ISO/IEC JTC1/SC32 Data Management & Interchange
WG2 Metadata

Title: Interim Study Period Report on Metadata for the Cloud Computing

Version : 1.5
Date of version : May 2012

Authors : Baba Piprani CA
Ewelina Szczekocka PL

Contributors :

Description :

Keywords : metadata, interchange, interoperability, semantics
Theme :

Table of Contents

1 Introduction

1.1 Motivation

- *we put Rationale from the study group proposal*

1. Cloud approach is a subject of a great interest of business domains (Telecommunication, etc) as well as public domains (Government, health, etc) that perceive potential huge benefits from operating in the Cloud environment
2. Focus on Interoperability (Interchange) aspects on the data and services level (in general resources level) is crucial as it refers to one of the primary opportunities of operating in the Cloud concerned with involvement of different partners in the purpose of the Cloud service delivery. Resources can be hosted by different partners, that work in federation and need to use each other resources.
3. There are already several standards candidates in ISO/IEC JTC1 SC32 purposed for interoperability and interchange and it is a need to check to what extend they already support a cloud case

1.2 Cloud Computing concepts

1.2.1 Cloud Computing definition from ITU-T TR FG Cloud (based on NIST definition)

Cloud computing: A model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service-provider interaction. **Cloud computing enables cloud services.**

1.2.2 Cloud computing features

There are several cloud computing features, called cloud computing essential characteristics (provided by NIST, ongoing work on ISO/IEC JTC1 SC38 and ITU-T TR FG Cloud).

The essential characteristics are:

- **On-demand self-service**: A cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's cloud service provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The cloud service provider's computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources that are dynamically assigned and reassigned according to user demand. There is a sense of location independence in that

the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify the location at a higher level of abstraction (e.g., country, state, data centre). Examples of resources include storage (typically on hard or optical disc drives), processing, memory (typically on DRAM), network bandwidth, and virtual machines.

- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the cloud service user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured service: Cloud systems automatically control and optimize resource use (e.g., storage, processing and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., the number of active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the cloud service provider and cloud service user of the utilized service.

Another important feature, considered also to be included to the set of essential characteristics by ISO/IEC JTC1 SC38, is multi-tenancy.

Multi-tenancy [b-SC38 N430]: A characteristic of cloud in which resources are shared amongst multiple cloud tenants. There is an expectation on the part of the cloud tenant that its use of the cloud is isolated from other tenants' use of any shared resources; that tenants in the cloud are restricted from accessing or affecting another tenant's assets; that the cloud tenant has the perception of exclusive use of, and access to, any provisioned resource. The means by which such isolation is achieved vary in accordance with the nature of the shared resource, and can affect security, privacy and performance.
Resource: Any kinds of resources to be shared to compose cloud services, including computing power, storage, network, database, and applications

1.2.3 Cloud Computing deployment models

- **Private cloud** [b-NIST DFN]: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud** [b-NIST DFN]: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public cloud** [b-NIST DFN]: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud: The cloud infrastructure is a composition of two or more clouds using different deployment models (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

NOTE - It should be noted that the cloud-deployment models do not reflect where services, platforms, applications, or resources are actually hosted. For example, a private cloud can be hosted internally (on site) or externally (outsourced).

1.2.4 Cloud Service Models

Cloud service models (called by ITU-T cloud service categories) identified so far by NIST are:

- **Cloud software as a service (SaaS):** A category of cloud services where the capability provided to the cloud service user is to use the cloud service provider's applications running on a cloud infrastructure.
  NOTE - All applications have the common characteristic to be non-real-time and may be of different kinds, including IT and business applications, and may be accessible from different user devices. The cloud service user does not manage or control the underlying cloud infrastructure, with the possible exception of limited user-specific application configuration settings.

- **Cloud platform as a service (PaaS):** A category of cloud services where the capability provided to the cloud service user is to deploy user-created or acquired applications onto the cloud infrastructure using platform tools supported by the cloud service provider.
  NOTE - platform tools may include programming languages and tools for application development, interface development, database development, storage and testing. The cloud service user does not manage or control the underlying cloud infrastructure, but has control over the deployed applications and, possibly, over the application hosting environment configurations.

- **Cloud infrastructure as a service (IaaS):** A category of cloud services where the capability provided by the cloud service provider to the cloud service user is to provision processing, storage, intra-cloud network connectivity services (e.g. VLAN, firewall, load balancer, and application acceleration), and other fundamental computing resources of the cloud infrastructure where the cloud service user is able to deploy and run arbitrary application.

