International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3501

(05/2013)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Cloud Computing

Cloud computing framework and high-level requirements

Recommendation ITU-T Y.3501

ITU International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3999**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3501

Cloud computing framework and high-level requirements

Summary

Recommendation ITU-T Y.3501 provides a cloud computing framework by identifying high-level requirements for cloud computing. It specifies the requirements which are derived from an analysis of several use cases.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.3501	2013-05-22	13

Keywords

Cloud computing, cloud service, framework, requirement, use case.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3501

Cloud computing framework and high-level requirements

1 Scope

This Recommendation provides a cloud computing framework by identifying the high-level requirements for cloud computing. It addresses the general requirements and use cases for:

– cloud computing;

– infrastructure as a service (IaaS), network as a service (NaaS), and desktop as a service (DaaS) cloud services;

– inter-cloud, end-to-end resource management, and cloud infrastructure.

The first edition of this Recommendation addresses a set of use cases and related requirements which are included in Appendix I. The next edition of this Recommendation will provide an update of this set of use cases and requirements. See Appendix II for further information on the methodology and edition plan of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2013), *Cloud computing framework for end-to-end resource management.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 hypervisor [ITU-T Y.3510]: A type of system software that allows multiple operating systems to share a single hardware host.

NOTE – Each operating system appears to have the host's processor, memory and other resources, all to itself.

3.1.2 resource management [ITU-T Y.3520]: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud service customer: A person or organization that consumes delivered cloud services within a contract with a cloud service provider.

3.2.2 cloud service partner: A person or organization which provides support to the services offered by a cloud service provider (e.g., service integration).

3.2.3 cloud service provider: An organization that provides and maintains delivered cloud services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

DaaS Desktop as a Service

IaaS Infrastructure as a Service

IP Internet Protocol

NaaS Network as a Service

PaaS Platform as a Service

QoE Quality of Experience

QoS Quality of Service

SaaS Software as a Service

SLA Service Level Agreement

VLAN Virtual Local Area Network

VM Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is required**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

In the body of this document and its appendices, the words shall, shall not, should and may sometimes appear, in which case they are to be interpreted, respectively as, is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

For readability, the short titles are attached to the requirements for referring to use cases in Appendix I.

6 General requirements for cloud computing

The general requirements for cloud computing derived from the use cases in Appendix I are as follows:

– **Service life-cycle management**: It is required that cloud computing supports automated service provisioning, modification and termination during the service life-cycle.

– **Regulatory aspects**: It is required that all applicable laws and regulations be respected, including those related to privacy protection.

– **Security**: It is required that the cloud computing environment be appropriately secured to protect the interests of all persons and organizations involved in the cloud computing ecosystem.

– **Accounting and charging**: It is recommended that cloud computing supports various accounting and charging models and policies.

– **Efficient service deployment**: It is recommended that cloud computing enables efficient use of resources for service deployment.

– **Interoperability**: It is recommended that cloud computing systems comply with appropriate specifications and/or standards for allowing these systems to work together.

– **Portability**: It is recommended that cloud computing supports the portability of software assets and data of cloud service customers (CSCs) with minimum disruption.

– **Service access**: Cloud computing is recommended to provide CSCs with access to cloud services from a variety of user devices. It is recommended that CSCs be provided with a consistent experience when accessing cloud services from different devices.

– **Service availability, service reliability and quality assurance**: It is recommended that the cloud service provider (CSP) provides end-to-end quality of service assurance, high levels of reliability and continued availability of cloud services according to the service level agreement (SLA) with the CSC.

7 General requirements for IaaS

The general requirements for IaaS derived from the use cases in clause I.2 are as follows:

– **Configuration, deployment and maintenance of resources**: IaaS CSP is recommended to configure, deploy and maintain computing, storage and networking resources to CSC.

– **Use and monitoring of resources**: IaaS CSP is recommended to provide the capability for CSC to use and monitor computing, storage and networking resources so that they are able to deploy and run arbitrary software.

