

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG Cloud TR

Version 1.0
(02/2012)

Focus Group on Cloud Computing
Technical Report

**Part 1: Introduction to the cloud ecosystem:
definitions, taxonomies, use cases and high-
level requirements**



FOREWORD

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. The ITU-T Focus Group on Cloud Computing (FG Cloud) was established further to ITU-T TSAG agreement at its meeting in Geneva, 8-11 February 2010, followed by ITU-T study group and membership consultation.

Even though focus groups have a parent organization, they are organized independently from the usual operating procedures of the ITU, and are financially independent. Texts approved by focus groups (including Technical Reports) do not have the same status as ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Technical Report may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU-T Focus Group participants or others outside of the Technical Report development process.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

1.	Scope.....	1
2.	Definitions	1
2.1	Cloud related basic terminology.....	1
2.2	Cloud deployment models.....	3
2.3	Inter-cloud	3
2.4	Other cloud related definitions	4
3	Abbreviations and acronyms	5
4	Introduction to cloud computing in telecommunications	6
4.1	The emergence of the cloud computing model	6
4.2	Opportunities for market players through cloud computing	6
5	Cloud ecosystem.....	7
5.1	Actors and Roles of a Cloud ecosystem.....	7
5.2	Scenarios of inter-cloud.....	9
6	Cloud services taxonomy and mappings to cloud service categories.....	11
6.1	Cloud services mapping	11
7	Use cases.....	12
8	High-level requirements to be considered for cloud infrastructure and cloud services	13
8.2	General requirements.....	13
8.3	Requirements for cloud services	15
8.4	SLA support.....	16
8.4	Management	19
8.5	Inter-cloud support	19
Annex A	Use cases	23
A.1	From the perspective of cloud service users and cloud service providers	23
A.2	From the inter-cloud perspective.....	37
Appendix I	Details on desktop as a service (DaaS).....	48
Appendix II	Schema-mapping techniques to support multi-tenancy.....	50
Appendix III	Details on SLA for cloud computing	52
III.1	Example of SLA metrics	52
III.2	Details on SLA measurement	54

Appendix IV Additional details on business aspects in a cloud ecosystem.....	56
IV. 1 Examples of a business-value chain	56
Appendix V Detailed scenarios of cloud interaction involving the inter-cloud role	58
V.1 Inter-cloud scenario with QoS control	58
V.2 Inter-cloud scenario with cloud service composition	58
Appendix VI Details on mobile cloud	60
VI.1 Configuration of a mobile cloud.....	60
Bibliography.....	62

1. Scope

Definitions, use cases, technologies, players, risks and benefits of cloud ecosystems are still an evolving paradigm.

The scope of this Technical Report is to provide an introduction to cloud ecosystems, focusing on integration and support of the cloud computing model and technologies in telecommunication environments. The Technical Report addresses:

- Cloud computing related definitions and taxonomies based on the current status of the art
- Actors and roles of a cloud ecosystem
- Scenarios of inter-cloud
- A set of relevant telecommunication-centric use cases
- High-level requirements for cloud infrastructure and cloud services

A companion Technical Report provides an introduction to cloud computing benefits from the telecommunication/ICT perspectives.

2. Definitions

2.1 Cloud related basic terminology

2.1.1 Cloud computing

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.

NOTE - It is considered from a telecommunication perspective that users are not buying resources but cloud services that are enabled by cloud computing environments.

The cloud computing model promotes availability and is composed of five essential characteristics, five cloud service categories and four deployment models.

2.1.2 Cloud service

Cloud service: A service that is delivered and consumed on demand at any time, through any access network, using any connected devices using cloud computing technologies.

2.1.3 Cloud ecosystem actors

Cloud service user (CSU): A person or organization that consumes delivered cloud services.

NOTE – A CSU can include intermediate users that will deliver cloud services provided by a cloud service provider (CSP) to actual users of the cloud service, i.e. end users. End users can be persons, machines, or applications.

Cloud service provider (CSP): An organization that provides and maintains delivered cloud services.

Cloud service partner (CSN): A person or organization that provides support to the building of the service offer of a cloud service provider (e.g. service integration).

2.1.4 Cloud computing essential characteristics

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.

2.1.5 Cloud service categories

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.

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.

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).

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.

2.2 Cloud 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).

2.3 Inter-cloud

Inter-cloud computing: Inter-cloud computing allows on-demand assignment of cloud resources, including computing, storage and network, and the transfer of workload through interworking of cloud systems.

NOTE 1 - In the context of the ITU-T FG Cloud deliverables, the term “inter-cloud” is used instead of “inter-cloud computing”.

NOTE 2 - From the view point of a CSP, inter-cloud computing can be implemented in different manners, including inter-cloud peering, inter-cloud service broker and inter-cloud federation. These manners correspond to distinct possible roles that a CSP can play when interacting with other CSPs.

Inter-cloud peering: direct inter-connection between two CSPs.

Inter-cloud service broker (ISB): indirect interconnection between two (or more) CSPs achieved through an interconnecting CSP which, in addition to providing interworking service functions between the interconnected CSPs, also provides brokering service functions for one (or more) of the interconnected CSPs. ISB also covers the case in which one (or more) of the interconnected entities receiving the brokering service is a cloud service user (CSU).

NOTE 1 - Brokering service functions generally include, but are not limited to, the following three categories: service intermediation, service aggregation and service arbitrage.

Inter-cloud federation: a manner to implement inter-cloud computing in which mutually trusted clouds logically join together by integrating their resources. Inter-cloud federation allows a CSP to dynamically outsource resources to other CSPs in response to demand variations.

2.4 Other cloud related definitions

Desktop as a service (DaaS): The capability provided to the cloud service user to use virtualized desktops from a cloud service provider in the form of outsourcing.

NOTE - A central server located in the cloud retains the virtualized desktops instead of maintaining and running desktop operating system and applications on the local storage of remote clients, 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.

Cloud communication centre: A cloud communication centre (service) enables advanced features for the customer-enterprise interaction using the communication and management capabilities provided by a cloud-based telecommunication infrastructure (managed by the cloud service provider).

NOTE - Such capabilities include for example: management in the cloud of communication centre relevant resources, such as customer resources, enterprise agent resources, media storage resources, content resources, transport resources and communication resources; access of fixed and mobile customers and enterprise agents via a unified client, such as a Web browser; sharing of enterprise applications which are common among different enterprises; and application charging to enterprises on a per-resource usage basis.

Service delivery platform as a service (SDPaaS): The capability provided to the cloud service user to use service delivery platform (SDP) functionalities and services provided by a cloud service provider, and the capability provided to a cloud service provider to deploy, control and manage SDP functionalities.

NOTE - SDPaaS may be implemented via utilization and intermediation of different SaaS/CaaS and PaaS cloud services.

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.

Service delivery platform [b-Moriana-SDP2.0]: A system architecture or environment that enables the efficient creation, deployment, execution, orchestration and management of one or more classes of services.

SLA [b-CSA Glossary]: An abbreviated service agreement stating the technical performance promises made by a provider, including remedies for performance failures. An SLA is composed of three parts. The first part is a collection of promises made to subscribers, (2) a collection of

promises explicitly not made to subscribers, i.e., limitations, and (3) a set of obligations that subscribers must accept.

NOTE - In practice, an SLA may contain non-quantitative parameters, such as specific regulations, citizenship requirements, business process standards (e.g. ISO 20000). Cloud services may have different types of SLAs.

3 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms

API	Applications Programming Interface
ASP	Application Service Provider
BI	Business Intelligence
BSS	Business Support System
CaaS	Communications as a Service
CPU	Central Processing Unit
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
DaaS	Desktop as a Service
DRAM	Dynamic Random-Access Memory
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IT	Information Technology
IDC	Internet Data Centre
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IPTV	Internet Protocol Television
ISB	Inter-cloud Service Broker
ISP	Internet Service Provider
M2M	Machine-to-Machine
NaaS	Network as a Service
OSS	Operations Support System
PaaS	Platform as a Service
PC	Personal Computer
QoS	Quality of Service
SaaS	Software as a Service
SDP	Service Delivery Platform

SDPaaS SDP as a Service

SLA Service Level Agreement

VLAN Virtual Local Area Network

VM Virtual Machine

VPN Virtual Private Network

4 Introduction to cloud computing in telecommunications

4.1 The emergence of the cloud computing model

The term “cloud” was first introduced in 2008 to designate a new approach for service delivery through the network (the network schema is usually illustrated by a cloud in telecommunication architecture diagrams).

Software as a service (SaaS) emerged in the last five years as a new concept for accessing a software application (computing task) which can be described as "IT service-centric": SaaS can be seen as a software distribution model in which applications are hosted by a service provider and made available to customers over a network, typically the Internet, and where a single instance (virtual application) of the software runs on the SaaS provider servers, following a multi-tenant 1-to-N architecture, and charged on a per usage basis. The SaaS model has some similarity with the application service provider (ASP) model introduced in the beginning of 2000 as an evolution of the Internet service provider (ISP) model, but it is considered a more advanced model for managing (self-management and rapid provisioning), hosting (virtualization resources), software architecture modularization (multi-tenant API), and licensed applications instantiation under a usage-based transaction.

The recent development of high-bit-rate access and improvement of the network layer availability by major ISPs can be considered as the most important starting point for the emerging online/SaaS and cloud market.

Considering cloud computing as an evolution of ASP and some generalization of SaaS online services, with an extension to platform and infrastructure services (PaaS and IaaS), cloud computing can be also named network computing (or Internet computing).

4.2 Opportunities for market players through cloud computing

Cloud computing is changing the ICT ecosystem with emerging business roles and modification of the ICT industry value chain.

- Opportunities for small and medium enterprises
Small and medium enterprises consider the usage of cloud computing to improve flexibility and to reduce the cost of their IT systems. Furthermore, their needs for hardware and software ownership may be reduced.
- Opportunities for hardware and software providers

The hardware and software for the support of cloud services may be increased, since operators need to possess extensive hardware and software resources for economies of scale. This may promote business growth for hardware and software providers.

- Opportunities for large ICT enterprises

In general, cloud computing offers opportunities of business transformation for large ICT enterprises.

- Opportunities for other market players

Cloud computing provides opportunities for other market players, e.g. application developers, application integrators, application providers, content providers. Cooperation with operators of cloud services enables the creation of a broader market and win-win situations between operators and these market players.

5 Cloud ecosystem

In line with a general definition of a business ecosystem [b-HBR], a cloud computing business ecosystem (cloud ecosystem) is a business ecosystem of interacting organizations and individuals - the actors of the cloud ecosystem - providing and consuming cloud services.

5.1 Actors and Roles of a Cloud ecosystem

The following actors are identified in a cloud ecosystem:

- Cloud service users (CSU),
- Cloud service providers (CSP),
- Cloud service partners (CSN).

NOTE – The definitions of these actors are provided in clause 2.

Figure 1 illustrates the three actors involved in a cloud ecosystem.

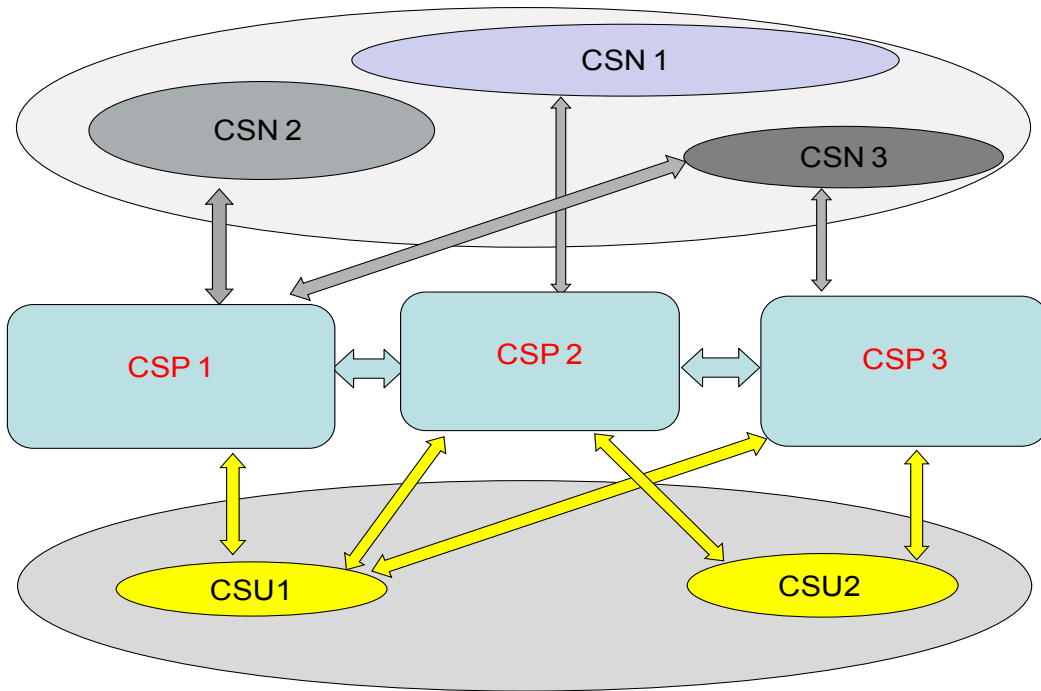


Figure 1 - The three actors of a cloud ecosystem

Figure 2 depicts the actors with some of their possible roles in a cloud ecosystem.

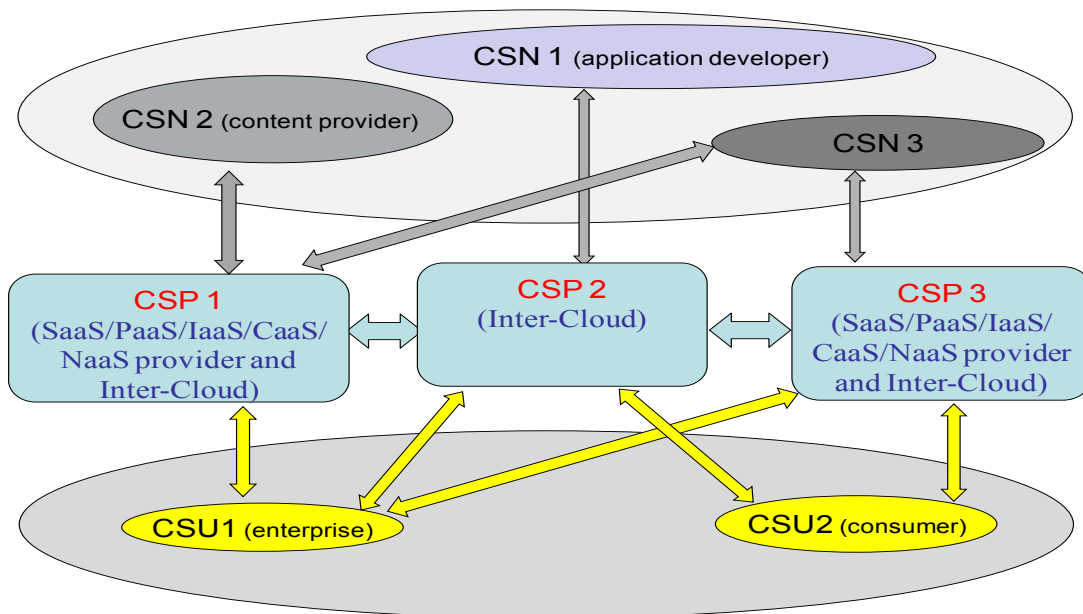


Figure 2 - Actors with some of their possible roles in a cloud ecosystem

The following provides a non-exhaustive list of possible roles that can be played by each of the three cloud eco-system actors:

- Cloud service provider (CSP):
 - Provider of SaaS and/or CaaS and/or PaaS and/or IaaS and/or NaaS

NOTE – a CSP may offer cloud services of one or more of these five cloud service categories.