  NOTE - The cloud service user does not manage or control the resources of the underlying cloud infrastructure but has control over operating systems, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

The other important cloud service models proposed by ITU-T (ITU-T TR, FG Cloud) are:

Communications as a service (CaaS): A category of cloud services where the capability provided to the cloud service user is to use real-time communication and collaboration services.
NOTE - Communication and collaboration services include voice over IP, instant messaging, and video conferencing, for different user devices.

Network as a service (NaaS): A category of cloud services where the capability provided to the cloud service user is to use transport connectivity services and/or inter-cloud network connectivity services.
NOTE - NaaS services include flexible and extended VPN, bandwidth on demand, etc.

The above mentioned two models are crucial from telecom perspective and the other ones do not comprise them, as there are specific functions proposed by the models. Accordingly, SaaS doesn't comprise CaaS, as there are communication functions proposed by the model. In the same time IaaS doesn't comprise NaaS, as there are specfific network functions, that can be offered "as-a-Service". Those models are important in order to characterise ICT (Information Communication Technology) systems.

1.2.5 Interoperability aspects

Inter-cloud function
In order to enable delivery of a wide offer of complex services Cloud Service Providers may have to establish inter-cloud connections with other Cloud Service Providers. Then some services could be offered in the areas that are not delivered by the original Cloud Service Provider. The scope of inter-cloud connections is between two cloud domains, operated by two different Cloud Service Providers.

2 Scenarios, Use Cases and Ecosystem

2.1 Public Transport domain Scenarios

Canadian use cases

2.2 Telecom domain Scenarios

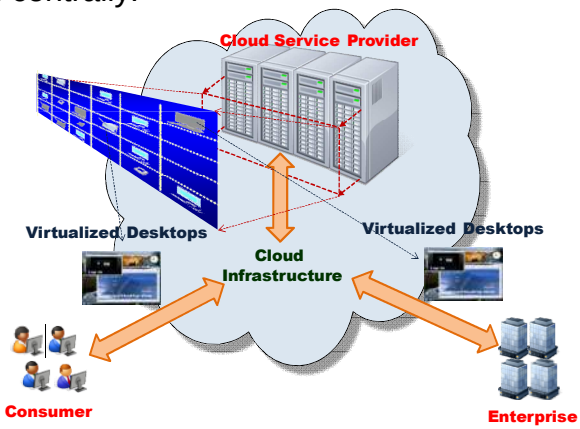
Candidates:
- *communication as a service example (CaaS)*
- *Desktop-as-a-Service example (IaaS)*
- *content delivery example (IaaS)*
- *Ecosystem? (roles, actors) from telecom perspective,*
- *add some specific information from domain, like service models etc. For instance for a telecom domain CaaS and DaaS will be very demanded)*

We consider several scenarios from telecom experience, such as:
- Communication as a Service example (CaaS), which belong to the unique service category, proposed by ITU-T.
- Desktop-as-a-Service example (DaaS) which is a kind of IaaS service category.
- Service Delivery Platform as a Service (SDPaaS), which is a kind of PaaS category.

Scenarios 2.2.1, 2.2.3 and 2.2.4 example of real world use case originate in ITU-T Technical Report FG Cloud and used in ISO/IEC JTC1 SC38 (in according to

proposed by German NB use cases methodology templates). The other scenarios also use German NB template for scenarios and use cases (SC38).

2.2.1 Scenario: Desktop as a Service

Usage scenario	
ITU-T01	Desktop as a Service
Description	DaaS is defined as the capability provided to the cloud service users to use virtualized desktops from a cloud service provider in the form of outsourcing. Instead of maintaining and running desktop operating system and applications on the local storage of remote clients, a central server located in the cloud retains the virtualized desktops and all of the used applications and data are kept and run centrally.  Based on application streaming and virtualization technologies, cloud service users can access desktop operating system and applications through a completely hosted system.
Domain	Generic
Goals and purpose	Identification of requirements for specific customer/provider relationships, in particular: • Consumers require accessing their desktop environments independently of locations, indeed, with their various devices. • Desktop environment needs to guarantee the business continuity and a recovery solution about a system failure. • Consumers desire to use their personal tasks separating business computing. Consumers eager to run various applications as in traditional PCs.