8 General requirements for NaaS

The general requirements for NaaS derived from the use cases in clause I.3 are as follows:

– **On-demand network configuration**: It is required that the CSP provides the network capability, which can be configured on demand by the CSC (user and applications).

– **Secure connectivity**: It is required that the NaaS CSP provides secure connectivity.

– **QoS-guaranteed connectivity**: The NaaS CSP is recommended to provide QoS-guaranteed connectivity according to the negotiated SLA.

– **Heterogeneous networks compatibility**: It is recommended that the CSP supports network connectivity through heterogeneous networks.

9 General requirements for DaaS

The general requirements for DaaS derived from the use cases in clause I.4 are as follows:

– **Configurability of the virtual environment**: It is recommended that a user is capable of configuring the virtual desktops' virtual environment, such as the CPU, memory, storage, network, etc.

– **Fast boot-up time**: The DaaS CSP is recommended to provide CSCs with appropriate boot-up time of their virtual desktops.

– **QoE**: The DaaS CSP is recommended to provide an acceptable user experience, including the running speed of application programs and the capability to select and run various applications, when application programs run in their CSC devices.

– **Single sign-on access control**: It is recommended that a CSC is capable of getting all of a DaaS functionality with the appropriate security requirements through a single sign-on mechanism.

10 General requirements for inter-cloud

The general requirements for inter-cloud derived from the use cases in clause I.5 are as follows:

– **On-demand assignment of cloud computing resources among CSPs**: For assigning cloud resources among CSPs on demand, it is required that a CSP defines (a) a trusted relationship between cooperating CSPs; (b) an appropriate agreement and means of exchanging data on cost, performance and other information for each resource; and (c) an agreed methodology for requesting, using and returning the resources of other CSPs.

– **Resource and load distribution**: A CSP in the inter-cloud federation is required to utilize appropriate resources distributed in other CSPs for wide-area load distribution according to the required promptness, flexibility and cost.

– **User environment adaptation**: A CSP is required to detect user environment changes, discover alternative resources in other CSPs for these changes, and migrate the service environment smoothly with minimum impact based on the CSC's approval.

NOTE – These actions are to be performed for all users.

– **Inter-cloud service intermediation**: Inter-cloud service intermediation enables the CSP to select the most suitable services and to create new services by integrating services offered by other CSPs. It is recommended that the CSP engages in support of intermediation for multiple cloud services of various services such as IaaS, NaaS, PaaS and SaaS.

– **Large-scale migration**: A CSP in the inter-cloud federation is recommended to be able to guarantee continuity of all the services in this CSP by large-scale service migration to other federated CSPs with minimum impact during a desired period. It is recommended to consider the priority of services when migrating.

11 General requirements for end-to-end cloud resource management

The general requirements for end-to-end cloud resource management derived from the use cases in Appendix I.6 are as follows:

– **Manageability for a single cloud service**: It is required that the CSP be able to collect management, telemetry and diagnostics and/or status information from components executing in various layers of cloud service implementation and report the information to the CSC.

– **Manageability for multiple cloud services**: It is recommended that multiple CSPs work together to offer comprehensive status awareness and management information to expand across multiple cloud data centres as composite cloud services are built from multiple services implemented by multiple cloud providers, requiring the need for multi-cloud, end-to-end management data.

NOTE – For more information on end-to-end resource management, refer to [ITU-T Y.3520].

12 General requirements for cloud infrastructure

The general requirements for cloud infrastructure from the use cases in Appendix I.7 are as follows:

– **Resource abstraction and control**: It is required for cloud infrastructure to provide resource abstraction and control capability to cloud services.

– **Resource provisioning**: It is required for cloud infrastructure to provide collaboratively compute, storage, and network resources to cloud services and supporting functions.

NOTE – For more information on compute, storage, network resources as well as resource abstraction and control, refer to [ITU-T Y.3510].