- Inter-cloud:
 - Inter-cloud peering,
 - Inter-cloud service broker,
 - Inter-cloud federation
- Cloud service user (CSU):
 - Consumer,
 - Enterprise (including enterprise administrator),
 - Governmental/public institution
- Cloud service partner (CSN):
 - Application developer,
 - Content provider,
 - Software provider,
 - Hardware provider,
 - Equipment provider,
 - System integrator,
 - Auditor

Appendix IV provides some additional details on business aspects of a cloud ecosystem.

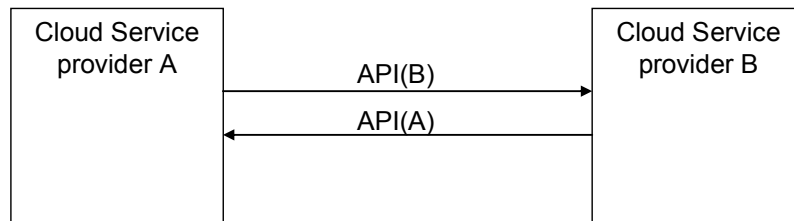
5.2 Scenarios of inter-cloud

This clause provides scenarios of inter-cloud involving the different inter-cloud roles identified in clause 5.1.

Appendix V describes detailed scenarios of cloud interaction involving the inter-cloud roles.

5.2.1 Scenario with inter-cloud peering

Two CSPs interwork directly with each other. Each CSP exposes its own API for cloud interworking, and the CSPs interwork with each other directly by using the other CSP's API. In Figure 3, CSP A interworks with CSP B using API provided by CSP B and vice versa.



API(X): API provided by Cloud Service provider X

Figure 3 – Inter-cloud peering

5.2.2. Scenario with inter-cloud federation

Mutually trusted CSPs logically join an alliance together. The common API for cloud interworking is defined in the alliance, and each CSP interworks with other CSPs in the alliance through the common API (Figure 4).

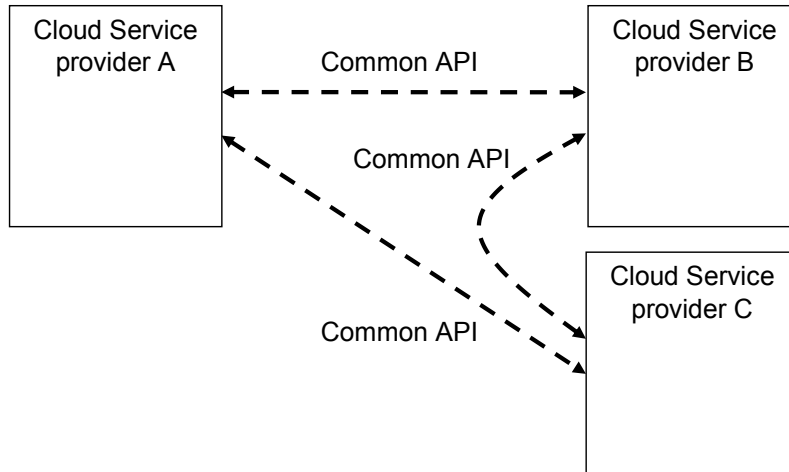
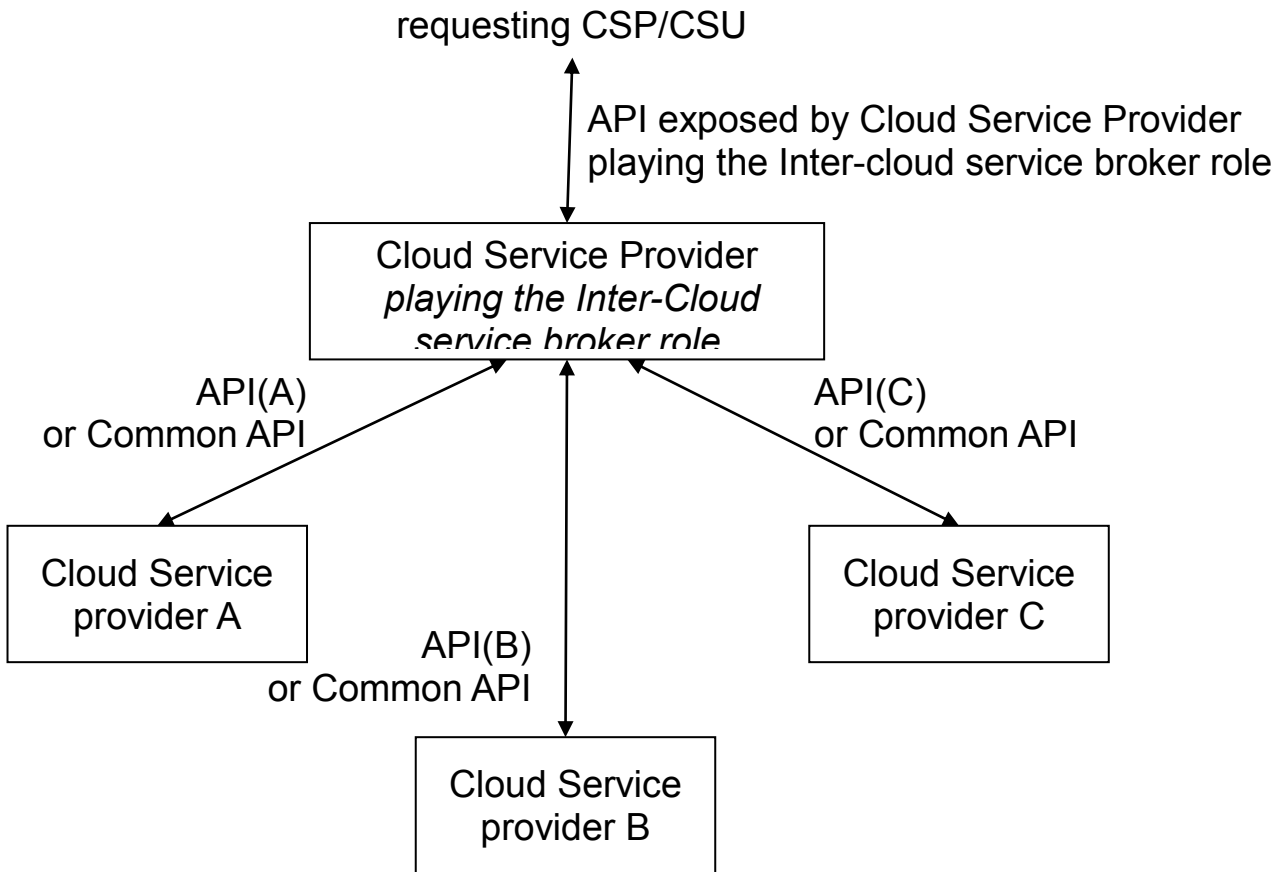


Figure 4 – Inter-cloud federation

5.2.3 Scenario with inter-cloud service broker

The scenario of inter-cloud with an inter-cloud service broker is shown in Figure 5. In this scenario, the CSP playing the inter-cloud service broker role receives a cloud service request from a cloud-service provider or a cloud-service user through its own API. The CSP playing the role of inter-cloud service broker, interworks with one or more other CSPs and provides brokering-service functions by integrating services provided by these CSPs. Interworking between the CSP playing the inter-cloud service broker role and the other CSPs, is established by either inter-cloud peering or inter-cloud federation.



API(X): API provided by Cloud Service provider
Figure 5 – Inter-cloud service broker

6 Cloud services taxonomy and mappings to cloud service categories

Clause 2 provides definitions for the following cloud service categories in a telecommunication-centric cloud ecosystem:

- SaaS
- IaaS
- PaaS
- NaaS
- CaaS

CaaS and NaaS are specialized service categories of a telecommunication-centric cloud ecosystem. Although services of these categories are assumed to be supported in different cloud deployment models, they fully empower the service offering of telecommunication service market players in a cloud ecosystem.

6.1 Cloud services mapping

Table 1 shows examples of mapping of some relevant cloud services to the identified cloud service categories.

Table 1 – Map of cloud services to cloud-service categories

	SaaS	PaaS	IaaS	NaaS	CaaS
Desktop as a service			X		
Service delivery platform as a service	X	X			X
Cloud communication centre	X				X
(Flexible and extended) VPN				X	
Bandwidth on demand				X	

7 Use cases

The following table identifies relevant use cases of a cloud ecosystem.

Details about each of these use cases are provided in Annex A.

Table 2 – Use cases

	Use case
From the perspective of cloud service users and cloud service providers	General use case of desktop as a service
	Specific use case of DaaS - Office automation of development-oriented enterprise
	Specific use case of DaaS - Customer service call centre
	Service delivery platform as a service (SDPaaS)
	Mobile Cloud
	Cloud migration and portability: Move three-tier application from on-premises to cloud
	Cloud migration and portability: Move three-tier cloud application to another cloud
	Cloud migration and portability: Move part of on-premises application to cloud to create “hybrid” application
	Cloud migration and portability: Hybrid cloud application that uses platform services
	Cloud migration and portability: Port the cloud application that uses platform services to another cloud
From the inter cloud perspective	User data inquiry and analysis based on massive data processing
	SLA mapping between CSP (inter-cloud service broker) and CSP
	Guaranteeing performance against an abrupt increase of the load
	Use case of guaranteeing performance regarding delay
	Guaranteed availability
	Service continuity
Market transactions via brokers	

8 High-level requirements to be considered for cloud infrastructure and cloud services

NOTE – As far as the requirements in this clause are concerned, the term “cloud infrastructure” is intended to address the capabilities to be supported by a cloud service provider (unless clearly specified otherwise).

The range of cloud services is very broad, thus a great number of requirements for cloud infrastructure and cloud services are expected.

This clause lists high-level requirements for cloud infrastructure and cloud services which should be considered by the actors of the cloud computing business.

It does not intend to mandate specific features, but proposes relevant considerations for further development of detailed specifications on requirements and capabilities of cloud infrastructure and cloud services.

8.2 General requirements

General requirements are as follows:

- **Multi-tenancy:** As defined in Clause 2.4, multi-tenancy is an essential characteristic of cloud systems aiming to provide isolation of the different users of the cloud system (tenants) while maximizing resource sharing among them. It is expected that multi-tenancy be supported at various levels of a cloud infrastructure.

NOTE - As an example, at the application level, multi-tenancy is a feature that allows a single instance of an application to satisfy several users at the same time. This results in the ability to consolidate several tenants within a single database and leverage the economy of scale. Some details about techniques for multi-tenancy are provided in Appendix II.

- **Service lifecycle management:** Cloud services are paid as used and can be started and ended anytime. Therefore, it is required that a cloud infrastructure supports automatic service provisioning. In addition, metering and charging settlement need to be provided for services that are dynamically created, modified and then released in virtual environments.
- **Security:** Security of each individual service needs to be ensured in the multi-tenant cloud environment, including when data and business logic move between servers to achieve optimal service.
It is also expected that a cloud infrastructure provides strict control for different tenants' access to different resources, to avoid the abuse of cloud resources and to facilitate the management of cloud service users by cloud service providers.
- **Responsiveness:** The cloud architecture is expected to enable early detection, diagnosis and fixing of infrastructure or service related problems.
- **Intelligent service deployment:** It is expected that the cloud architecture enables efficient use of resources in service deployment, i.e. maximising the number of deployed services while minimizing the usage of resources and still respecting the SLAs.

NOTE - For instance, the specific application characteristics (e.g. CPU-intensive, IO-intensive etc.) - which can be provided by application developers or via application monitoring - may help cloud service providers in making efficient use of resources.

- **Portability:** It is expected that a cloud infrastructure supports the portability of software and data over its underlying resources. It is also expected that cloud service providers be able to accommodate cloud workload portability (e.g. VM portability) with limited service disruption.
- **Interoperability:** It is expected to have available well-documented and well-tested specifications that allow heterogeneous systems in cloud environments to work together.
- **Regulatory aspects:** All applicable regulations shall be respected, including for privacy protection.
- **Accessibility:** It is expected that a cloud infrastructure supports capabilities for adaptation of cloud service user access to user requirements, including persons with disabilities and older persons with age-related disabilities. The usage of universal design criteria [b-UN-accessibility] should be considered in order to incorporate the needs of persons with disabilities and older persons with age-related disabilities at the design stage of cloud service user access interfaces.

NOTE - Applying universal design will also reduce expensive refits and redesign later.

It is expected that a cloud infrastructure supports capabilities to manage a cloud service user's personal profiles and, according to the profile of the user who wishes to access the cloud, to adapt – if and as needed - the cloud service user access. For example, persons with disabilities often gain access to assistive Technologies (ATs) in public access points, such as a library or an information kiosk, as well as at work and at home. They could rent the use of ATs from the cloud as required, reducing the cost of purchasing and consistently updating rarely used ATs.

Concerning the specific subject of ATs - ATs are typically only translated into a relatively small number of languages. It is expected that a cloud infrastructure provides AT translation capabilities so that this task is not left to each AT producer, thus contributing to making ATs more widely available.

- **Environmental sustainability:** a key characteristic of cloud computing is the capability to access, through broad network and thin clients, on-demand shared pools of configurable resources that can be rapidly provisioned and released. Cloud computing can then be considered in its essence as an ICT energy consumption consolidation model.

It is expected that cloud infrastructure deployments support mainstream technologies aiming to optimize energy consumption (e.g. in data centres) and application performance.

NOTE - examples of technologies include virtualization and multi-tenancy.

- **Service reliability, service availability and quality assurance:** Cloud service users demand for their services end-to-end quality of service assurance, high levels of reliability and continued availability to their cloud service providers.

NOTE - Service level agreements (SLAs) can be structured to meet the specific demands of the various businesses. See specific requirements for SLAs in clause 8.3.

- **Service access:** A cloud infrastructure is expected to provide cloud service users with access to cloud services from any user device. It is expected that cloud service users have a consistent experience when accessing cloud services.
- **Flexibility:** It is expected that the cloud architecture be capable of supporting multiple cloud deployment models and cloud service categories.
- **Accounting and charging:** It is expected that a cloud infrastructure be capable to support various accounting and charging models and policies.

- **Massive data processing:** It is expected that a cloud infrastructure supports mechanisms for massive data processing (e.g. extracting, transforming and loading data), for example to enable support of business intelligence capabilities.

NOTE - Distributed parallel processing systems will be used in cloud infrastructure deployments to provide large-scale integrated data storage and processing capabilities that scale with off-the-shelf hardware and provide software-based fault tolerance.

8.3 Requirements for cloud services

8.3.1 Requirements for cloud service categories

It is expected that requirements for services of the IaaS category include:

- computing hardware requirements (including processing, memory, disk, network interfaces, virtual machines, etc.);
- computing software requirements (including OS and other pre-installed software)
- storage requirements (including storage capacity);
- network requirements (including QoS specifications, such as bandwidth and traffic volumes);
- availability requirements (including protection/ backup plan for computing, storage and network resources).

It is expected that service requirements for services of the NaaS category include:

- network requirements (including QoS specifications such as bandwidth and traffic volumes);
- availability requirements (including protection/ backup plan for network resources).

It is expected that service requirements for services of the PaaS category include:

- requirements similar to those of the IaaS category;
- deployment options of user-created applications (e.g. scale-out options).

It is expected that service requirements for services of the SaaS and CaaS categories include:

- application specific requirements (including licensing options);
- network requirements (including QoS specifications such as bandwidth and traffic volumes).

8.3.2 Requirements for specific cloud services

8.3.2.1 DaaS

Some of the general requirements in clause 8.1 are particularly important for DaaS, including service reliability and quality assurance, environmental sustainability, accessibility and security.

DaaS specific requirements include (but are not limited to):

- **Comparable experience:** DaaS users require a comparable experience, including the running speed of application programs and the capability to select and run various applications, to when application programs run in their local PCs.
- **Fast boot-up time:** DaaS users, especially paying users, are eager for fast boot-up time of their virtualized desktops.
- **Support for high-definition applications:** High definition applications (e.g. high-definition 3D videos or games) are becoming one of the major user demands in the PC software market. Some DaaS users may also need to execute high-definition applications on virtualized desktops.