Stakeholders	***Actor***	***Roles***
	IaaS Provider	Cloud service provider
	Consumer	Cloud service user
	Enterprise	Cloud service user
Software layers	IaaS	
Deployment model	Private, public	
Components	***Component***	***Description***
	Virtual desktop environment	Virtual environment provided to the cloud service user.
	VDDP	Virtual desktop delivery protocol.
New specifications required between the actors	Identification of specification (and standardization) requirements (derived from the corresponding entry in the use case descriptions)	
Related use cases	**ITU-T01.01 - ITU-T01.03**	

2.2.1.1 Use Case: Consumer/Provider Interaction

Technical use case		
ITU-T01.01	**Consumer/Provider Interaction**	
Description	A **consumer** accesses and uses data or applications in a **IaaS provider** which offers **virtual desktop** service. A **consumer** can enjoy the environment with all programs and applications which are identical with those of traditional PCs. Of course, the **consumer** can choose the virtual hardware specification of its virtual desktops. If necessary, the **environment** (i.e. operating system) can be changed to another one immediately. All the **consumer** has to do is keeping up with a password since all data are totally stored and managed in the CSP.	
Actors and roles	***Actor***	***Roles***
	IaaS Provider	Cloud Service Provider
	Consumer	Cloud Service User
Primary Actor	Consumer	

<table>
<tr><td>Goals and aspirations for the UC</td><td colspan="2">The use case illustrates necessary interactions between Consumer and IaaS provider.</td></tr>
<tr><td>Components</td><td>Component</td><td>Description</td></tr>
<tr><td></td><td>Virtual desktop environment</td><td>Virtual environment provided to the service user.</td></tr>
<tr><td></td><td>VDDP</td><td>Virtual desktop delivery protocol.</td></tr>
<tr><td>Preconditions</td><td colspan="2">IaaS provider and consumer have an agreed Contract/SLA.</td></tr>
<tr><td>Criteria for success</td><td colspan="2">The consumer should send information about authentication (i.e. password). The IaaS provider offers virtual desktop environment of corresponding data such as OS, applications, and user data by VDDP. In case of the consumer’s change in the virtual desktop environment including virtual hardware specification, the consumer can transfer additional information related with selection.</td></tr>
<tr><td>New specifications required between the actors</td><td colspan="2">TBD</td></tr>
</table>

2.2.1.2 Use Case: Enterprise/Provider Interaction

<table>
<tr><th colspan="3">Technical use case</th></tr>
<tr><td>ITU-T01.02</td><td colspan="2">Enterprise/Provider Interaction</td></tr>
<tr><td>Description</td><td colspan="2">An enterprise using virtual desktop service from a IaaS provider for its internal processes is included in this use case. In this scenario, the enterprise can select applications or OS in the DaaS service for certain enterprise functions. Unlike the use case between a consumer and a IaaS provider, the enterprise normally uses storage for backups. Also, the enterprise can overcome peak loads and save energy by requesting the IaaS provider online to increase or decrease the number of virtual desktops, respectively.</td></tr>
<tr><td>Actors and roles</td><td>Actor</td><td>Roles</td></tr>
<tr><td></td><td>IaaS Provider</td><td>Cloud service provider</td></tr>
<tr><td></td><td>Consumer</td><td>Cloud service user</td></tr>
<tr><td>Primary Actor</td><td colspan="2">Enterprise</td></tr>
</table>

Goals and aspirations for the UC	The use case illustrates necessary interactions between **enterprise** and **IaaS provider**.
Components	***Component*** / ***Description*** **Virtual desktop environment** — Virtual environment provided to the service user. **VDDP** — Virtual desktop delivery protocol.
Preconditions	**IaaS provider** and **enterprise** have an agreed Contract/SLA.
Criteria for success	This case is similar to that between a **consumer** and a **IaaS provider** (ITU-T001.01, 9.3.1.1) except controlling the number of the virtual desktops. The **enterprise** can send warning information when abnormal situation (i.e. peak load) occurs.
New specifications required between the actors	**TBD**