13 Security considerations

It is recommended that the security requirements of [b-ITU-T Y.2201], [b-ITU-T Y.2701], and applicable X, Y and M series of ITU-T security Recommendations be taken into consideration; this includes access control, authentication, data confidentiality, communications security, data integrity, availability and privacy.

Appendix I

Use cases of cloud computing

(This appendix does not form an integral part of this Recommendation.)

This appendix identifies use cases of cloud computing. The table below shows the template used for the description of use cases.

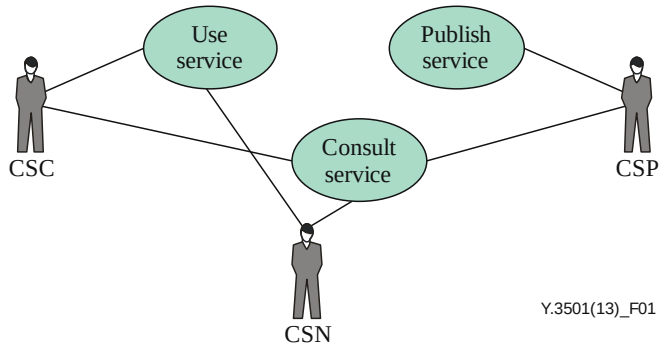
Table I.1 – Template for the description of a use case

Use case	
Name	Title of use case
Abstract	Overview and features of use case
Roles	Roles relating to/appearing in use case
Figure	Figure to present the use case. (A UML-like diagram is suggested for clarifying relations between roles)
Pre-conditions (optional)	Pre-conditions represent the necessary conditions or use cases that should be achieved before starting the described use case. NOTE – As dependency may exist among different use cases, pre-conditions and post-conditions are introduced to help understand the relationships among use cases.
Post-conditions (optional)	As the same for pre-condition, the post-condition describes conditions or use cases that will be carried out after the termination of a currently described use case.
Requirements	The title of requirements derived from the use case. For example: – Large-scale migration

Table I.2 – List of use cases

Domains	**Use cases**
Generic use case	– General CSC-CSP-CSN use case – Use case publish service – Use case consult service – Use case use service
IaaS	– IaaS general use case
NaaS	– NaaS general use case
DaaS	– DaaS general use case
Inter-cloud	– Inter-cloud use case for federation – Inter-cloud use case for intermediation
Cloud resource management	– End-to-end cloud service resource management use case
Cloud infrastructure	– Cloud infrastructure use case

I.1 Generic use case

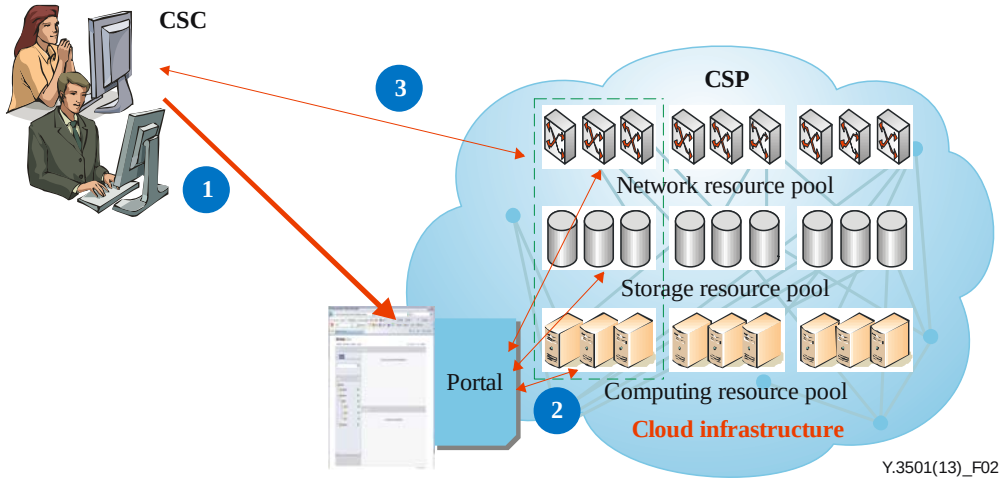
Use case	
Name	General CSC-CSP-CSN use case
Abstract	This general use case, which describes the general activities of the CSC, CSP and CSN, consists of a set of use cases. It introduces a basic scenario where a CSP publishes a cloud service. A CSC or CSN consults this cloud service and uses this cloud service. These use cases clarify the relationships between these three main cloud roles.
Roles	CSC, CSP, CSN
Figure	
Included use Cases	– UC-US (Use case use service) – UC-CS (Use case consult service) – UC-PS (Use case publish service)