- **Configurability of the virtual environment:** DaaS users require the capability to configure the virtualized desktops' virtual environment, such as CPU, memory, storage, network etc.
- **Storage for data backup:** DaaS users may require DaaS to provide storage service (e.g. for backups or seldom-used data) in order to supplement the local storage resources.

8.3.2.2 SDPaaS

- SDPaaS is required to provide support for service delivery platform (SDP) capabilities based on cloud architecture;
- SDPaaS is required to provide support for SDP applications as SaaS;
- SDPaaS is required to provide support for services (like those provided by a traditional SDP) as SaaS/CaaS;
- SDPaaS is required to support SDP deployment as PaaS;
- SDPaaS is required to support SDP control and management functions as PaaS.

8.4 SLA support

This clause provides features for SLA in a cloud infrastructure from both cloud service user's perspective and cloud service provider's perspective.

8.4.1 A cloud service user's perspective

There are a number of features that cloud service users should consider for SLA in a cloud infrastructure.

Table 3 – Cloud service user's SLA requirements

Component	Description
Responsibilities	Cloud service users should be responsible for limits on system usage and restrictions on the type of data that can be stored. NOTE – implications and validity if this requirement is for further study.

Business continuity and disaster recovery	Cloud service users should ensure their cloud service providers have adequate protection in case of a disaster. NOTE – implications and validity if this requirement is for further study.
System redundancy	Cloud service users moving data and applications that must be constantly available should consider the redundancy of their cloud service provider's systems.
Location of Data	Cloud service users should ensure that their cloud service providers comply with the regulations on data location associated with the cloud service user's governing jurisdiction.
Security	Cloud service users should understand their security requirements and what controls and federation patterns are necessary to meet those requirements.
Transparency	Cloud service users bear the burden of proving that the cloud service provider failed to live up to the terms of the SLA under the SLAs of some cloud service providers. NOTE – implications and validity if this requirement is for further study.
Certification	Cloud service users might have the certification requirement that their cloud service provider be ISO 27001 certified.

8.4.2 A cloud service provider's perspective

There are a number of features that cloud service users should consider for SLA in a cloud infrastructure.

Table 4 – Cloud service user's SLA requirements

Component	Description
Security	Cloud service provider must understand what they must deliver to the cloud service users to enable the appropriate controls and federation patterns.
Data encryption	The details of the encryption algorithms and access control policies should be specified in the SLA.
Privacy	Regulations applicable in the cloud service user's governing jurisdiction shall be respected.
Data retention and deletion	Regulations applicable in the cloud service user's governing jurisdiction shall be respected.
Hardware erasure and destruction	Cloud service providers should offer the added protection of zeroing out memory space after a consumer powers off a VM.
Regulatory compliance	Cloud service providers must be able to prove their compliance if regulations must be enforced.
Transparency	Cloud service providers must be proactive in notifying consumers when the terms of the SLA are breached for critical data and applications.
Certification	Cloud service provider is responsible for proving their certification and keeping it up-to-date.

SLA monitoring	The cloud service provider should be able to monitor the quantitative parameters of the applicable SLA, when it is feasible and relevant. Note: In practice, an SLA may contain non-quantitative parameters, such as specific regulations, citizenship requirements, and business process standards (e.g. ISO 20000). Cloud services may have different types of SLAs.
----------------	---

8.4.3 Common features

There are a number of common features that should be considered for SLA in a cloud infrastructure.

Table 5 – Common SLA requirements

Component	Description
Auditability	An SLA should make it clear how and when those audits take place.
Metrics	Monitoring and auditing require something tangible that can be monitored as it happens and audited after the fact. The metrics of an SLA must be objectively defined and preferably broadly used.
Human interaction	Although on-demand self-service is one of the basic characteristics of cloud computing, the fact remains that there will always be problems that can only be resolved with human interaction. These situations must be rare, but many SLAs will include guarantees about the cloud service provider's responsiveness to requests for support.
Inter-cloud service brokers and resellers	Inter-cloud service brokers and resellers must be able to prove their compliance if regulations must be enforced.

8.4.4 Classification of SLA metrics

SLA metrics can be classified in a number of categories. These include availability, performance and security.

Table 6 – SLA metrics classification

Classification	SLA metrics
Availability	Service availability; time of data recovery point; service suspension time; business continuity; disaster recovery
Reliability	Transparency
Performance	Online response time; online response time compliance ratio; batch processing time; batch processing time compliance ratio; maximum number of processing tasks per unit time; compliance ratio of maximum processing tasks per unit time
Scalability	System redundancy
Security	Status of the cloud service provider's acquisition of the relevant security standard; status of certification of the party possessing management authority; status of operational restrictions included in security measures taken on the management system; assuring

	confidentiality of data transmitted between cloud systems; data location; status of acquisition of a log for detection of malicious acts; period during which a log is kept for detection of malicious acts; status of communication control to block malicious communication; status of measures against network congestion to circumvent denial of service (DoS)/distributed denial of service (DDoS) attacks; implementation of measures against malware; certification.
Data Management	Data encryption; privacy; data retention and deletion; hardware erasure and destruction
Serviceability	Policy of maintenance; human interaction

An example of SLA metrics is shown in Appendix III.

8.4 Management

- Security management: It is expected that a cloud infrastructure supports integrated management of the IT security and network security.
- Performance management: It is expected that a cloud infrastructure supports integrated management of performance from an end-to-end perspective (including management of both IT and network performances).
- Accounting management: It is expected that a cloud infrastructure supports integrated accounting management of both network and IT sides.
- Customer self-monitoring and supervision (according to the SLAs): It is expected that a cloud infrastructure provides capabilities to cloud service users for service-level self-monitoring and automatic supervision of the resources allocated to them if allowed, included and according to the SLAs.
- Unified management: It is expected that cloud infrastructure deployments support unified management platforms on which the various OSSs can be built on. This allows rapid deployment of new OSSs as well as unified management and scheduling. In order to support unified management platforms, unified data management is expected to be supported.
- Resource management:
 - It is expected that a cloud infrastructure supports capabilities for resource planning, discovery, reservation, allocation, release and monitoring;
 - Unified resource management: It is expected that a cloud infrastructure supports unified management and on-demand distribution of heterogeneous computing, storage and network resources based on virtualization.

8.5 Inter-cloud support

This clause describes the requirements derived from the Inter-cloud use cases in Annex A.

8.5.1 Matching between QoS requirements and SLA, and policy negotiation

This capability deals with the matching between QoS requirements (requested by cloud service users), and SLAs (proposed by the cloud service providers), to enable the multiple interworked cloud service providers to satisfy the user's QoS requirements. This capability deals also with negotiation of the service provisioning policies associated with different cloud service providers.

The QoS requirements of a given cloud service are expected to be met by appropriate interworking with selected cloud service providers, even in the event of service performance degradation or of a disaster.

The general requirements for this capability are:

- In order for the inter-cloud service brokering capability to compare cloud service user's QoS requirements with the SLAs offered by other cloud service providers' infrastructures, the QoS and performance aspects of the SLAs of cloud infrastructures shall be presented (publication or distribution) using standard formats.

- It should be possible to compare, negotiate, and settle down service provisioning policies between multiple cloud service providers (for example, based on the settlement, these cloud service providers may be considered as a trusted group for inter-cloud support).

NOTE - In this clause, policy refers to a way for a CSP to provide services in terms of presumed reliability, including its backup scheme and target service levels. The policy impacts on SLAs. Policies may be different among CSPs. Policies may be negotiated beforehand and settled down. This process refers to policy negotiation.

8.5.2 Resource management

This capability deals with the management of resource configurations in a secure way for each service across multiple cloud infrastructures.

The general requirements for this capability are:

- It should be possible to describe resource information (e.g. resource type, resource status, etc.) in a standard manner, in order to be able to manage resources across multiple cloud infrastructures.

- It should be possible to update cloud infrastructure's configuration information across multiple cloud infrastructures in synchronization with events (e.g., reserve or release of resources) involving multiple cloud infrastructures.

8.5.3 Resource and service status monitoring

This capability deals with the collection and monitoring of the various status attributes of cloud infrastructure's resources (e.g. usage, performance, service quality etc.) residing in the interworked CSPs.

By monitoring status information about resource availability (e.g., dead/alive status of machines) or service level performance degradation (e.g., delay or response time degradation), a CSP can initiate actions to maintain the service availability with the help of other CSPs (see inter-cloud use cases in Annex A).

The general requirements for this capability are:

- It should be possible to, periodically or on a request basis, collect information about the usage and performance status of the resources of the different CSPs' cloud infrastructures.
- It should be possible to, periodically or on a request basis, collect information about the availability (e.g. dead/alive status of machines) of the different CSPs' cloud infrastructures.

- It should be possible to exchange monitoring information, in commonly-defined ways, across different CSPs' cloud infrastructures. In case of mutual monitoring among interworked CSPs, it should be possible to maintain the appropriate level of security.

8.5.4 Resource performance estimation and selection

This capability deals with the resource selection from those which are candidate and have been already reserved in other CSPs' cloud infrastructures. This capability estimates the achievable performance by available reserved resources and assists the selection of the resources to be effectively used from all the reserved resources.

The general requirements for resource planning are:

- It should be possible to estimate the achievable performance of available reserved resources (e.g. computing resources, storage resources, input/output capacity between storages, network bandwidth) in other CSPs' cloud infrastructures.

8.5.5 Resource discovery and reservation

This capability deals with search, discovery, and reservation of the available resources in other CSPs' cloud infrastructures. This capability deals also with reservation acknowledgement for the candidate resources which have been tentatively reserved in other CSPs' cloud infrastructures.

The general requirements for resource discovery and reservation are:

- It should be possible to search resources available in other CSPs' cloud infrastructures.
- It should be possible to reserve the discovered resources in other CSPs' cloud infrastructures.
- It should be possible to provisionally reserve the discovered resources, i.e. to keep the resources to be used (as candidates), for later acknowledgement (for some of them) or release (for others).
- It should be possible to search for resources based on different priorities (e.g., in a different order of searching).

NOTE - Quality requirements may vary from service to service and each resource contribution to the service quality may vary as well. For example, if latency is critical, it should be possible to firstly reserve servers that are near to the user, and then network resources. In contrast, if bandwidth is critical, it should be possible to firstly reserve networks that can provide sufficient bandwidth, and then search for available servers that are connected to those networks.

- It should be possible to reserve available resources based on different priorities (e.g. early recovery, required quality guarantee, service type etc.).

NOTE - For example, a huge quantity of resources are required for recovery from a large-scale disaster. However, all required resources may not necessarily be available. Then, it should be possible, to forcefully reserve resources for lifeline services rather than for other services.

8.5.6 Resource setup and service activation

This capability deals with the setup of the reserved resources in the remote interworked CSPs and the activation of the middleware and applications for service provision over the remote CSPs. This includes connecting cloud infrastructures via networks, remotely activating (i.e. invoking) application or middleware, and transferring or copying data to enable the use of resources in other CSPs' cloud infrastructures.

The requirements for setup of reserved resources are:

- It should be possible to remotely set up reserved resources in the remote cloud infrastructure, and to access their configuration and policy settings from the requesting cloud infrastructure.

8.5.7 Switch-over and switch-back of the cloud service user access

This capability deals with the switch-over of the cloud service user access from the original cloud infrastructure to other cloud infrastructures to which the services may be delegated in order to cope with a disaster or degradation in service performance. It also deals with the switch-back to the original cloud infrastructure when it becomes able to provide the services again.

The general requirements for switch-over and switch-back of the cloud service user access are:

- It should be possible to switch over the cloud service user access to the substitute cloud infrastructure without any cloud service user's operations, in order to allow cloud service users to use services similarly to the pre-disaster situation.
- It should be possible to switch over the cloud service user access without any cloud service user's operations if load distribution between interworking cloud infrastructures is no longer needed.
- It should be possible to switch back the cloud service user access to that of the original cloud infrastructure, when the affected original cloud infrastructure has recovered from a disaster or when load distribution between interworking cloud infrastructures is no longer needed.

8.5.8 Releasing resources

This capability deals with release of resources reserved and used from other cloud infrastructures by judging that cloud interworking is no longer needed based on monitoring results, e.g. that disaster recovery has been completed or load distribution has been adopted.

The general requirements for release of reserved resources are:

- It should be possible to release other resources that were activated when the reserved resources began to be used, to update the remote cloud infrastructure's configuration information, and to erase and/or transfer back the previously received data.

8.5.9 Inter-cloud service brokering

The inter-cloud service brokering capability (for support of inter-cloud as inter-cloud service broker, as described in clause 5) is required to provide the following key features:

- Service intermediation: enhancing a given service, by improving some specific capability and providing value-added services.
- Service aggregation: combining and integrating multiple services into one or more new services, with integration and secure movement of data.
- Service arbitrage: similarly to service aggregation, except that the services being aggregated are not fixed.

Annex A Use cases

A.1 From the perspective of cloud service users and cloud service providers

A.1.1 Desktop as a service

A.1.1.1 Introduction

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.

Figure 6 shows the concept of DaaS.

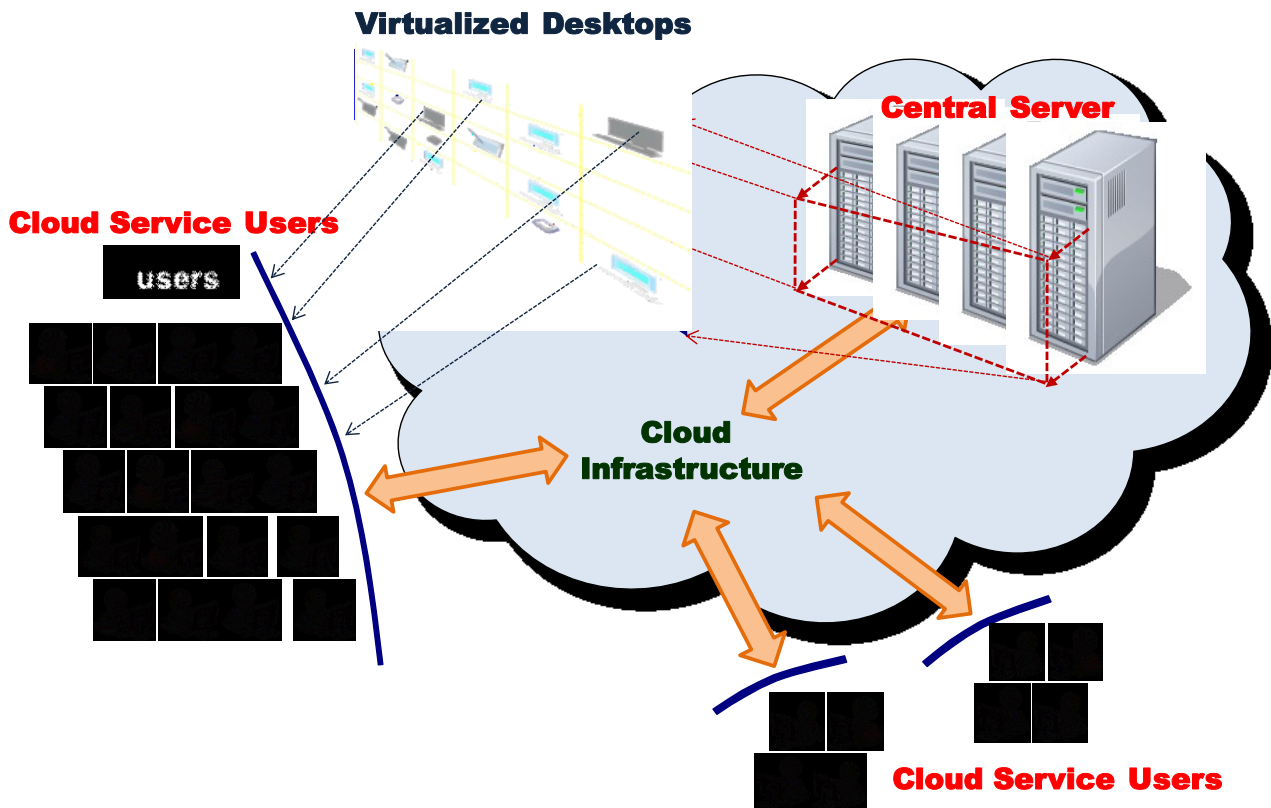


Figure 6 - The concept of DaaS

Instead of maintaining and running a 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 the desktop operating system and applications through a completely hosted system.