2.2.1.3 Use Case: Enterprise/Consumer/Provider Interaction

Technical use case	
ITU-T01.03	**Consumer/Enterprise/Provider Interaction**
Description	In this use case, the **enterprise** makes the **consumer** do works with its internal processes at the outside of the enterprise by transferring virtual desktops and related data through the **IaaS provider**. Contrary to above two cases, the **consumer** cannot select applications freely and more limitations to access data in the **enterprise** may exist than at inside of the **enterprise**. Whenever the consumer connects with the **IaaS provider**, the **IaaS provider** sends feedback data to the **consumer** by accessing the enterprise to handle or bypass corresponding data.
Actors and roles	***Actor*** / ***Roles*** **IaaS Provider** — Cloud service provider **Consumer** — Cloud service user **Enterprise** — Cloud service user
Primary Actor	Enterprise
Goals and aspirations for the UC	The use case illustrates necessary interactions between

	consumer, **enterprise**, and **IaaS provider**.
Components	***Component*** / ***Description*** **VDDP** / Virtual desktop delivery protocol.
Preconditions	**IaaS provider** and **enterprise** have an agreed Contract/SLA.
Criteria for success	Among an **enterprise**, a **consumer**, and a **IaaS provider**: Information for authentication flows from the consumer to the enterprise through the **IaaS provider**. Once the **consumer** is identified, information regarding internal processes is transferred to the **IaaS provider** and it is dispatched to the end-user by **VDDP**. The **consumer's** output data is stored to the **IaaS provider** or the **enterprise** but there is no path for selection information as in the first case since the **consumer** cannot have an authority to alter the virtual desktop environment.
New specifications required between the actors	**TBD**

2.2.2 Scenario: Communication as a Service - Unified Communication

Usage scenario	
ITU-T02	Communication as a Service – Unified Communication (UCaaS)
Description	Communication as a Service – Unified Communication is defined as the capability provided to the cloud service users, that is to use real time communication functionalities from a cloud service provider in a flexible way. Those functionalities can be embedded in web applications accessible e.g. via Internet. This is a kind of Communication as a Service (CaaS). CaaS - is a category of cloud services, where the capability provided to the cloud service user is to use real-time communication and collaboration services. (Communication and collaboration services include voice over IP, instant messaging, and video conferencing, for different user devices).The unified communication means switch in using different kinds of communication agile and transparent for the users, depending on their dynamically changed accessibility. It is a comprehensive, converged communication system for real time data, voice, video, communication, unified messaging for fixed and mobile systems, with presence management. It enables more effective and secure way of personal communication, concerned with moving the user session between different devices and different kind of communication. It should be used with different devices, PC, tablet and mobile

<table>
<tr><td></td><td>terminals.
<UcaaS schema>
Real time Communication features can be accessible in the Cloud and variety of business models are possible, like different cloud service providers can deliver different kinds of communication and it can be integrated into a one system with a simple web interface to the users. On the top of the services a provisioning system will enable a smooth provisioning of the particular real time communication features, possibly of different third parties, but for the user it will be a single bill for the usage, enabling a distinction of kinds of communication used.
Cloud service users can access the unified real time communication system in a completely hosted way.
The unified real time communication system can be enriched with different value-added functionalities, like different IT features.
Note: It is possible, that some solutions can use the cloud infrastructure (IaaS) to provide real time communication, that is not available via Web. In this case we called the services “cloud-based services” as distinct from “cloud services”.</td></tr>
<tr><td>Domain</td><td>Communication and collaboration</td></tr>
<tr><td>Goals and purpose</td><td>Identification of requirements for specific user - provider relationships, in particular:
Cloud service users MUST have possibility to communicate with the others independently of their location and situations (e.g. in the office, at home, in the way to/from the office, in car, during the conference etc.), with various devices and with respect to the users profiles (like presence feature)
Real Time Communication system delivered by cloud service provider MUST guarantee the communication continuity
Real Time Communication system delivered by cloud service provider MUST guarantee relevant security for the communication
Real Time Communication system delivered by cloud service provider MUST guarantee a recovery from a system failure</td></tr>
<tr><td>Stakeholders</td><td><table><tr><th>Actor</th><th>Roles</th></tr><tr><td>Cloud Service Provider (CSP)</td><td>CaaS Provider</td></tr></table></td></tr>
</table>

	Cloud Service Provider (CSP)	IaaS Provider
	Cloud Service User (CSU)	Consumer
	Cloud Service User (CSU)	Enterprise
Software layers	IaaS, CaaS	
Deployment model	Private, Public	
Components	***Component***	***Description***
New specifications required between the actors	Identification of specification (and standardization) requirements (derived from the corresponding entry in the use case descriptions)	
Related use cases		