Use case	
Name	Use case publish service
Abstract	A CSP publishes cloud service information to the public so that any users including a CSP, CSC or CSN could use the published cloud service. In terms of service publishing, the CSP puts the service to a service catalogue which will be accessible by others. The CSP also maintains the catalogue.
Roles	CSP
Pre-conditions (optional)	
Post-conditions (optional)	– The CSP should maintain the public service.
Requirements	– Service life-cycle management – Security – Efficient service deployment – Portability – Regulatory aspects – Service availability, service reliability and quality assurance – Service access – Accounting and charging

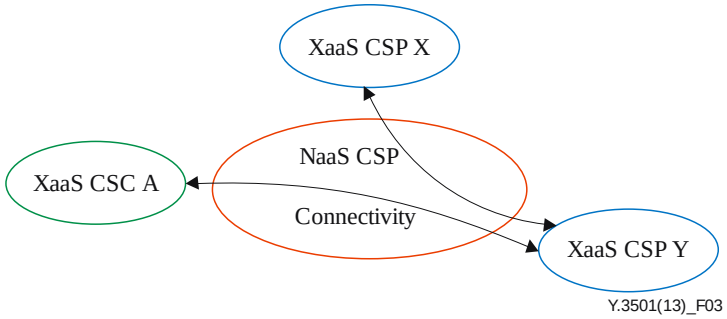
Use case	
Name	Use case consult service
Abstract	A CSC, CSP or CSN consults a published service. For all the published services in the cloud service catalogue, any users including the CSC, CSP and CSN can access them. The consult scenario refers to consulting published-service details and associated SLAs.
Roles	CSC, CSP, CSN
Pre-conditions (optional)	– The service to be used has already been published by a CSP (UC-PS). – The CSC, CSP or CSN has been authenticated.
Post-conditions (optional)	– A given service should be accessible.
Requirements	– Security – Service availability, service reliability and quality assurance – Service access – Interoperability – Regulatory aspects – Accounting and charging

Use case	
Name	Use case use service
Abstract	A CSC or a CSN uses a published service. According to the agreement of the SLA, the user invokes the cloud service.
Actors	CSC, CSN
Pre-conditions (optional)	– The service to be used has already been published by a CSP (UC-PS). – The CSC or the CSN has been authenticated.
Post-conditions (optional)	– The used service should be kept available during the whole invocation. – The SLA should be met for service use.
Requirements	– Service life-cycle management – Security – Portability – Interoperability – Regulatory aspects – Service availability, service reliability and quality assurance – Service access – Accounting and charging