Further details on DaaS-related characteristics and technical solutions are provided in Appendix I.

A.1.1.2 General use case of DaaS

Table 7 – Desktop as a service use case

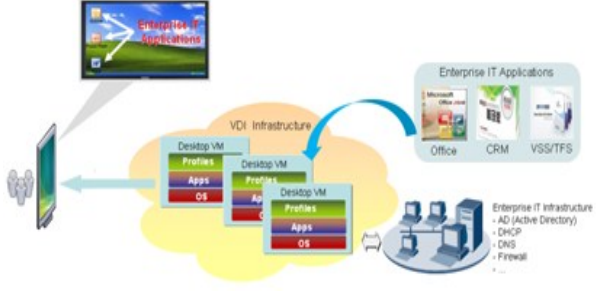
	Legend	Use case
Row 1	Use case title	Desktop as a service
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider), cloud service user (consumer, enterprise)
Row 3	Relevant cloud services categories	IaaS
Row 4	Relevant cloud deployment models	Private cloud, public cloud
Row 5	Use case description	<p>- Between a consumer and a CSP: In this scenario, a consumer accesses and uses data or applications in a CSP 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 to keep up with a password, since all data are totally stored and managed in the CSP.</p> <p>- Between an enterprise and a CSP: An enterprise using a virtual desktop service from a CSP 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 CSP, the enterprise normally uses storage for backups. Also, the enterprise can overcome peak loads and save energy by requesting the CSP online to increase or decrease the number of virtual desktops, respectively.</p> <p>- Among an enterprise, a consumer, and a CSP: In this scenario, 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 CSP. Contrary to the above two scenarios, the consumer cannot select applications freely and more limitations to access data in the enterprise may exist than within the enterprise. Whenever the consumer connects with the CSP, the CSP sends feedback data to the consumer by accessing the enterprise to handle or bypass corresponding data.</p>
Row 6	Information flow	<p>- Between a consumer and a CSP: The consumer should send information about authentication (i.e. password). The CSP offers virtual desktop environment of corresponding data such as OS, applications, and</p>

		<p>user data by virtual desktop delivery protocol (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.</p> <ul style="list-style-type: none"> - Between an enterprise and a CSP: This case is similar to that between a consumer and a CSP, except with regard to controlling the number of virtual desktops. The enterprise can send warning information when an abnormal situation (i.e. peak load) occurs. - Among an enterprise, a consumer, and a CSP: Information for authentication flows from the consumer to the enterprise through the CSP. Once the consumer is identified, information regarding internal processes is transferred to the CSP and is dispatched to the end user by VDDP. The consumer's output data is stored to the CSP 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.
Row 7	High-level figure describing the use case	<p>The diagram illustrates a cloud ecosystem. At the top, a cloud labeled 'Cloud Service Provider' contains server racks. Below it, 'Virtualized Desktops' are shown on both sides, connected to a central 'Cloud Infrastructure' cloud. At the bottom, a 'Consumer' and an 'Enterprise' are represented by icons, with arrows pointing from them to the 'Cloud Infrastructure'.</p>
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> - Consumers require accessing their desktop environments independently of locations, with their various devices. - Desktop environment needs to guarantee the business continuity and a recovery solution for a system failure. - Consumers desire to use their personal tasks, separating business computing. - Consumers eager to run various applications as in traditional PCs.
Row 9	Other information specific to the use case	

A.1.1.3 Specific use case of DaaS - Office automation of development-oriented enterprise

Table 8 – Office automation of development-oriented enterprise use case

	Legend	Use case
Row 1	Use case title	Office automation of development-oriented enterprise

Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider), cloud service user (consumer, enterprise)
Row 3	Relevant cloud services categories	IaaS
Row 4	Relevant cloud deployment models	Private cloud, public cloud
Row 5	Use case description	<p>In this scenario, the end users access the enterprise applications and data hosted in virtual desktops which are created within a DaaS server. Common applications of this type include online word processing, email, communication, co-operating development, and so on. The sales staff also can view customer information and marketing records on the enterprise website. The DaaS server interacts with traditional enterprise IT facilities to achieve many control tasks, for instance, using DHCP to assign an IP address for thin client, leveraging internal DNS server to resolve local host names, and consulting AD to authenticate user desktop sessions.</p>
Row 6	Information flow	
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> - Authorization: Currently, the most virtual desktop solutions care for enterprise's internal usage only, and use local security facilities to authenticate user desktop session. This indeed cannot satisfy the needs for small and medium enterprises (SME) because they cannot afford the capital investment of virtual desktop implementation. Being aware of this huge market opportunity, telecom operators are driving into public cloud based virtual desktop implementation aimed at providing desktop VM services for SME based on their own existing IT Infrastructure, e.g. RADIUS. So current virtual desktop solutions must be changed to accommodate new security requirements. - Coherency: Since a variety of VM infrastructure implementations exist today, there is an increasingly urgent demand that a high-level abstract layer should provide unified access methods without concerning the technical details of the underlying infrastructure. Unfortunately, almost all virtual desktop implementation is bundled with a specific VM infrastructure. Coherency

		<p>is needed in order to increase the expandability and scalability of DaaS system.</p> <p>- Equipment specification: Thin client as the new coming user-side equipment needs to be standardized, including electric characteristics, physical port, video decode, desktop protocols and others, in order to carry more powerful applications and further enhance end-user experience just like the rich client did.</p>
Row 9	Other information specific to the use case	

A.1.1.4 Specific use case of DaaS - Customer service call centre

In a traditional telecommunication operator call centre (customer support), various issues exist from different perspectives: a growing complexity of the application environment, the need of frequent updates for the computer configurations, the presence of a large number of PCs with high energy consumption, a multi-level IT environment with high maintenance costs, no uniform PC/terminal configurations, and multiple PC/terminal management platforms.

This case describes a cloud-based telecommunication call centre, which provides a solution for the main issues of a traditional call centre. This cloud-based customer service call centre can also be seen as a specific use case of DaaS.

The replacement of PCs/terminals by the combination of one (or multiple) cloud server(s) and DaaS terminals can reduce both hardware and software cost. In particular, DaaS terminals consume less power and run without fan cooling; software is only installed and configured on the cloud server as a SaaS application; upgrades and maintenance are performed only on the cloud server; DaaS terminal do not need to be protected (no data being stored in the DaaS terminals, they are not a target of security attacks).

Table 9 – Customer service call centre use case

	Legend	Use case
Row 1	Use case title	Customer service call centre
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider), cloud service user (consumer, enterprise)
Row 3	Relevant cloud services categories	IaaS
Row 4	Relevant cloud deployment models	Private cloud, public cloud
Row 5	Use case description	<p>Virtual desktop pool supports distributed deployment model and can be deployed in the cloud computing IaaS resource pool with the dynamic stretching of resources.</p> <p>By adopting cloud computing technology (virtualization, distributed computing and storage, cluster, etc.) to consolidate queuing resource and</p>

		desktop resources, unified phone call dispatching and delivery and maintenance of the desktop can be achieved in an intensive way.
Row 6	Information flow	
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> - Management convenience: New methods, such as virtual desktops, are required to achieve desktop and application delivered centrally as needed. And centrally maintenance of a virtual desktop for the service representatives could be achieved so as to achieve dynamically deploying, scaling and upgrading the virtual desktops. - Security assurance: It must be guaranteed that the virtual desktops and the data in the call centre prevented from stolen and loosen, also the system in the data centre prevented from attacking by computer virus or hackers. - Cost saving: It is desired that the total cost of ownership could be reduced. So the capital expenditure (CAPEX) or operating expenditure OPEX should be reduced. Since virtual desktop mainly using thin client device so the power consumption could be brought down than PCs, and manpower for operational maintenance could also be brought at the same time. - Terminal diversity: multiple kinds of terminal devices are desired to be used, e.g. PC, thin client, pad computer, even intelligent mobile phones could be used.
Row 9	Other information specific to the use case	

A.1.2 Service delivery platform as a service (SDPaaS)

A.1.2.1 Introduction

The term “service delivery platform” (SDP) [b-Moriana-SDP2.0] usually refers to an environment-enabling efficient creation, deployment, execution, orchestration and management of one or more classes of services. SDPs apply to both consumer and business applications.

As SDPs evolve, they often require integration of telecom and IT capabilities and the creation of services beyond technology and network boundaries. SDPs available today are optimized for the delivery of a service in a given technological or network domain (examples of such SDPs include IMS, IPTV, M2M/IoT, etc.) and application developers cannot fully collaborate and share services.

SDPs typically provide a service-creation environment, a service orchestration and execution environment, a service-delivery control environment, and abstraction functions for network service capabilities.

Through the abstraction of network service capabilities and the introduction of new service capabilities, SDPaaS (Service Delivery Platform as a Service) can provide service integration and convergence of capabilities offered by different network domains. Via the exposure of SDPaaS APIs by cloud service providers, cloud service users can access anytime and anywhere cloud converged services supported by easily manageable and chargeable capabilities.

By expanding the service delivery process of the traditional SDPs, SDPaaS not only supports service capability operations, but also provides platform capabilities for full collaboration and service sharing among application developers, significantly accelerating the development cycle of end-to-end applications.

Also, SDPaaS allows traditional service providers deploying SDP platforms to be cloud service providers offering SDPaaS.

A.1.2.2 SDPaaS use case

Table 10 – SDPaaS use case

	Legend	Use case
Row 1	Use case title	Service delivery platform as a service (SDPaaS)
Row 2	Relevant actors (played roles)	Cloud service users (consumer, enterprise, governmental/public institution), cloud service providers (SaaS, CaaS, PaaS, IaaS, NaaS provider and inter-cloud), cloud service partners (application developer, content provider)
Row 3	Relevant cloud services categories	PaaS, SaaS/CaaS
Row 4	Relevant cloud deployment models	Public cloud, private cloud, community cloud, hybrid cloud
Row 5	Use case description	<p>The traditional SDPs are not able to support multi-domain service convergence, or an environment where application developers can fully collaborate and share services.</p> <p>In the new world of converged service delivery, SDP should also be considered not just as a core function within a telecommunication service provider infrastructure, but as a number of interconnected, distributed service nodes which may support various requirements, including redundancy, support of different service profiles for different business and market sectors, full support for application developers [b-Y.2240].</p> <p>Through the exposure of “SDP as a service” (SDPaaS) by a cloud service provider via open SDPaaS APIs, cloud service users can easily access new converged ICT services (e.g. IMS applications, IPTV applications, M2M/IoT applications) through multiple kinds of</p>

		<p>terminal devices e.g. PC, thin client, pad computer, mobile phone, smart phone, virtual desktop client.</p> <p>Also, through the SDPaaS capabilities, application developers can fully collaborate and share services developing new converged ICT services.</p>
Row 6	Information flow	
Row 7	High-level figure describing the use case	<p>The diagram illustrates the SDPaaS architecture for convergent services. It features a central 'SDPaaS platform for convergent services' layer. Below this platform are three 'App Engines': 'Telecom App Engines', 'Internet/Web App Engines', and 'Other App Engines'. These engines are connected to their respective domains: 'Telecom', 'Internet', and 'Other Domain'. Above the platform, three categories of services are shown: 'Telecom Services' (including MMS, News, UC, and IPTV), 'Internet/Mobile Internet' (including diary, blog, Address Book, mobile search, video surf, and map), and 'Other Applications' (including eHealth, Ear monitoring, City emergency, eTraffic, agriculture monitoring, and Smart Grid).</p>
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> - Cloud service providers are required to provide support for service delivery platform (SDP) capabilities based on cloud architecture. - It is required that cloud service users be enabled to use convergent ICT applications via SDPaaS (e.g. IMS applications, IPTV applications, M2M/IoT applications). - SDPaaS is required to provide support for services (like those provided by a traditional SDP) as SaaS/CaaS. - It is required to provide support for SDP capabilities as PaaS via SDPaaS. For example, it is required that application developers be enabled to develop convergent IT/telecom applications through SDPaaS capabilities. - It is required to provide support for SDP deployment as PaaS via SDPaaS. - SDPaaS is required to support SDP control and management functions as PaaS.
Row 9	Other information specific to the use case	

A.1.3 Mobile cloud

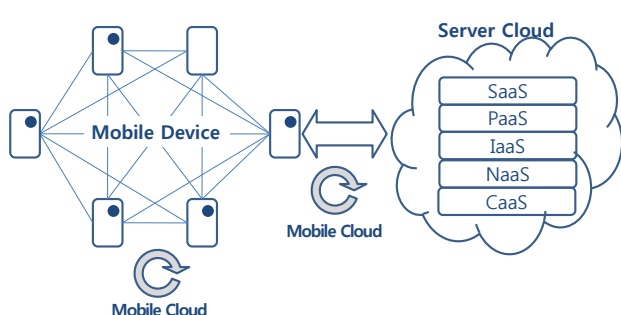
Mobile cloud is a model in which mobile applications are built, powered and hosted using cloud computing technology. The data storage and the data processing happen outside of the mobile device with minimal processing power from which an application is launched, and the resources in terms of computing, platform support required to execute these applications are available through the cloud.

Another important capability of mobile cloud services is the possibility to reuse devices capabilities such as camera, GPS, memory, etc. If CSU configures the mobile cloud among granted mobile devices, the device capabilities are accessible via mobile cloud to use respective device capabilities.

Further details on mobile cloud are provided in Appendix VI.