2.2.3 Scenario: Service Delivery Platform as a Service (SDPaaS)

Usage scenario	
ITU-T03	Service Delivery Platform as a Service (SDPaaS)
Description	SDPaaS is the capability provided to the Cloud Service User (CSU) to use service delivery platform (SDP) functionalities, and services provided by a Cloud Service Provider, and the capability provided to a CSP to deploy, control and manage service delivery platform functionalities. SDPaaS allows a CSU to access, as a service, functionalities and services offered by a CSP similar to those offered by a traditional SDP. Services offered by a traditional SDP include different types of services (e.g. telecom services, Internet access and portal services, etc.). Functionalities offered by a traditional SDP include service creation, service execution and service delivery management, as the functional groups: ▪ The service creation functional group provides capabilities to realize an application development environment for application developers.

<table>
<tr><td></td><td>

The service execution functional group provides capabilities to support a service execution environment.
The service delivery management functional group provides capabilities to realize the management of different aspects, provisioning of applications and charging, to ensure the proper functioning of the service creation and service execution functional groups, and to provide associated delivery functionalities.

SDPaaS exposes services and functionalities, similar to those offered by a traditional SDP, as cloud services:

Services are provided as SaaS/CaaS services.
Functionalities are provided as PaaS services

</td></tr>
<tr><td>Domain</td><td>Generic</td></tr>
<tr><td>Goals and purpose</td><td>Identification of requirements for specific customer/provider relationships, in particular:

Consumers require accessing their desktop environments independently of locations, indeed, with their various devices.
Desktop environment needs to guarantee the business continuity and a recovery solution about a system failure.
Consumers desire to use their personal tasks separating business computing.
Consumers eager to run various applications as in traditional PCs.

</td></tr>
<tr><td>Stakeholders</td><td>
<table>
<tr><th>Actor</th><th>Roles</th></tr>
<tr><td>Cloud service provider</td><td>PaaS provider</td></tr>
<tr><td>Cloud service user</td><td>Consumer</td></tr>
<tr><td>Cloud service partner</td><td>Developer</td></tr>
<tr><td>Cloud service user</td><td>Enterprise</td></tr>
</table>
</td></tr>
<tr><td>Software layers</td><td>PaaS, SaaS/CaaS</td></tr>
<tr><td>Deployment model</td><td>Private, public</td></tr>
</table>

Components	***Component***	***Description***
	Service Delivery Platform **Cloud Services**	
New specifications required between the actors	Identification of specification (and standardization) requirements (derived from the corresponding entry in the use case descriptions)	
Related use cases	**ITU-T03.01 - ITU-T03.03**	

2.2.3.1 Use Case: Consumer/Provider Interaction

Technical use case		
ITU-T03.01	**Consumer/Provider Interaction**	
Description	A **consumer** accesses and uses data or applications in a **IaaS provider** which offers **virtual desktop** service. A **consumer** can enjoy the environment with all programs and applications which are identical with those of traditional PCs. Of course, the **consumer** can choose the virtual hardware specification of its virtual desktops. If necessary, the **environment** (i.e. operating system) can be changed to another one immediately. All the **consumer** has to do is keeping up with a password since all data aretotally stored and managed in the CSP.	
Actors and roles	***Actor***	***Roles***
	IaaS Provider	Cloud Service Provider
	Consumer	Cloud Service User
Primary Actor	Consumer	
Goals and aspirations for the UC	The use case illustrates necessary interactions between Consumer and IaaS provider.	
Components	***Component***	***Description***
	Virtual desktop environment	Virtual environment provided to the service user.
	VDDP	Virtual desktop delivery protocol.
Preconditions	**IaaS provider** and **consumer** have an agreed Contract/SLA.	

Criteria for success	The **consumer** should send information about authentication (i.e. password). The **IaaS provider** offers **virtual desktop environment** of corresponding data such as OS, applications, and user data by **VDDP**. In case of the consumer's change in the **virtual desktop environment** including virtual hardware specification, the consumer can transfer additional information related with selection.
New specifications required between the actors	**TBD**