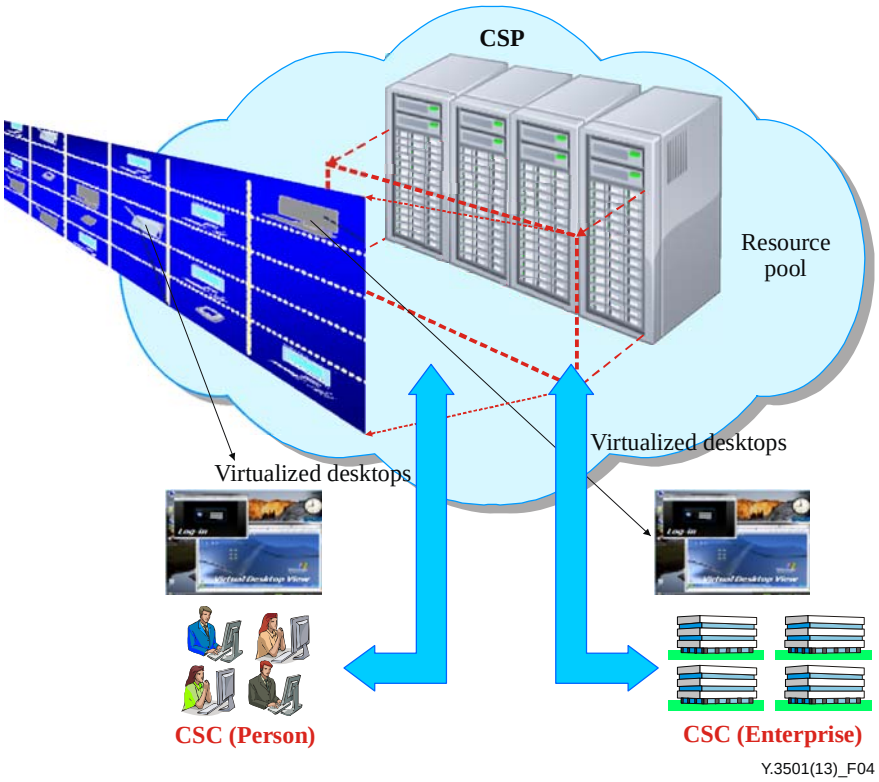
I.2 IaaS general use case

Use case	
Name	IaaS general use case
Abstract	CSC uses IaaS services including computing, storage and network capabilities to deploy and run arbitrary applications.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– ① The CSC has accessed the IaaS service through the CSP portal with an appropriate security mechanism. – ② The CSC has selected the template or configured a specific VM and/or physical host. – ② The CSC has selected the storage resources, such as block, file and object storage, then attached them via their computing capabilities or used them directly. – ② The CSC has selected the network connectivity services, such as the IP address, VLAN, firewall and load balance, and then applied them to the related computing and/or storage capabilities. – ② The CSC confirmed the SLAs and charge model with selected computing, storage and network connectivity services provided by the CSP.
Post-conditions (optional)	– ③ The CSC manages and monitors computing, storage and network capabilities with arbitrary applications. – ③ The CSP configures, deploys and maintains hypervisors and storage resources. – ③ The CSP establishes, configures, delivers and maintains network connectivity to the CSC. – ③ The CSP provides security infrastructure to the CSC.
Requirements	– Configuration, deployment and maintenance of resources – Use and monitoring of resources

I.3 NaaS general use case

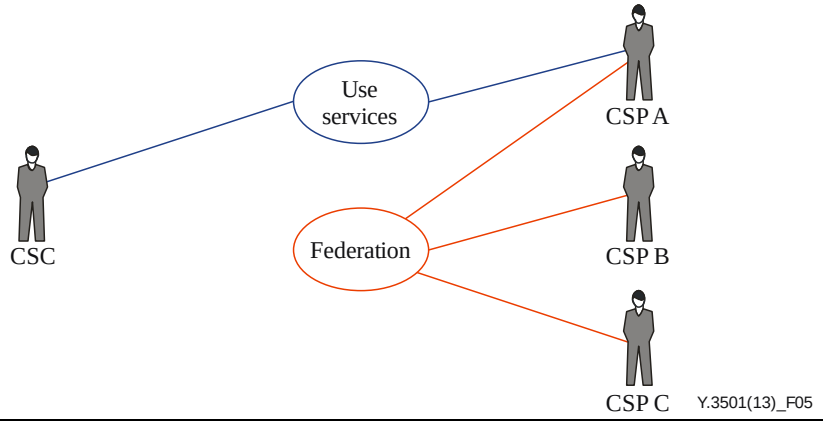
Use case	
Name	NaaS general use case
Abstract	A NaaS CSP sets up, maintains, and releases the network connectivity between CSCs and between the CSP and CSC as a cloud service. This can include on-demand and semi-permanent connectivity.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– There is no connectivity between XaaS CSC A and XaaS CSP Y. – There is no connectivity between XaaS CSP X and XaaS CSP Y. – Either XaaS CSC A or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity. – Either XaaS CSP X or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity.
Post-conditions (optional)	– XaaS CSC A and XaaS CSP Y can communicate with each other. – XaaS CSC X and XaaS CSP Y can communicate with each other.
Requirements	– On-demand network configuration – Heterogeneous networks compatibility – QoS-guaranteed connectivity – Secured connectivity

