-reference-framework-06.txt>
- [11] European Grid Infrastructure (EGI). [online] <http://www.egi.eu/about/EGI.eu/>
- [12] GEANT Project. [Online] <http://www.geant.net/pages/home.aspx>
- [13] Demchenko, Y., J. van der Ham, C.Ngo, T.Matselyukh, S.Filiposka, C. de Laat, Open Cloud eXchange (OCX): Architecture and Functional Components. Proc. The 5th IEEE International Conference and Workshops on Cloud Computing Technology and Science (CloudCom2013), 2-5 December 2013, Bristol, UK
- [14] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project). [Online] <http://www.geysers.eu/>
- [15] Demchenko, Y., C. de Laat, O. Koeroo, D. Groep, "Re-thinking Grid Security Architecture". Proceedings of IEEE Fourth eScience 2008 Conference, December 7-12, 2008, Indianapolis, USA. Pp. 79-86.
- [16] GFD.80 "The Open Grid Services Architecture, Version 1.5", I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam, J. Treadwell, J. Von Reich. Open Grid Forum, September 5, 2006.
- [17] 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.
- [18] Ngo, C., Y.Demchenko, C. de Laat, Toward a Dynamic Trust Establishment Approach for Multi-provider Intercloud Environment. The 4th IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2012), 3 - 6 December 2012, Taipei, Taiwan
- [19] Shibboleth Attribute Authority Service. [online] <http://shibboleth.net/>
- [20] OpenSAML. [online] <https://wiki.shibboleth.net/confluence/display/OpenSAML/>
- [21] OpenID. [online] <http://openid.net/>
- [22] CILogon [online] <http://www.cilogon.org/>
- [23] OASIS Identity in the Cloud Use Cases Version 1.0. OASIS Identity in the Cloud TC Note 01, 08 May 2012. [online] <http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html>
- [24] Moonshot Project [online] <https://community.ja.net/groups/moonshot>
- [25] IETF Working Group Application Bridging for Federated Access Beyond web (ABFAB) [online] <http://datatracker.ietf.org/wg/abfab/>
- [26] OpenStack KeyStone [online] <http://docs.openstack.org/developer/keystone/>
- [27] Demchenko Y. Virtual Organisations in Computer Grids and Identity Management. - Elsevier Information Security Technical Report - Volume 9, Issue 1, January-March 2004.
- [28] Demchenko, Y., L.Gommans, C. de Laat, M.Steenbakkers, V.Ciaschini, V.Venturi, VO-based Dynamic Security Associations in Collaborative Grid Environment, COLSEC2006 Workshop, Proc. Intl Symp on Collaborative Technologies and Systems CTS2006, 14-17 May, 2006.
- [29] Garzoglio, G., et al, Definition and Implementation of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware in OSG and EGEE, Journal of Grid Computing 7 (3), 2009, pp. 297-307
- [30] García-Espín, J. A., J. F.Riera, S. Figuerola, E. López, A Multi-tenancy Model Based on Resource Capabilities and Ownership for Infrastructure Management. Proc. The 4th IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2012), 3 - 6 December 2012, Taipei, Taiwan.
- [31] "Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0, OASIS standard," OASIS, SAML, Mar. 2005. [Online]. Available: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [32] Kaila, P., OAuth and OpenID 2.0, From End-to-End to Trust-to-Trust, 2008. [online] <https://www.zotero.org/jod999/items/itemKey/S449GVRK>
- [33] Demchenko Y., L. Gommans, C. de Laat. "Using SAML and XACML for Complex Resource Provisioning in Grid based Applications". In Proceedings IEEE Workshop on Policies for Distributed Systems and Networks (POLICY 2007), Bologna, Italy, 13-15 June 2007.
- [34] Chadwick, D., K. Siu, C. Lee, Y. Fouillat, D. Germonville, Adding Federated Identity Management to OpenStack, Journal of Grid Computing, to appear, 2014.
- [35] Demchenko, Y., D.R. Lopez, J.A. Garcia Espin, C. de Laat, Security Services Lifecycle Management in On-Demand Infrastructure Services Provisioning, Proc The 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom2010), 30 November - 3 December 2010, Indianapolis, USA.
- [36] 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