2.2.3.2 Use Case: Enterprise/Provider Interaction

Technical use case		
ITU-T03.02	**Enterprise/Provider Interaction**	
Description	An **enterprise** using virtual desktop service from a **IaaS provider** for its internal processes is included in this use case. In this scenario, the **enterprise** can select applications or OS in the DaaS service for certain enterprise functions. Unlike the use case between a **consumer** and a **IaaS provider**, the **enterprise** normally uses storage for backups. Also, the **enterprise** can overcome peak loads and save energy by requesting the **IaaS provider** online to increase or decrease the number of virtual desktops, respectively.	
Actors and roles	***Actor***	***Roles***
	IaaS Provider	Cloud service provider
	Consumer	Cloud service user
Primary Actor	Enterprise	
Goals and aspirations for the UC	The use case illustrates necessary interactions between **enterprise** and **IaaS provider**.	
Components	***Component***	***Description***
	Virtual desktop environment	Virtual environment provided to the service user.
	VDDP	Virtual desktop delivery protocol.
Preconditions	**IaaS provider** and **enterprise** have an agreed Contract/SLA.	
Criteria for success	This case is similar to that between a **consumer** and a **IaaS**	

	provider (ITU-T001.01, 9.3.1.1) except controlling the number of the virtual desktops. The **enterprise** can send warning information when abnormal situation (i.e. peak load) occurs.
New specifications required between the actors	**TBD**

2.2.3.3 Use Case: Enterprise/Consumer/Provider Interaction

Technical use case		
ITU-T03.03	**Consumer/Enterprise/Provider Interaction**	
Description	In this use case, the **enterprise** makes the **consumer** do works with its internal processes at the outside of the enterprise by transferring virtual desktops and related data through the **IaaS provider**. Contrary to above two cases, the **consumer** cannot select applications freely and more limitations to access data in the **enterprise** may exist than at inside of the **enterprise**. Whenever the consumer connects with the **IaaS provider**, the **IaaS provider** sends feedback data to the **consumer** by accessing the enterprise to handle or bypass corresponding data.	
Actors and roles	***Actor***	***Roles***
	IaaS Provider	Cloud service provider
	Consumer	Cloud service user
	Enterprise	Cloud service user
Primary Actor	Enterprise	
Goals and aspirations for the UC	The use case illustrates necessary interactions between **consumer**, **enterprise**, and **IaaS provider**.	
Components	***Component***	***Description***
	VDDP	Virtual desktop delivery protocol.
Preconditions	**IaaS provider** and **enterprise** have an agreed Contract/SLA.	
Criteria for success	Among an **enterprise**, a **consumer**, and a **IaaS provider**: Information for authentication flows from the consumer to the enterprise through the **IaaS provider**. Once the **consumer** is identified, information regarding internal processes is transferred to the **IaaS provider** and it is dispatched to the end-user by	

	VDDP. The **consumer's** output data is stored to the **IaaS provider** or the **enterprise** but there is no path for selection information as in the first case since the **consumer** cannot have an authority to alter the virtual desktop environment.
New specifications required between the actors	**TBD**

2.2.4 Internet television ecosystem example

In the example, we consider a federated ecosystem of cloud-based entertainment services, where multiple commercial retailers interoperate in order to offer a complex service including:

- a streaming video,
- download of premium video content,
- ownership of the above recorded by a central rights locker.

There are involved several actors, such as:

- Media retailer (Cloud Service Provider) - company A,
- Streaming service provider (Cloud Service Provider) - company B,
- Rights locker (Cloud Service Provider) - company C,
- Internet TV service user (Cloud Service User).

Media Retailer "A" - Company "A":
Media retailer could be for instance:

- a video-retailing website,
- a telco IPTV service,
- a hotel entertainment system,
- an adjunct to a Pay-TV,
- other broadcaster, or similar.

This actor:

- operates a cloud service that offers a consumer-facing catalogue of entertainment content, with recommendations, payment processing, etc.
- is able to offer content for sale or rent to the consumer through a cloud application, collect payment, and authorise use of the media.
- is also able to determine that the consumer already owns a given title by reference to the Rights Locker cloud service operated by company "C".
- can use cloud service orchestration to find a suitable cloud streaming or download source for a given media delivery.

Streaming Service CSP "B"
This actor:

- delivers media (stream) to consumers
- delivers DRM licences

Rights Locker "C"
This actor:

- keeps a record of authorised devices and media owned by a customer account
- is able to authorise a set of devices to be used with a customer's account

Scenario:

In this scenario:

1. Media Retailer "A" is responsible for finding and invoking a suitable Streaming Service CSP "B" from the cloud. This decision is based on several parameters, such as:

- location,
- content availability,
- available stream capacity,
- cost to the retailer, etc.