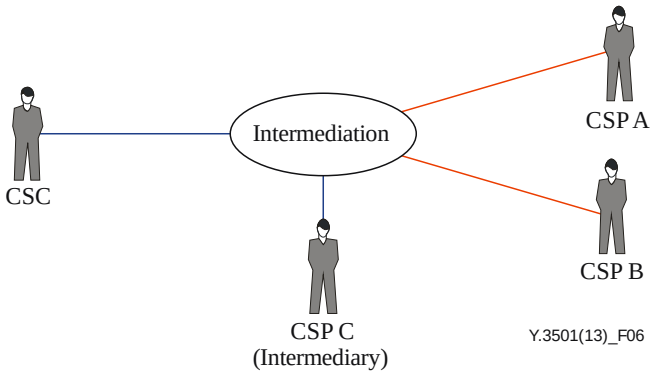
I.4 DaaS general use case

Use case	
Name	DaaS general use case
Abstract	– Between a consumer and a CSP: In this scenario, a consumer accesses and uses data or applications in a CSP which offers a virtual desktop service. A consumer can enjoy the environment with all programs and applications which are identical with those of traditional PCs. 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. Since all data is totally stored with password protection and managed in the CSP, all the consumer has to do is keep up with a password. – 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. – Between an enterprise, a consumer, and a CSP: In this scenario, the enterprise makes the consumer work with its internal processes 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 data to the consumer by accessing the enterprise to handle or bypass corresponding data.
Roles	CSP, CSC
Figure	
Pre-conditions (optional)	– A CSP offers the configuration menu of the virtual desktop to CSCs. – A CSC specifies parameter-settings shown in the configuration menu.

Use case	
Post-conditions (optional)	– A CSC uses DaaS service.
Requirements	– QoE – Fast boot-up time – Configurability of the virtual environment – Single sign-on access control