A.1.3.1 Mobile cloud use case

Table 11 – Mobile cloud use case

	Legend	Use case
Row 1	Use case title	Mobile cloud
Row 2	Relevant actors (played roles)	Cloud service provider (SaaS, CaaS, PaaS, IaaS, NaaS provider inter-cloud), cloud service user (consumer, enterprise, governmental institution), cloud service partner (application developer, content provider, software provider, hardware provider, network equipment provider, auditor)
Row 3	Relevant cloud services categories	IaaS, PaaS, SaaS, NaaS, CaaS
Row 4	Relevant cloud deployment models	Public cloud, private cloud, hybrid cloud and community cloud
Row 5	Use case description	<ul style="list-style-type: none"> - A cloud service can be developed by cloud providers - A mobile cloud application can be developed by service partners or cloud provider or third-party service provider - The mobile cloud application for cloud service can be downloaded and users can interact between cloud services. Also, users can directly access cloud service using Web browser - The mobile cloud application sends processing tasks to the cloud and stores data in the cloud, and receives results generated by the resources from the cloud, including computing resources and storage sources.
Row 6	Information flow	
Row 7	High-level figure describing the use case	 <p>The diagram illustrates the Mobile Cloud architecture. On the left, a group of five mobile devices is interconnected with a central 'Mobile Device' icon. Below this group is a circular arrow icon labeled 'Mobile Cloud'. A double-headed arrow connects this 'Mobile Cloud' to a larger cloud icon on the right labeled 'Server Cloud'. Inside the 'Server Cloud' are five stacked boxes representing service categories: SaaS, PaaS, IaaS, NaaS, and CaaS.</p>
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> - Web capabilities such as HTML5, Device API, etc. on device - Interaction mechanism among devices - Mobile-specific rendering and transcoding - Capability to mobile device support such as SDK for Mobile

		<ul style="list-style-type: none"> - Secure access mechanism for device resources - Application packaging and delivery way
Row 90	Other information specific to the use case	

A.1.4 Cloud migration and portability

A.1.4.1 Move three-tier application from on-premises to cloud

Table 12 – Move three-tier application from on-premises to cloud

Row 1	Use case title	UC1: Move three-tier application from on-premises to cloud
Row 2	Relevant actors (played roles)	Cloud service users, cloud service providers, cloud service partners
Row 3	Relevant cloud services categories	IaaS for machine execution;
Row 4	Relevant cloud deployment models	Private cloud, public cloud, community cloud, hybrid cloud
Row 5	Use case description	<p>An organization moves a three-tier application from an on-premises data centre to a cloud infrastructure provider that will run the application off-premises.</p> <p>A three-tier application consists of the front-end web server, back-end database, and middle-tier business logic that services data requests between the user and the database</p> <p>Platform services for data, identity and access are considered available for source and target clouds but not addressed in this case.</p> <p>This use case represents the most common type of web-based application deployed both in enterprises and mid-sized companies.</p>
Row 6	Information flow	<ol style="list-style-type: none"> 1. Requires agreement between the parties on cloud “appliance” packaging file format support: <ol style="list-style-type: none"> a. Package multiple VMs, one per application tier, in one or more “appliance” files. b. Each VM image contains the respective initialization data, application user account data for ID/access, database if applicable. 2. May require upload/import of bulk user data to the cloud over the network or by sending a disk with agreed-to data packaging. 3. May require access to separate identity/authentication/authorization system if using federation. <ol style="list-style-type: none"> a. To protect the privacy of cloud users, cloud identity providers should not be able to track and trace user identity and access patterns. The user should not have to provide more information than the minimum necessary to be granted access. 4. Requires cloud-based VM management/control for lifetime management of each application tier running as one or more VMs. 5. Virtual LAN/networking support for managing application’s IP address space.
Row 7	High-level figure describing the use case	

Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> • VM portability: Create portable appliances from existing on-premises apps and move them to the cloud • Bulk import/export of customer data • VM management protocol
Row 9	Other information specific to the use case	This use case represents the most common type of web-based application deployed both in enterprises and mid-sized companies.

A.1.4.2 Move three-tier cloud application to another cloud

Table 13 – Move three-tier cloud application to another cloud

Row 1	Use case title	UC2: Move three-tier cloud application to another cloud
Row 2	Relevant actors (played roles)	Cloud service users, cloud service providers, cloud service partners
Row 3	Relevant cloud services categories	IaaS for machine execution;
Row 4	Relevant cloud deployment models	Private cloud, public cloud, community cloud, hybrid cloud
Row 5	Use case description	<p>An organization moves a three-tier application from one cloud infrastructure provider to another.</p> <p>Actors involved in this use case include: cloud service providers, software developers, system administrators/operators</p>
Row 6	Information flow	<ol style="list-style-type: none"> 1. Requires VM portability: Create portable appliances from existing VMs in source cloud, and then move to 2nd cloud. 2. Connections to inside-firewall systems (e.g., VPNs) or outside systems (e.g., identity federation servers) need to be easily reconfigurable/ reusable. 3. Requires bulk import/export of customer data. 4. Requires VM management. 5. Customer may require “erase” delete of the application on the old cloud. 6. Regardless of the choice of programming language, runtime and tools used to develop the original on-premises application, the cloud service should be available on-premises as a private cloud or offered by a third party as a hosted cloud if the customer chooses not to deploy to the public cloud.
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> • VM portability: Create portable appliances from existing on-premises apps and move them to the cloud • Bulk import/export of customer data • VM management protocol • May require “erase” delete of the application in the old cloud
Row 9	Other information specific to the use case	

A.1.4.3 Move part of on-premises application to cloud to create “hybrid” application

Table 14 – Move part of on-premises application to cloud to create “hybrid” application

Row 1	Use case title	UC3: Move part of on-premises application to cloud to create “hybrid” application
-------	----------------	--

Row 2	Relevant actors (played roles)	Cloud service users, cloud service providers, cloud service partners
Row 3	Relevant cloud services categories	IaaS for machine execution;
Row 4	Relevant cloud deployment models	Private cloud, public cloud, community cloud, hybrid cloud
Row 5	Use case description	An organization moves one or more parts – or tiers – of an on-premises application to the cloud, in order to separate data storage from processing, for example. This creates a cloud that is a hybrid of both public (off-premises) and private (on-premises) clouds. Actors involved in this use case include: cloud service providers, software developers, system administrators/operators.
Row 6	Information flow	<ol style="list-style-type: none"> 1. Requires VM management, appliance packaging, bulk import/export, as in the above scenarios. 2. Also requires runtime web interfaces for the on-premises and cloud components to interact/exchange/sync data with interoperability primitives such as file/object sync/invocation. 3. Will likely require cloud storage for caching intermediate results (simple cloud storage APIs/semantics). 4. Regardless of choice of programming language, runtime and tools used to develop the original on-premises application, the cloud service should be offered by a third party as a hosted cloud if the customer chooses not to deploy to the provider’s public cloud.
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> • VM portability: Create portable appliances from existing on-premises apps and move them to the cloud • Bulk import/export of customer data • VM management protocol
Row 9	Other information specific to the use case	

A.4.1.4 Hybrid cloud application that uses platform services

Table 15 – Hybrid cloud application that uses platform services

Row 1	Use case title	UC4: Hybrid cloud application that uses platform services
Row 2	Relevant actors (played roles)	Cloud service users, cloud service providers, cloud service partners
Row 3	Relevant cloud services categories	PaaS services – e.g., structured/unstructured cloud storage and identity/access interfaces/APIs – are available from cloud vendor.
Row 4	Relevant cloud deployment models	Private cloud, public cloud, community cloud, hybrid cloud
Row 5	Use case description	An organization moves one or more parts – or tiers – of an on-premises application to the cloud and chooses to implement cloud components of a hybrid application using platform services available from the cloud platform provider, such as structured or unstructured cloud storage or identity and access control services.

Row 6	Information flow	<ol style="list-style-type: none"> 1. User accounts, databases, data stores and bulk data would have to be transferred from equivalent on-premises capabilities. 2. Requires porting code for use of new cloud services. Cost of porting on-premises application is lowered when application logic is written to semantic interfaces that stay valid when the application logic is ported to a new cloud. <ol style="list-style-type: none"> a. ID/Access: Runtime web interfaces to deal with federated user identity/access and security would cut porting costs. b. Data: Common semantics for data structures and interfaces/APIs. 3. If cloud A or B is IaaS-style, appliance packaging would benefit from identifying the various platforms, runtimes and languages required in widely understood semantics and taxonomies. 4. Developer choice for tools, languages, and runtimes/ frameworks will offer flexibility, promote competition in richness of capabilities, and reduce porting costs. <p>Regardless of choice of programming language, runtime, and tools used to develop the application, the cloud service should be available on-premises as a private cloud or offered by a third party as a hosted cloud if the customer chooses not to deploy the cloud components to the public cloud.</p>
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> • Bulk import/export of customer data • Semantic cloud application management protocol
Row 9	Other information specific to the use case	

A.1.4.5 Port cloud application that uses platform services to another cloud

Table 16 – Port cloud application that uses platform services to another cloud

Row 1	Use case title	UC5: Port cloud application that uses platform services to another cloud
Row 2	Relevant actors (played roles)	Cloud service users, cloud service providers, cloud service partners
Row 3	Relevant cloud services categories	PaaS services – e.g., structured/unstructured cloud storage and identity/access interfaces/APIs – are available from cloud vendor.
Row 4	Relevant cloud deployment models	Private cloud, public cloud, community cloud, hybrid cloud
Row 5	Use case description	Porting an application that uses services provided by the cloud platform to another cloud platform implies these requirements: 1) bulk import/export of customer data, and 2) Semantic cloud application management protocol.
Row 6	Information flow	<ol style="list-style-type: none"> 1. Developer choice for tools, languages, runtimes, storage, database and other infrastructure services should be supported at both IaaS (VM) level as well as PaaS (platform level) to ensure richness of cloud platform offerings and promote innovation.

		<p>2. Use of semantic APIs and protocols would allow for the application logic/algorithm to be similar, allowing similar underlying pseudo code. This will help cut porting costs.</p> <p>3. The application’s use of storage (structured or unstructured) could often be costly to port. However:</p> <ol style="list-style-type: none"> For non-structured storage (blobs, queues, tables, etc.) using simple, semantically similar cloud storage APIs would cut porting costs since algorithm/pseudo code would be similar. For structured storage, costs of porting code based on SQL data access interfaces are often similar regardless of runtime or language used. <p>4. Regardless of choices made in 1., the new cloud service should be available on-premises as a private cloud or offered by third-party as hosted cloud if customer opts not to deploy to public cloud.</p>
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> • Bulk import/export of customer data • VM management protocol • Semantic or syntactic cloud application management protocol • Non-structured storage (blobs, queues, tables, etc.) – use of simple, semantically similar cloud storage APIs would cut porting costs since underlying algorithm/pseudo code would be similar.
Row 9	Other information specific to the use case	

A.1.5 User data inquiry and analysis based on massive data processing

Table 17 – User data inquiry and analysis based on massive data processing

	Legend	Use case
Row 1	Use case title	User data inquiry and analysis based on massive data processing
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider, NaaS provider, PaaS provider), cloud service user (consumer, enterprise)
Row 3	Relevant cloud services categories	IaaS, NaaS and PaaS
Row 4	Relevant cloud deployment models	Private cloud
Row 5	Use case description	Large-scale telecom operators generate a lot of information in the normal course of running their communication networks. Typical data comprises call data records (CDR) and Internet-surfing data records (IDR). For example, each call generates CDR, which includes information such as the caller’s phone number, the callee’s phone number, the start time of the call, the call’s duration, information about the call’s routing, etc. In addition to CDR and IDR, the network also generates various signalling data between switches and nodes. We need all the data to complete the telecom services

		and bill customers. At the same time, we also need them to analyze and predict user behaviour, optimize network QoS, filter spam messages, and so forth. Traditional user data inquiry and analysis systems require all data to be processed within a single server. Hardware capacity thus becomes a performance bottleneck and the current system takes too much time for many applications. Because of the limitations of the current system, the parallel data inquiry and mining tool set on the distributed parallel processing system could be a better solution and achieve massive scalability (using a distributed file system and distributed database for a scale-out architecture) and high-speed processing (based on parallel loading, ETL (extract, transform and load) and computing).
Row 6	Information flow	<ul style="list-style-type: none"> - Data source uploading: CSP collects the original CSU's IDRs and CDRs. - Data storing: Real time and batch ETL by CSP. - Distributed data processing: original CSU's records are processed in the distributed environment, including distributed database, distributed computing and distributed file system, by CSP. - Inquiry & analysis: CSU could acquire near real-time inquiry and analysis of their CDRs and IDRs.
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<p>The system is required to support:</p> <ul style="list-style-type: none"> - CSU's data collection (e.g. CDRs and IDRs) - CSU's data real-time and batch ETL - Distributed data processing environment including distributed database, distributed computing and distributed file system - Enough network bandwidth depending on data collection interval
Row 9	Other information specific to the use case	

A.2 From the inter-cloud perspective

This clause describes use cases in which multiple cloud systems interact with each other to satisfy the specified requirements, and how cloud systems work in each use case.

A.2.1 SLA mapping between CSP (inter-cloud service broker) and CSP

This use case deals with the SLA mapping between the CSP playing the inter-cloud service broker role (CSP-ISB) and other CSPs.

Multiple CSPs will contribute to, or impact concurrently, the SLA between the CSP-ISB and the CSU when an orchestrated service is provided.

Table 18 – SLA mapping between CSP-ISB and CSP




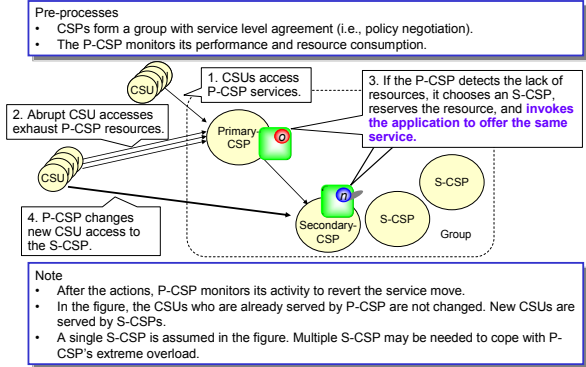
	Legend	Use case
Row 1	Use case title	SLA mapping between CSP (inter-cloud service broker) and CSP
Row 2	Relevant actors (played roles)	Cloud service user (consumer, enterprise, governmental institution), cloud service provider (IaaS provider, PaaS provider, SaaS provider, inter-cloud service broker)
Row 3	Relevant cloud services categories	IaaS, PaaS, SaaS
Row 4	Relevant cloud deployment models	Public cloud
Row 5	Use case description	<p>CSP-ISB is the contact point for CSU, and there is SLA (SLA0) between them.</p> <p>CSP-ISB integrates services from multiple CSPs, for instance, storage service from CSP-1 and computing service from CSP-2. There are B2B level SLA between CSP-ISB and CSP-1, CSP-2 respectively (SLA1, SLA2).</p> <p>For CSP-ISB, in order to guarantee SLA0 for CSU, it needs to map SLA0 to SLA1 and SLA2, because SLA0 is actually implemented by SLA1 and SLA2.</p>
Row 6	Information flow	
Row 7	High-level figure describing the use case	
Row 8	Derived requirements for the cloud ecosystem	<ul style="list-style-type: none"> - It should be possible for CSP-ISB and CSPs to negotiate SLAs. - It should be possible for CSP-ISB to coordinate the SLAs from multiple CSPs (which is related to a business decision).
Row 9	Other information specific to the use case	

A.2.2 Guaranteed performance

A.2.2.1 Guaranteeing performance against an abrupt increase of the load

Table 19 – Inter-cloud use case; guaranteeing performance against an abrupt increase of the load

	Legend	Use case
Row 1	Use case title	Inter-cloud use case; guaranteeing performance against an abrupt increase of the load
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider, NaaS provider, inter-cloud federation), cloud service user (consumer, enterprise, governmental institution)
Row 3	Relevant cloud services categories	IaaS, NaaS
Row 4	Relevant cloud deployment models	Hybrid cloud
Row 5	Use case description	<ul style="list-style-type: none"> - A CSP guarantees its service performance, even when an unexpected surge of access to the service arises, by using cloud resources provided by other CSPs on a temporary basis. - When the overload is detected at a CSP, available resources in other CSPs are autonomously discovered and reserved through the inter-cloud federation. - Network connections among interworking CSPs are instantaneously established or reconfigured. Then service-related data including user ID, user data, and application data are transferred from the original CSP to the CSP that is leasing the resources. - Access from CSUs is appropriately changed to the interworking CSPs so as to achieve load distribution, and thus mitigate the overload of the original CSP.
Row 6	Information flow	<ul style="list-style-type: none"> - Relevant CSPs are supposed to join a common trusted alliance in advance and set up the service level agreements (SLAs). - A CSP inquires about the resource availability of other CSPs in the alliance, and requests a reservation of available resources to meet the quality requirements of the CSU. The requested CSPs reply whether or not they are able to lease the resources. - The cloud resource management (such as create, read, update, and delete or CRUD) are operated across multiple CSPs. The management is to enable to lease cloud resources from different CSPs in the alliance. - The relevant CSPs exchange monitoring and auditing information of the leased resources.