Once this is determined, Media Retailer's (A) application on the Internet TV will pass the appropriate URL to the media player function (by pointing to an MPEG DASH MPD file).

2. "B" provides a service that fulfils the delivery of media to consumers when requested by another cloud service. "B" provides stream fulfilment for numerous Media Retailers in addition to "A". "B" also delivers DRM licences for any protected content, when authorised to do so by the relevant Media Retailer.
3. Company "C" acts as the ecosystem's Rights Locker, the central governing entity within the ecosystem. "C" keeps a record of which devices are authorised and which media titles are owned by a given consumer account. In this way, content that was bought through one Media Retailer may also be watched using the service of another Media Retailer, possibly using the same or a different Streaming Service CSP.
   In this example, "C" is also responsible for authorising a set of devices to use the consumer's account. This requires tracking the various DRMs that are in use, verifying the total number of authorised devices, and supplying them with "domain" credentials for each DRM as required. In this way, content that is delivered to the consumer can be played on any of the consumer's authorised devices without fear of it being more widely distributed.

Implementation (Cloud Computing service models):
Media Retailer's (A) service is implemented as a SaaS, since it communicates directly with a user through a cloud application running with the browser and communicating with a back-end. The solution provides a rich catalogue experience with recommendations, ratings, social media connections, account management, billing, special offers, etc.

"B"'s streaming service is implemented as a PaaS, since it is a generic streaming platform that delivers stored content using standardised streaming protocols. Differentiation is based on "B"'s location, catalogue, and pricing of the service. In this scenario, "B" will bill "A" for the cost of media delivery.

"C"'s Rights Locker service is implemented as a PaaS, since for this scenario it is invoked by "A"'s application, not by the human user. While "C"'s Rights Locker service provides a rich and complex API, and is specific to this particular vertical application, it does not in itself provide a service to the consumer. The only direct consumer UI is that "C" provides a web-based account management page; however this is a "management plane" function and not part of daily consumer operation (such as buying and/or watching a movie).

3 Examples of Cloud Computing solutions

3.1 Amazon Web Services

- to add Amazon example to the list: http://aws.amazon.com/ec2/

4 Requirements

- requirements on Interchange in the Cloud (Cloud Computing)
- requirements will come from Use Cases

4.1 Public Transport domain requirements

4.2 Telecom domain requirements

We can bring in some requirements related to cloud architecture that can be of importance for interchange and interoperability issues (like from ITU-T TR, Part 2, 02/2012):

1. Cloud deployments MUST support many standards within the same cloud infrastructure, e.g. in terms of resource allocation, orchestration, or Cloud Service User access.
The cloud architecture must allow and support the evolution of these standards, without requiring disruptive infrastructure changes for Cloud Service Provider.

2. A Cloud Service Provider MUST be able to support multiple standards within the same architecture and migrate to a newer standard, if they so wish, without having to change everything in the CSP network or lose the existing customer base.

3. The cloud architecture MUST enable multiple deployment models (like private, public, hybrid), cloud service categories (like IaaS, PaaS, SaaS - according to NIST or additionally CaaS, NaaS - important from telecom perspectives to form ICT systems). It is possible, that different service categories will co-exist in the same cloud deployment

5 Domain model (examples)

- telecom domain model
- other models

6 Current Cloud Computing Related Standards Work

- *architectural components (what we have from SC38)*
- *the standardisation for interchange (ISO/IEC SC32)*

7 A preliminary model for metadata in the Cloud

7.1 High level overview metamodel for the Cloud Computing

7.2 Example Metadata for Cloud components

7.3 A Preliminary metamodel for the Cloud Computing

7.4 Validation: Mapping Use Case examples to the preliminary metamodel for the Cloud Computing

8 Gap Analysis between the Cloud Computing models and the current standards of SC32

Recommendations

goal: to set up NWIP for new Part of MFI standard 19763 – Metamodel for the Cloud Computing model registration" (one of the Clauses will be Cloud Service Registration and using the model as defined in MFI Part 7)

Note: Our suggestion is to stay at the service level, as this is the point of an interaction with the Consumer.

9 References

1. ISO/IEC JTC1 SC32 MFI (19763)
2. ITU-T TR FG Cloud, 2012, http://www.itu.int/ITU-T/newslog/Cloud+Computing+And+Standardization+Technical+Reports+Published.aspx
3. ISO/IEC JTC1 N585, German National Body Contribution on Standing Document for Usage Scenario Methodology, 2012