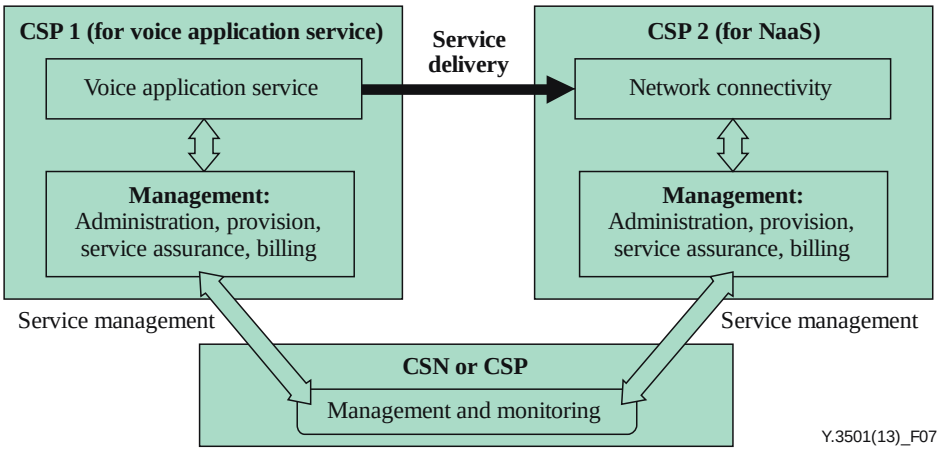
I.5 Inter-cloud use case

Use case	
Name	Inter-cloud use case for federation
Abstract	CSPs federate to provide a service to the CSC
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSPs federate with each other by establishing a trust relationship and policy settlement. – A CSC uses a service provided by one of the federated CSPs. – Case-A: The CSP that offers the service to the CSC is going to spend all resources due to of overload, or has lost the resources due to disaster. – Case-B: The CSC changes its environment (e.g., location) and reaches the CSP from a place which is further away than before.
Post-conditions (optional)	– Case-A: The CSP ensures that its services continue to be offered by the support of other federated CSPs, even when performance or availability of the service may be degraded due to CSP's resource problems (e.g., overload or disaster). – Case-B: Another CSP in the federation, on behalf of the CSP which has offered the service to the CSC, provides a new appropriate service environment to the CSC to compensate for possible degradation, even when performance or availability of the service may be degraded due to a CSC's environmental change (e.g., location changes).
Requirements	– On-demand assignment of cloud resource among CSPs – Resource and load distribution – Large-scale migration – User environment adaptation

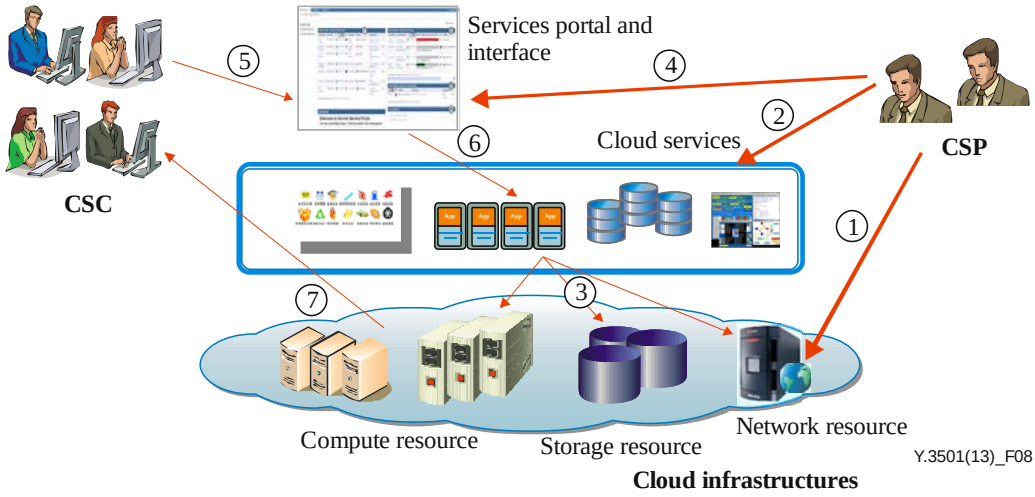
Use case	
Name	Inter-cloud use case for intermediation
Abstract	A CSP intermediates services from other CSPs to provide a service to the CSC.
Actors	CSP, CSC
Figure	
Pre-conditions (optional)	
Post-conditions	– A CSP selects a service from other CSPs' services, and intermediates them to a CSC. – A CSP creates a new service by integrating several services in other CSPs, and intermediates them to a CSC.
Requirements	– On-demand assignment of cloud resource – Inter-cloud service intermediation

I.6 End-to-end cloud resource management use case

Use case	
Name	End-to-end cloud resource management use case
Abstract	A CSC uses a service offered by multiple CSPs and/or CSNs, one of which supports customer services. In order to deliver customer services properly, the CSN manages end-to-end health and QoS of the service offered by a CSP which can integrate several base services offered by multiple CSPs.
Actors	CSC, CSP, CSN