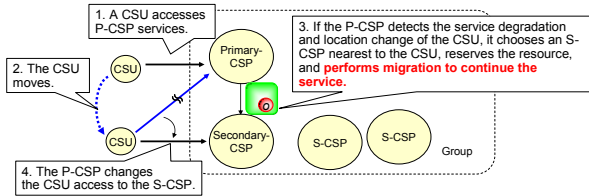
<p>Row 7</p>	<p>High-level figure describing the use case</p>	<p>Legends</p> <p>General CSU: Cloud Service User</p> <p>First four use cases P-CSP: Primary Cloud Service Provider S-CSP: Secondary Cloud Service Provider</p> <p>The last use case CSP: Cloud Service Provider CSP-ISB: Cloud Service Provider with an Inter-cloud service broker</p> <p>  Virtual resources (i.e., virtual machine, virtual storage, and virtual network)  Ongoing applications (e.g., snapshot image of the main memory)  Newly invoked applications [WITH SHADOW] </p> <p>Case 1. Guaranteeing performance against an abrupt increase of the load - CSP overload and load distribution</p> <p>Pre-processes</p> <ul style="list-style-type: none"> • CSPs form a group with service level agreement (i.e., policy negotiation). • The P-CSP monitors its performance and resource consumption.  <p>Note</p> <ul style="list-style-type: none"> • After the actions, P-CSP monitors its activity to revert the service move. • In the figure, the CSUs who are already served by P-CSP are not changed. New CSUs are served by S-CSPs. • A single S-CSP is assumed in the figure. Multiple S-CSP may be needed to cope with P-CSP's extreme overload.
<p>Row 8</p>	<p>Derived requirements for the cloud ecosystem</p> <p><i>Note: requirements should be written as much as possible in a clear way such that we can then move (re-use) all of them to the requirements clause (clause 9) and possibly identify common requirements derived for different use cases beyond those specific to each case.</i></p>	<p>The system is required to support:</p> <ul style="list-style-type: none"> - Policy negotiation including SLA management among the multiple CSPs within a pre-established group. <p>NOTE - Policy refers to a way for a CSP to provide services in terms of presumed reliability of a machine, including its backup scheme and target service levels. The policy may be different with each CSP. To keep the same quality of service to the CSU even when CSP changes, the difference should be negotiated beforehand and settled down. This process refers to policy negotiation. The same note applies to the other use cases.</p> <ul style="list-style-type: none"> - Self-performance monitoring at a CSP. If the performance degrades, the CSP should initiate the configured next actions. - Discovery, reservation, use, and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within a pre-established group. - Application invocation over the reserved resources on other CSPs within a pre-established group. - Alteration and reversion of CSU access from one CSP to another CSP in a dynamic manner (i.e., not relying on the pre-configuration) within a pre-established group. - Exchange of monitoring and auditing information among the multiple CSPs within a pre-established

		<p>group</p> <ul style="list-style-type: none"> - Exchange of authentication information about CSU (user / enterprise) authentication status among the multiple CSPs within a pre-established group
Row 9	Other information specific to the use case	

A.2.2.2 Use case of guaranteeing performance regarding delay

Table 20 – Inter-cloud use case; guaranteeing performance regarding delay

	Legend	Use case
Row 1	Use case title	Inter-cloud use case; guaranteeing performance regarding delay
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider, NaaS provider, inter-cloud federation), cloud service user (consumer, enterprise, governmental institution)
Row 3	Relevant cloud services categories	IaaS, NaaS
Row 4	Relevant cloud deployment models	Hybrid cloud
Row 5	Use case description	<ul style="list-style-type: none"> - CSPs guarantee their service performance (in particular, network delay and response time), even when CSUs move to a remote location (e.g., on a business trip), by using cloud resources provided by a CSP located close to CSU on a temporary basis. - When the degradation in response time is detected for a CSU at a CSP, available resources are autonomously discovered and reserved in another CSP, which is near the CSU, based on the user's location information. - Network connections among interworking CSPs are instantaneously established or reconfigured. Then service-related data including user ID, user data, and application data are transferred from the original CSP to the CSP that is leasing the resources. - Access from CSUs is appropriately changed to the interworking CSP so as to achieve route optimization, and thus mitigate the performance degradation caused by the original distant CSP. - The CSU, who keeps the same user ID, can continuously access the service at the same level of response time as before.
Row 6	Information flow	<ul style="list-style-type: none"> - Relevant CSPs are supposed to join a common trusted alliance in advance and set up the service level agreements (SLAs). - A CSP inquires about the resource availability of other CSPs in the alliance, and requests a reservation of available resources to meet the quality requirements of the CSU. The requested CSPs reply whether or not they are able to lease the resources.

		<ul style="list-style-type: none"> - The cloud resource management (such as create, read, update, and delete) are operated across multiple CSPs. The management is to enable to lease cloud resources from different CSPs in the alliance. - The relevant CSPs exchange monitoring and auditing information of the leased resources.
<p>Row 7</p>	<p>High-level figure describing the use case</p>	<p>Case 2. Guaranteeing performance regarding delay – Performance degradation and CSP optimization</p> <div data-bbox="858 488 1394 546" style="border: 1px solid black; padding: 2px;"> <p>Pre-processes</p> <ul style="list-style-type: none"> • CSPs form a group with service level agreement (i.e., policy negotiation). • P-CSP monitors CSU's quality of service. </div>  <div data-bbox="858 775 1394 860" style="border: 1px solid black; padding: 2px;"> <p>Note</p> <ul style="list-style-type: none"> • After the actions, S-CSP monitors the CSU's quality of service. • P-CSP may take care of the CSU even after CSU moves. • A single S-CSP is assumed as the recipient because the migration is triggered by one CSU to be served by another CSP. </div>
<p>Row 8</p>	<p>Derived requirements for the cloud ecosystem</p>	<p>The system is required to support:</p> <ul style="list-style-type: none"> - Policy negotiation including SLA management among the multiple CSPs within a pre-established group - CSU service level monitoring at CSP. If the service level degrades, the CSP should initiate the configured next actions. - Discovery, reservation, use, and release of cloud resources, based on CSU location, in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within a pre-established group. - Capability migration (e.g., VM and applications) over the reserved resources on other CSPs within a pre-established group. - Alteration and reversion of CSU access to one CSP to another CSP in a dynamic manner (i.e., not relying on the pre-configuration) within a pre-established group. - Exchange of monitoring and auditing information among the multiple CSPs within a pre-established group - Exchange of authentication information about CSU (user / enterprise) authentication status among the multiple CSPs within a pre-established group
<p>Row 9</p>	<p>Other information specific to the use case</p>	

A.2.3 Guaranteed availability

Table 21 – Inter-cloud use case; guaranteeing availability in the event of a disaster or a large-scale failure

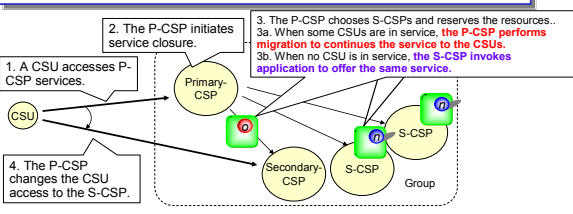
	Legend	Use case
Row 1	Use case title	Inter-cloud use case; guaranteeing availability in the event of a disaster or a large-scale failure
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider, NaaS provider, inter-cloud federation), cloud service user (enterprise, governmental institution)
Row 3	Relevant cloud services categories	IaaS, NaaS
Row 4	Relevant cloud deployment models	Hybrid cloud
Row 5	Use case description	<ul style="list-style-type: none"> - CSPs continue their service offering by the resources leased from each other, even when systems in one CSP are damaged due to natural disasters or large-scale failures. - Available resources in other CSPs are autonomously discovered and reserved through the inter-cloud federation. - The services with a high priority are only recovered if available resources are not enough to recover all services. In examining the availability of the resources given from other CSPs, the guaranteed level of quality of the resources is taken into account. - The services requiring early recovery are recovered using available resources on a best-effort basis even if their quality requirements are partly satisfied. - Network connections among interworking CSPs are instantaneously established or reconfigured. The lead CSP, which is preconfigured and governs the recovery procedure, manages the roles of available CSPs and instructs service continuation based on the original CSP data. - Access from CSUs is appropriately distributed to the interworking CSPs so as to achieve the disaster recovery, and thus mitigate the service discontinuity.
Row 6	Information flow	<ul style="list-style-type: none"> - Relevant CSPs are supposed to join a common trusted alliance in advance and set up the service level agreements (SLAs). - The lead CSP, which is preconfigured and governs the recovery procedures, inquires about the resource availability of other CSPs in the alliance to recover its cloud services to meet quality requirements of CSUs. The requested CSPs reply whether or not they are able to lease the resources. - The cloud resource management (such as create, read, update, and delete or CRUD) are operated across

		<p>multiple CSPs. The management is to enable to lease cloud resources from different CSPs in the alliance.</p> <ul style="list-style-type: none"> - The relevant CSPs exchange monitoring and auditing information of the leased resources.
Row 7	High-level figure describing the use case	<p>Case 3. Guaranteed availability – Disaster and recovery</p> <div style="border: 1px solid black; padding: 5px;"> <p>Pre-processes</p> <ul style="list-style-type: none"> • CSPs form a group with service level agreement (i.e., policy negotiation). • P-CSP replicates its data to other S-CSPs in advance. • The lead S-CSP, pre-configured, monitors P-CSP activity on behalf of the group. </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <ul style="list-style-type: none"> • S-CSPs may try to guarantee some services by prioritizing them than the other services. • S-CSPs offer the original P-CSP service for new CSUs. Ongoing services for existing CSUs, though, may not be resumed because of the lost status at that moment. Damaged P-CSP may send the status, if available, and assist service continuation at S-CSPs. • Multiple S-CSPs are assumed as the recipients. Each S-CSP supports some of the P-CSP services. A single S-CSP may be sufficient in case of backing up a small P-CSP. </div>
Row 8	Derived requirements for the cloud ecosystem	<p>The system is required to support:</p> <ul style="list-style-type: none"> - Policy negotiation including SLA management among the multiple CSPs with in a pre-established group - Self activity monitoring at a CSP or mutual activity monitoring among CSPs in a pre-established group. If the activity disappears, the detecting CSP should initiate the configured next actions. - Discovery, reservation, use, and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within a pre-established group - Application invocation over the reserved resources on other CSPs within a pre-established group - Alteration and reversion, in a dynamic manner (i.e., not relying on the pre-configuration), of CSU access to one CSP to another CSP within a pre-established group. - Exchange of monitoring and auditing information among the multiple CSPs within a pre-established group - Exchange of authentication information about CSU (user / enterprise) authentication status among the multiple CSPs within a pre-established group
Row 9	Other information specific to the use case	

A.2.4 Service continuity

Table 22 – Inter-cloud use case; service continuity

	Legend	Use case
Row 1	Use case title	Inter-cloud use case; service continuity

Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider, NaaS provider, inter-cloud federation), cloud service user (consumer, enterprise, governmental institution)
Row 3	Relevant cloud services categories	IaaS, NaaS
Row 4	Relevant cloud deployment models	Hybrid cloud
Row 5	Use case description	<ul style="list-style-type: none"> - A CSP continues its service offering by the collaboration with other CSPs, even when the original CSP terminates its business. - Available resources in CSPs other than the service-terminating CSP are discovered and reserved in advance. - Network connections among interworking CSPs are established or reconfigured. Then service-related data including user ID, user data and, application data are transferred from the original CSP to new CSPs. - Access from CSUs is appropriately changed to the interworking CSPs so that the same service is continuously offered. - If the capabilities (VM and applications) at the original CSP migrate to other CSPs, the CSU, who keeps the same user ID, can continuously access the service at the same level of performances as before.
Row 6	Information flow	<ul style="list-style-type: none"> - Relevant CSPs are supposed to join a common trusted alliance in advance and set up the service level agreements (SLAs). - The terminating CSP inquires about the resource availability of other CSPs in the alliance, and requests a reservation of available resources to continue the services. - The cloud resource management (such as create, read, update, and delete or CRUD) are operated across multiple CSPs. The management is to enable to lease cloud resources from different CSPs in the alliance.
Row 7	High-level figure describing the use case	<p>Case 4. Service continuity – Service closure and continuation</p> <div style="border: 1px solid black; padding: 5px;"> <p>Pre-processes</p> <ul style="list-style-type: none"> • CSPs form a group with service level agreement (i.e., policy negotiation). • P-CSP replicates its data to other S-CSPs in advance </div>  <p>1. A CSU accesses P-CSP services.</p> <p>2. The P-CSP initiates service closure.</p> <p>3. The P-CSP chooses S-CSPs and reserves the resources. 3a. When some CSUs are in service, the P-CSP performs migration to continue the service to the CSUs. 3b. When no CSU is in service, the S-CSP invokes application to offer the same service.</p> <p>4. The P-CSP changes the CSU access to the S-CSP.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <ul style="list-style-type: none"> • When all services and their users are moved to other S-CSPs, P-CSP will close the service. </div>
Row 8	Derived requirements for the cloud ecosystem	<p>The system is required to support:</p> <ul style="list-style-type: none"> - Policy negotiation including SLA management among the multiple CSPs within a pre-established group

		<ul style="list-style-type: none"> - Discovery, reservation, use, and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) across the multiple CSPs within a pre-established group - Capability migration (e.g., VM and applications) among multiple CSPs within a pre-established group. - Alteration of CSU access, in a dynamic manner (i.e., not relying on the pre-configuration), to one CSP to another CSP within a pre-established group. - Exchange of authentication information about CSU (user / enterprise) authentication status among the multiple CSPs within a pre-established group
Row 9	Other information specific to the use case	

A.2.5 Market transactions via brokers

Table 23 – Inter-cloud use case; market transactions via brokers

	Legend	Use case
Row 1	Use case title	Inter-cloud use case; market transactions via brokers
Row 2	Relevant actors (played roles)	Cloud service provider (IaaS provider, NaaS provider, Inter-cloud Service Broker), cloud service user (consumer, enterprise, governmental institution)
Row 3	Relevant cloud services categories	IaaS, NaaS
Row 4	Relevant cloud deployment models	Hybrid cloud
Row 5	Use case description	<ul style="list-style-type: none"> - The CSP with an ISB role (CSP-ISB) mediates between CSPs meeting the CSU's quality requirements and provides the list of selected CSPs to the CSU. - The CSP-ISB coordinates multiple services offered by other CSPs
Row 6	Information flow	<ul style="list-style-type: none"> - The SLAs of CSPs are submitted to CSP-ISB in advance. - A CSU asks the CSP-ISB to select CSPs that provide a service which satisfies the user's quality requirements. - The CSP-ISB compares the CSU quality requirements with SLAs of other CSPs. Then the CSP-ISB discovers and reserves the CSP resources that meet CSU quality requirements. - The CSP-ISB returns the CSP candidate list to the CSU. - The CSU selects a CSP or CSPs in the list.

		<ul style="list-style-type: none"> - The CSP-ISB sends cloud service adaptation request to the selected CSP to invoke and adapt to concrete cloud services and resources. - The CSP returns adaptation response to the CSP-ISB.
<p>Row 7</p>	<p>High-level figure describing the use case</p>	<p>Case 5. Market transactions via brokers – Front-end request handling and recommendation</p> <pre> graph LR CSU((CSU)) -- "1. The CSU requests the service from CSP-ISB. The request includes CSU's quality requirements" --> CSP-ISB((CSP-ISB)) CSP-ISB -- "2. CSP-ISB compares the quality requirements (including priorities) of CSU with the SLAs of multiple CSPs. The CSPs reserve the resources" --> CSP1((CSP)) CSP-ISB -- "2. CSP-ISB compares the quality requirements (including priorities) of CSU with the SLAs of multiple CSPs. The CSPs reserve the resources" --> CSP2((CSP)) CSP-ISB -- "3. The CSP-ISB informs the CSU of candidate CSPs." --> CSU CSU -- "4. The CSU chooses some of the CSPs and accesses it." --> CSP1 CSU -- "4. The CSU chooses some of the CSPs and accesses it." --> CSP2 </pre>
<p>Row 8</p>	<p>Derived requirements for the cloud ecosystem</p>	<p>The system is required to support:</p> <ul style="list-style-type: none"> - Policy negotiation including SLA management among the multiple CSPs including CSP-ISB in a pre-established group - Discovery, reservation, use, and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within a pre-established group - Creation of network connections in a dynamic manner (i.e., not relying on the pre-configuration) from the CSU to the selected CSP that provides the resources - Flexible reallocation of applications, to meet requirements at different stages in its lifecycle, across multiple CSPs.
<p>Row 9</p>	<p>Other information specific to the use case</p>	

Appendix I

Details on desktop as a service (DaaS)

Key characteristics of DaaS are as follows:

- **Enhanced management and security:** Since all applications actually run in a central server, they are much more secure than if they were installed on each user's PC because the cloud service provider can focus more on patches and virus protection. In addition, the user's IT department no longer needs to worry about support and maintenance of a high number of individual desktops.
- **Lower TCO (Total cost of ownership):** By placing emphasis on the data centre rather than individual devices, DaaS promotes longer hardware life. Organizations or enterprises seeking to avoid additional costs can switch part of their IT infrastructure from capital expenditure (CAPEX) to operating expenditure (OPEX), as they now pay for virtualized desktops. Also, by decoupling the desktop operating system from the hardware, smaller and cheaper PCs or even thin clients can be employed, leading to substantial savings.
- **Preservation of the rich client experience:** DaaS can provide an uncompromised client experience. This is due to the fact that it leverages a hypervisor layer which enables the hosting of authentic client OSs (i.e. Windows XP, Vista, etc.). Conversely, shared service environments offer a client experience that may compromise between application compatibility and user personalization.
- **Separation of service-provider and service-user responsibilities:** DaaS allows clean separation between the responsibilities of the cloud service provider and the cloud service user. The cloud service provider is responsible for everything up to the virtualized desktops (i.e. servers, storage, virtualization software, etc.), and the cloud service user is responsible for everything inside the virtualized desktops (i.e. OS image/licensing, application packaging/licensing, user profiles, etc.)

Key technical solutions of DaaS are as follows:

- **Server-based computing (SBC):** a technical solution whereby applications are deployed, managed, supported and executed on the server, not on the client. Instead, only the screen information is transmitted between server and client. This technology solves various fundamental problems that occur when executing the applications on the client itself.
- **Presentation virtualization:** a technical solution whereby an application's user interface is separated from its logic, and the user interface is presented in a different location than where the application logic is processed. This separation allows the application to be presented in one location whilst the application's deployment, configuration and maintenance are done in another location.
- **Desktop virtualization:** a technical solution separation of a PC desktop environment from a physical machine using a client-server model of computing. It involves encapsulating and delivering either access to an entire information system environment or the environment itself to a remote client device. The client device may use an entirely different hardware architecture than that used by the projected desktop environment, and may also be based upon an entirely different operating system.

- Virtual Desktop Infrastructure (VDI): the server-based computing technical solution that enables desktop virtualization and encompasses the hardware and software systems required to support the virtualized environment. It takes the users' operating environments (operating systems, applications, files and data) and recreates them in an environment hosted on a remote system, typically a virtualized desktop. The users then access this environment remotely from their computers, with all the processing associated with the environment taking place on the remote virtualized desktop.

Appendix II

Schema-mapping techniques to support multi-tenancy

A schema-mapping technique is to map multiple single-tenant logical schemas to one multi-tenant physical schema in a database. In the example in Figure II.1, three tenants' separate schemas are consolidated into one physical schema through a schema-mapping technique. Tenant 17 is working in the healthcare industry, tenant 35 is in the book business, and tenant 42 is in the automobile industry.

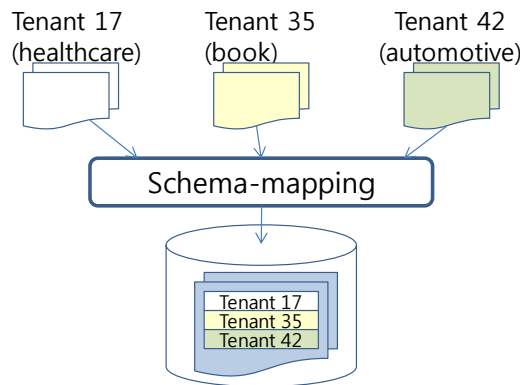


Figure II.1 - Schema-mapping technique to consolidate three tenants' schemas

Figure II.2 shows the original layout for account tables of the three tenants in the example. Tenant 17 has an extension for the healthcare industry while tenant 42 has an extension for the automotive industry.

Account_17				Account_35		Account_42		
Aid	Name	Hospital	Beds	Aid	Name	Aid	Name	Dealers
1	Acme	St. Mary	135	1	Ball	1	Big	65
2	Gump	State	1042					

Figure II.2 - The original layout for account tables of three tenants

Common schema-mapping techniques for multi-tenancy at the application layer include an extension table, a universal table, a pivot table and a chunk table. The extension table technique combines the above layouts by splitting off the extensions into separate tables with a tenant column. A row column must also be added so that the logical source tables can be reconstructed as shown in Figure II.3. The two red columns in Figure II.3 represent the overhead for meta-data in the data itself. This approach provides some sort of consolidation, but the number of tables will increase in proportion to the number of tenants.

Account_common				Account_Healthcare				Account_Automotive		
Tenant	Row	Aid	Name	Tenant	Row	Hospital	Beds	Tenant	Row	Dealers
17	0	1	Acme	17	0	St. Mary	135	42	0	65
17	1	2	Gump	17	1	State	1042			
35	0	1	Ball							
42	0	1	Big							

Figure II.3 - Extension table layout for account tables of three tenants

A universal table is a generic structure with a tenant column, a table column, and a large number of data columns having a flexible type. By keeping all of the values for a row together, this approach obviates the need to reconstruct the logical source table. However, the rows need to be very wide and the database has to handle many null values.

Universal

Tenant	Table	Col1	Col2	Col3	Col4	Col5	Col6
17	0	1	Acme	St. Mary	135	-	-
17	0	2	Gump	State	1042	-	-
35	1	1	Ball	-	-	-	-
42	2	1	Big	65	-	-	-

Figure II.4 - Universal table layout for account tables of three tenants

The following scheme is another possible option to give more flexibility and consolidation. As presented in Figure II.5, the same technique is used to compose a common table as an extension table, but the rest extended columns for each tenant are composed in an extension table with an Ext_XML column using a XML type. The XML typing makes the schema more flexible, but requires a correlated subquery to access extension data.

Account_common				Account_ext		
Tenant	Row	Aid	Name	Tenant	Row	Ext_XML
17	0	1	Acme	17	0	<ext><hospital>St. Mary</hospital><Beds>135</beds></ext>
17	1	2	Gump	17	1	<ext><hospital>State</hospital><Beds>1042</beds></ext>
35	0	1	Ball	42	0	<ext><dealers>65</dealers></ext>
42	0	1	Big			

Figure II.5 - XML Extension table layout for account tables of three tenants

Appendix III Details on SLA for cloud computing

III.1 Example of SLA metrics

Table III.1 – Example of SLA for cloud computing

SLA Item	Description	
Availability	Service availability, Availability	Probability at which the service is usable ((planned service time - service suspension time) ÷ planned service time)
	Average recovery time	Average time from a fault occurrence to completion of its repair (total repair times ÷ number of fault occurrences)
	Service suspension time	Recovery time in cases where business continuity measures against expected faults are available
		Objective of the time needed for recovery from a disaster
	Time of data recovery point	Point in time from which data is recovered
Performance	Online response time	Response time for online processing
	Online response time compliance ratio	Percentage of online transactions that have been completed within the target time
	Batch processing time	Response time for batch processing
	Batch processing time compliance ratio	Percentage of batch processing tasks that have been completed within the target time
	Maximum number of processing tasks per unit time	Maximum number of processing tasks per unit time
	Compliance ratio of maximum processing tasks per unit time	Percentage of cases where the maximum number of processing tasks per unit time is equal to or has exceeded the target number
Security	Status of the cloud service	Whether or not the cloud service provider has

provider's acquisition of the relevant security standard	acquired certification for the information security management system standard: " ISMS Certification Standards (Ver.2.0) ISO27001"
Status of certification of the party possessing management authority	Whether or not measures have been implemented against threat of information leakage that may be caused by an attacker who has gained management authority
Status of operational restrictions included in security measures taken on the management system	Whether or not there are access restrictions to prevent installation of malicious software that may cause information leakage, and to prevent the setting of unnecessary access paths
Keeping data transmitted between cloud systems confidential	Whether or not data transmitted between clouds are kept confidential
Data location	Storing data at domestic sites
Status of acquisition of a log for detection of malicious acts	Whether or not a log can be acquired to detect malicious access attempts and to enable the taking of necessary measures if such attempts have been detected
Period during which a log is kept for detection of malicious acts	Period during which evidence is kept to confirm any malicious acts conducted or correct processing
Status of communication control to block malicious communication	Whether or not communication control is available to block threat of attacks that use stepping stones and to block information from being taken outside
Status of measures against network congestion to circumvent DoD/DDoS attacks	Whether or not measures to circumvent denial of service attacks are available
Implementation of measures against malware	Whether or not measures to prevent infection by malware are available

NOTE - The role of networks in SLA metrics needs further study.

III.2 Details on SLA measurement

Cloud service users need a way to compare services from competing cloud service providers, as well as with their own internal capabilities, to offer an appropriate basis for cloud service operations. [b-TMF GB917] provides an approach that can analyse through periodically sampling the performance data in order to form a QoS report for the quality evaluation statistically. However, this approach does not provide a quantitative evaluation of the QoS and is thus not able to reflect the quality of service operation in real time.

In the service quality evaluation process, a quantitative assessment which directly reflects the service is essential. It can be quantified from both the service parameters and customer perception point of view. Quantitative units can be described and/or calibrated in terms of linear capability, throughput, or consumption-based.

- For computing, there must be a consistent benchmark that is useful for comparison across a wide range of cloud subscriber needs.
- For storage, measurement units must allow comparison of capacity, performance and quality. Quality would be rated by level.
- For networks, measurement units must allow comparison of bandwidth, performance and quality. Bandwidth can be represented in gigabits/second. Performance can be quantified in latency/jitter/throughput per minute.

III.3 Details on SLA life cycle management

SLAs are the contractual basis between the cloud service users and cloud service providers. They contain details of shared information and service level guarantees that are offered by cloud service providers. They will play an important role in future cloud development steps.

Cloud service management can be achieved by the effective SLA lifecycle management. SLA lifecycle can be normally divided into 6 steps:

- Product/service development
- Negotiation and sales
- Implementation
- Execution
- Assessment
- Decommission

The SLA lifecycle should be considered in SLA development. Different methods are combined to support each step in the SLA lifecycle, and different parameters are used for relevant steps.

In a cloud computing environment, requirements of end-to-end QoS are different. The use of SLA guarantees in a product can make the network more customer-focused. The traditional technical components of an SLA are made up of a number of negotiated service level objectives (SLO) which are based on key performance indicators (KPI). In a cloud environment, a KPI is measured by a standard unit of measure (SUoM), as shown in Figure III.1. SLA-based services are becoming a key requirement for the provisioning of IP-based cloud services in order to ensure QoS.

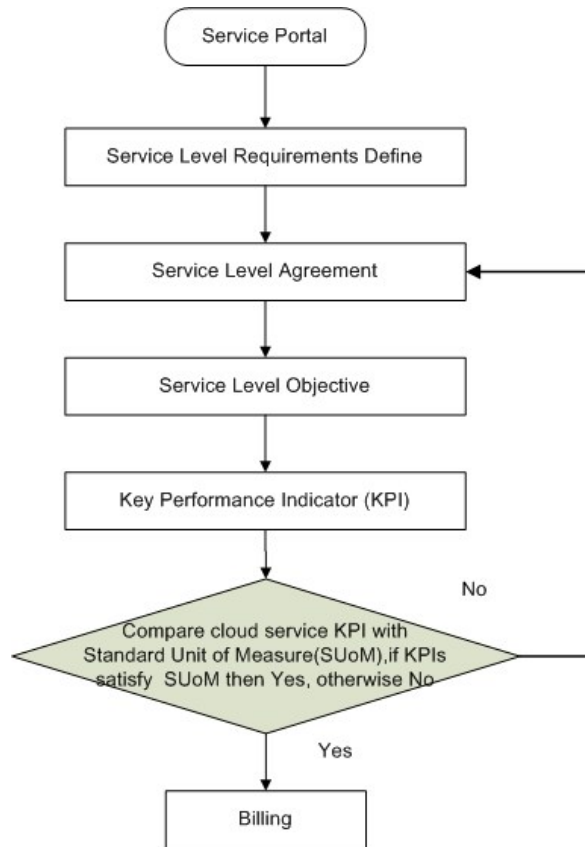


Figure III.1 - Cloud service SLA lifecycle management

Appendix IV

Additional details on business aspects in a cloud ecosystem

This appendix provides additional details on business aspects in a cloud ecosystem based upon the actors and possible business roles identified in clause 6.

IV. 1 Examples of a business-value chain

The traditional IT outsourcing services' business-value chain is usually shared by actors playing the following roles: the infrastructure vendors, the application developers, the outsourcing service integrators, and the users.

Since each level of the cloud infrastructure can be provided as services to the cloud service users, the value chain in a cloud ecosystem includes a number of possibilities. Currently, the business-value chain in a cloud ecosystem is shared among the following actors:

- The **cloud service partners** playing the role of resource suppliers, supply hardware and/or basic software to the cloud service providers.
- The cloud service providers provide virtual and/or physical computing capability, storage, communication facilities, API and/or application resources to cloud service users, i.e., the provision of infrastructure (IaaS and NaaS), platform (PaaS) and/or application services (SaaS and CaaS).
- They purchase hardware and basic software from cloud service partners playing the role of hardware and software providers and provide resources/services to other cloud service partners (e.g. playing the role of application developer) and/or the cloud service users. They also integrate applications from cloud service partners so as to provide application resources/services to the other cloud service providers (playing one or more of the possible CSP roles, including the role of inter-cloud) and/or the cloud service users. They are in the core position in the business-value chain.
- The cloud service partners playing the role of hardware and software providers supply hardware and/or basic software to the cloud service providers and those playing the role of application developers utilize the virtual and/or physical computing capability, storage, communication facilities and/or API resources provided by the cloud service providers to develop applications.
- The cloud service users do not utilize their purchased cloud services to generate additional value. The cloud service users purchase cloud services from cloud service providers. The large enterprises and institutions usually buy either private or public cloud services, while the small and medium enterprises as well as individual persons usually buy public cloud services.

Figure IV.1 shows one example of a business-value chain between actors of a cloud ecosystem. The distribution of the business value among these actors may vary.

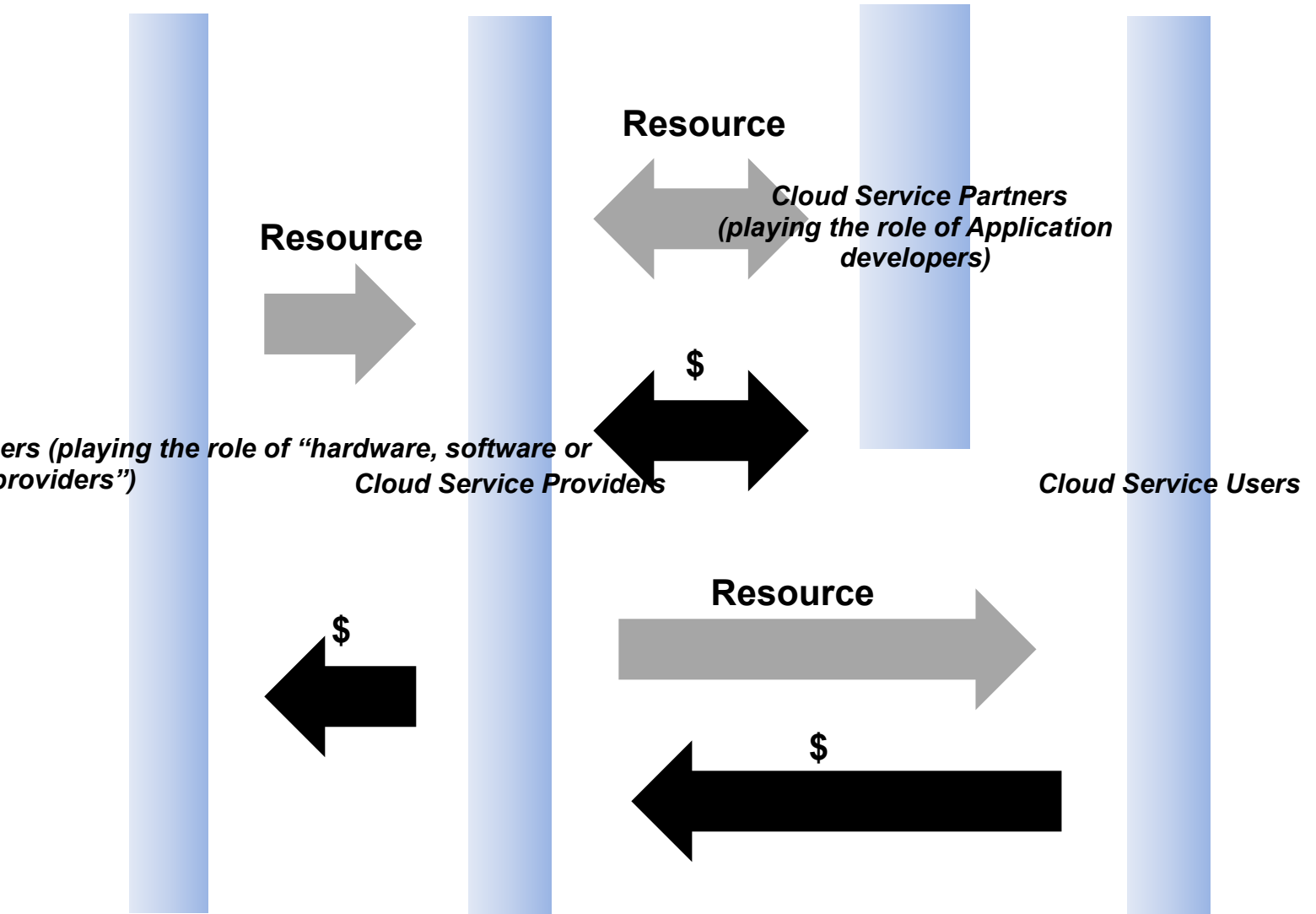


Figure IV.1 - Example of business-value chain between actors of a cloud ecosystem

Appendix V

Detailed scenarios of cloud interaction involving the inter-cloud role

V.1 Inter-cloud scenario with QoS control

In this scenario CSPs are enabled to play the role of inter-cloud with QoS control for cloud services. An example of inter-cloud scenario with QoS control is the following.

The CSP playing the inter-cloud role supports the capability to monitor the QoS of cloud services offered by different cloud service providers, and chooses the most suitable cloud service provider to provide the requested service.

When the CSP playing the role of inter-cloud receives a service request from the originating cloud service provider, it processes the request. This process takes into account the originating cloud service provider's QoS requirements (the request information may include service type information, the required QoS parameters information, etc.) and the candidate terminating cloud service provider(s)' resource status (eventually monitored or got from other Inter-Clouds). Then, the CSP returns the result to the originating cloud service provider.

NOTE 1 – For example, in the case of strict bandwidth requirements, resource reservation of the candidate terminating cloud service provider(s) can be applied, in addition to monitoring their resource status. This process includes resource reservation for the multiple candidates, acknowledgement for the selected one, and release for the un-selected ones.

NOTE 2 – QoS control needs further study (e.g. performance monitoring not only at network-level but also at storage- and process-level).

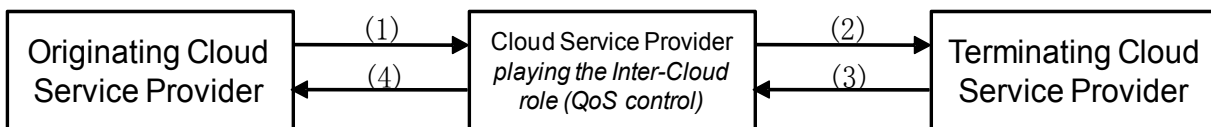


Figure V.1 - Example of inter-cloud scenario with QoS control

V.2 Inter-cloud scenario with cloud service composition

Cloud service composition enables the CSP to play the role of inter-cloud in order to provide a service to the originating CSP via mechanisms by which multiple services offered by different CSPs are invoked under the control of a service logic (the service logic describes the order of the invoking of services and the related parameters).

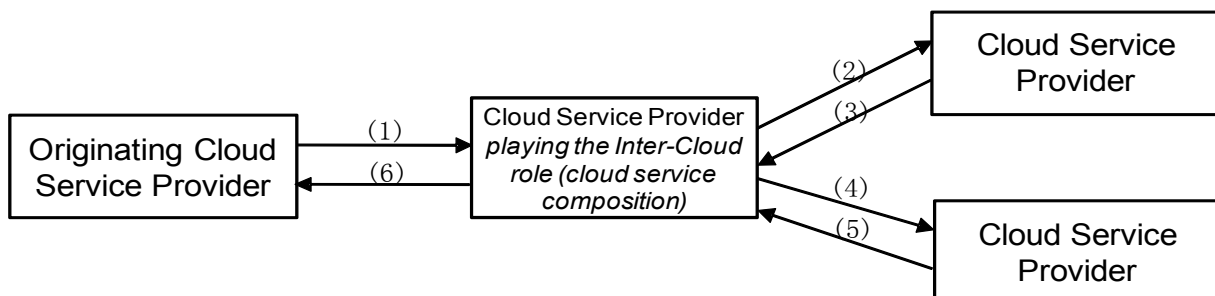


Figure V.2 - Example of inter-cloud scenario with cloud service composition

There are two different kinds of cloud service composition: static and dynamic cloud service compositions.

For static cloud service composition, the CSP playing the role of inter-cloud uses a concrete service logic specifying concrete services, interface invoking information, data flow (services input/output parameters) and control flow (services invoking order) of the services. The concrete service logic is given by the originating CSP (Arrow (1) in Figure V.2). The CSP playing the role of inter-cloud invokes these concrete services according to the data flow and control flow and gets the results of these services. The service may comprise resources and capabilities of multiple CSPs (Arrows (2), (3), (4), and (5) in Figure V.2). The CSP playing the role of inter-cloud then composes the entire service as the final result and returns it to the originating cloud service provider (Arrow (6) in Figure V.2).

For dynamic cloud service composition, the CSP playing the role of inter-cloud uses an abstract service logic specifying service classes (different services which provide the same service function belong to the same service class), data flow and control flow of these services. The abstract service logic is given by the originating CSP (Arrow (1) in Figure V.2). The CSP playing the role of inter-cloud translates the abstract service logic into the concrete service logic before searching the concrete services that can fulfil the requirements. Specifically, the translation is to replace the service classes with concrete services and create interface invoking information for the services. Then the CSP playing the role of inter-cloud executes the concrete service logic and gets the results of the services. Finally, it composes the entire service as the final result and returns it to the originating cloud service provider.

Appendix VI Details on mobile cloud

Mobile cloud can be considered as a kind of cloud computing with evolved computing processing, as processing and data storage move from desktop and laptops to large data centres.

Several terms and definitions related to mobile cloud have been developed till now, and the following two terms are the most relevant ones at the present time:

- Mobile cloud applications [b-mob-cloud-1]: these are applications that:
 - are aimed at mobile devices with minimal processing power. This would include smartphones, feature phones and low-cost phones, but would not include netbooks, mobile internet devices and laptops.
 - exclude read-only applications.
 - require some form of mobile-specific rendering and transcoding.
- Mobile cloud computing [b-mob-cloud-3]: this term refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device from which an application is launched. To consumers, a cloud-based mobile application looks and feels just like any traditional application purchased or downloaded from a mobile application store. However, the application sends processing tasks to the cloud and stores data in the cloud, and receives results generated by the resources in the cloud, including computing resources and storage sources, not from the handheld device itself.

VI.1 Configuration of a mobile cloud

In the case of a mobile cloud, the mobile device (client) can be defined as software (service) which relies on the cloud to process/deliver the application. It essentially acts as the on-device gateway which enables the user to access the information which is stored and processed within the cloud.

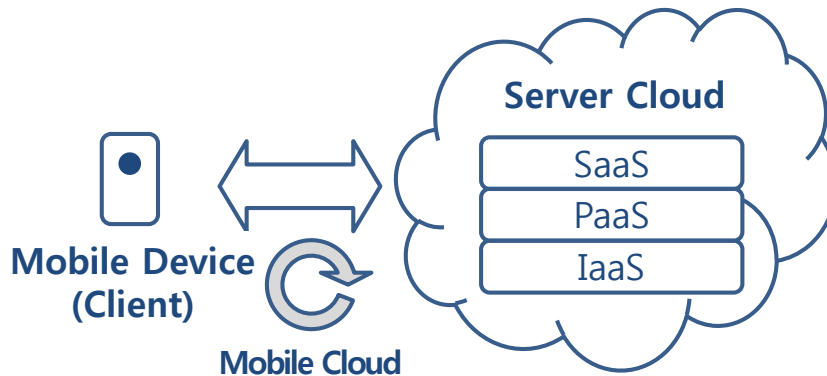


Figure VI.1 - Basic mobile cloud configuration

Table VI.1 – Examples of implementations supporting mobile cloud features

Clients	Mobile cloud applications (Soonr, etc), browsers
SaaS	MobileMe, Funambol, Salesforce.com, etc.
PaaS	Google AppsEngine, Windows Azure, Force.com, etc.

IaaS	AWS, HP Adaptive Infrastructure, etc.
------	---------------------------------------

The clients in Figure VI.1 and Table V.1 are applications which function independently of the network and where processing and data storage thus occur on the handset.

As the mobile cloud becomes ubiquitous, it is likely to see widespread deployment of the following categories of client applications:

- Mobile cloud applications: they are downloadable, client-side applications which store data in the cloud rather than on the mobile device. Rather than obliging the end user to launch a web browser and then navigate the mobile web, these applications communicate directly with the cloud. NOTE - the difference between an installed mobile application and a mobile cloud application is that a mobile cloud application needs more computing power, large scale storage, real-time data access to the cloud server, mash-up API, and n-screen capability, than an installed mobile application.
- Web browsers: these applications are wholly web-based operating on data stored in the cloud. They do not require any other application on the handset.

Compared with traditional cloud computing, another important capability of mobile cloud services is the possibility to reuse device capabilities.

The future of mobile cloud services includes “device as a service”: this service could reuse the device capabilities (for instance, camera, GPS, memory, etc.) available among devices. In this case, it is expected that a cloud can be created by those mobile devices and these are able to interact with each other in order to use respective device capabilities such as shown in Figure VI.2. For example, a camera capability is available in device A, but device B has no camera capability. So, if the camera capability of device A can be exposed to device B, device B can use it.

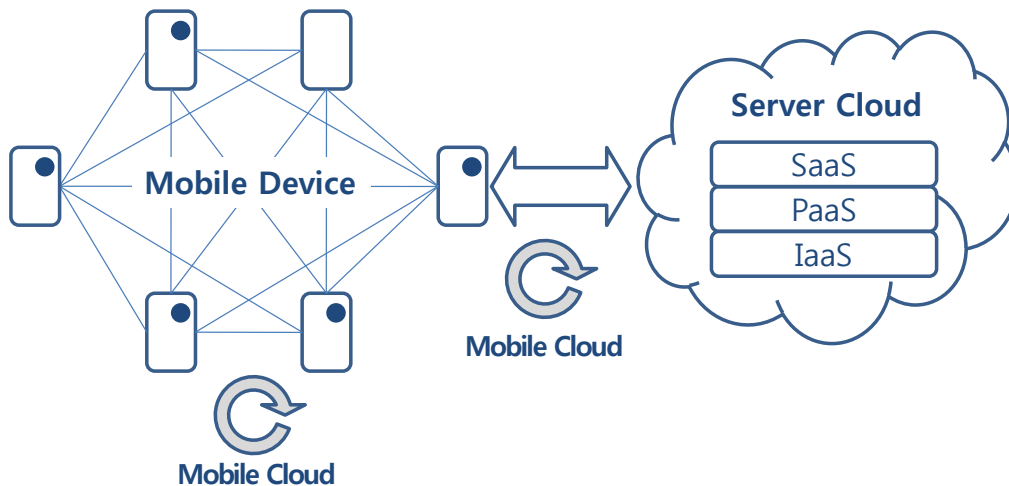


Figure VI.2 - Extended configuration of a mobile cloud

Concerning related standards developments, the World Wide Web Consortium (W3C) has already started work in the fields of device APIs and related security policy in the W3C DAP working group WG. One goal of the DAP WG is to define API specifications for devices' services that can be exposed to widgets and web applications, the target devices being different types of devices including desktop computers, laptop computers, mobile internet devices (MIDs), cellular phones, TV, etc. Also, the DAP WG works to define a framework for the expression of security policies that govern the access of web applications and widgets to security-critical APIs (the W3C DAP WG is currently reviewing the XACML language for security policy description).

Bibliography

- [b-cloud-fed] *Cloud federation*, [http://www.cloudswitch.com/blog/tag/cloud federation](http://www.cloudswitch.com/blog/tag/cloud%20federation)
- [b-cloud-fed-ic] *Cloud Federation and the Intercloud*
<http://www.cloudswitch.com/page/cloud-federation-and-the-intercloud>
- [b-CSA Glossary] *Appendix: Cloud Security Alliance Glossary*
<https://cloudsecurityalliance.org/research/security-guidance/>
- [b-discuss-group-wp] *Cloud Computing Use Cases Discussion Group White Paper Version 4.0*, available at <http://cloud-computing-use-cases.googlegroups.com/>
- [b-GICTF IC] *Use Cases and Functional Requirements for Inter-Cloud Computing, GICTF White Paper, August 2010*
- [b-HBR] *Harvard Business Review (Moore), June 1993*
- [b-infoworld] *Cloud Computing Deep Dive, Infoworld, Sep. 2009*, available at http://akamai.infoworld.com/sites/infoworld.com/files/pdf/infoworld_cloudcomputing_premium.pdf
- [b-itechthoughts] *Cloud Computing: The New IT Paradigm, 2010*, available at <http://itechthoughts.wordpress.com/2010/02/23/cloud-computing-the-new-it-paradigm/>
- [b-mob-cloud-1] *ABIresearch, "Mobile Cloud Computing," 2009*
- [b-mob-cloud-2] *Junifer Research, Mobile Cloud Applications and Service, 2009*
- [b-mob-cloud-3] *Mobile Cloud Computing: \$9.5 Billion by 2014*,
http://www.readwriteweb.com/archives/mobile_cloud_computing_95_billion_by_2014.php
- [b-Moriana] *Service Delivery Platforms in the WEB 2.0 Era, The Moriana Group, Sep 2008*
- [b-NIST] *NIST, The NIST Definition of Cloud Computing, version 15 (2009)*,
<http://csrc.nist.gov/groups/SNS/cloud-computing/>
- [b-SC38 N430] *Study Group Report on Cloud Computing*
- [b-TMF GB917] *TMF Guidebooks, GB917, SLA Management Handbook, Release 2, 26 July 2005*,
<http://www.tmforum.org/Guidebooks/GB917SLAManagement/30753/article.html>
- [b-UN-accessibility] *UN Convention on the Rights of Persons with Disabilities, Article 9 Accessibility*
- [b-vmware] *Virtual desktop infrastructure, whitepaper, vmware.com*,
http://www.vmware.com/pdf/virtual_desktop_infrastructure_wp.pdf
- [b-ITU-T Y.2240] *Recommendation ITU-T Y.2240, Requirements and capabilities for NGN service integration and delivery environment*