Use case	
Figure	 As shown in the above figure, this problem requires visibility into CSP2's management systems delivering the voice application service, as well as similar CSP's management systems. When the voice application customer calls into CSP2 support, then the CSP2 support person should have visibility into the health and welfare of the CSP1's voice application service, its underlying cloud infrastructure, as well as the local service provider's network management systems relevant to the voice application service.
Pre-conditions	In this service syndication example involving multiple clouds, voice application is being provided as SaaS to a CSP that is bundling it with other services and reselling a package to a CSC. Although a voice application service provider may run a global data network, it does not own the carrier's network and enterprise infrastructures that actually connect the cloud and network services to end-user devices. A local service provider might provide an IP network service to provide an optimized voice application experience for an enterprise customer's employees using the voice application service. In this use case, there are the two types of connection paths, namely a service delivery path and a service management path. When the CSC is experiencing a problem with the voice application service, the responsibility for the diagnostics, management and resolution of the problem involves more than one service provider. End-to-end resource management cannot require a major system integration effort with each new service deployment. In order for the composite cloud computing services to work effectively, all the prerequisite services of both the CSP1 and CSP2 must function properly.
Post-conditions	Voice application service is restored rapidly and easily. End-to-end resource management of components that deliver the voice application customer service support and the administrative, provisioning, service assurance and billing that make up a complete voice application service is necessary.
Requirements	– Manageability for a single cloud service – Manageability for multiple cloud services

I.7 Cloud infrastructure use case

Use case	
Name	Cloud infrastructure use case
Abstract	The CSP uses cloud infrastructure which consists of compute, storage and network resources to deploy and deliver any kind of cloud services. The CSC accesses and uses cloud services deployed in and delivered by cloud infrastructure.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– ① A CSP builds a cloud infrastructure with cloud resources including compute, storage and network resources. – ②,③ The CSP allocates and configures related compute, storage and network resources in the cloud infrastructure needed for deploying any kind of cloud services through resource orchestration functions. – ④ The CSP publishes the deployed cloud services in the catalogue of the cloud service portal. – ⑤ A CSC accesses the cloud services published by the CSP through service portals or service interfaces which are protected by appropriate security mechanisms. – ⑥ Related cloud resources and capabilities have been invoked to respond to the CSC's access and interaction.
Post-conditions	– ⑦ The CSP manages and monitors pooled compute, storage and network resources in the cloud infrastructure.
Requirements	– Resource provisioning – Resource abstraction and control

Appendix II

Methodology and edition plan of this Recommendation

(This appendix does not form an integral part of this Recommendation.)

This Recommendation adopts a use-case-driven approach. Use cases are selected and elaborated first. Based on these use cases, relevant requirements are derived. As an example shown in the following figure, one use case may derive multiple requirements.

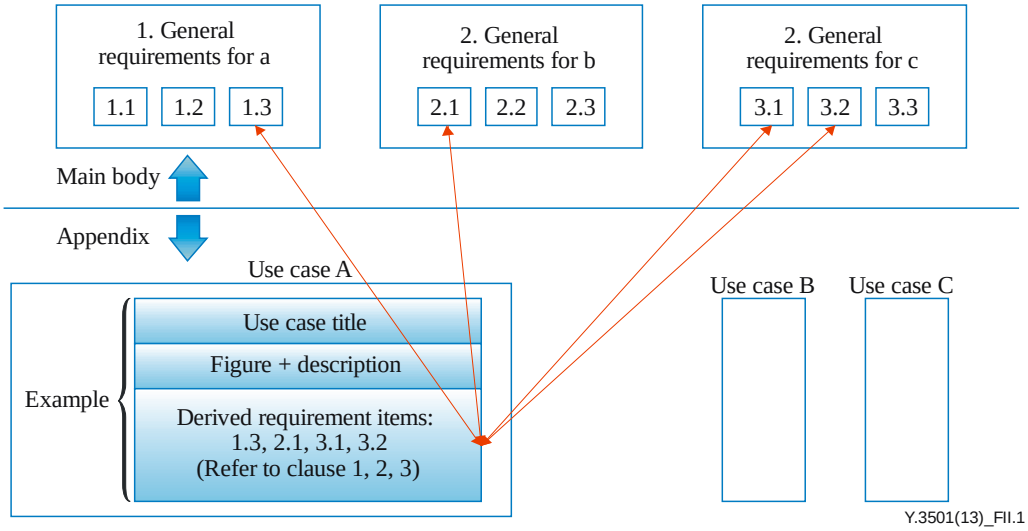
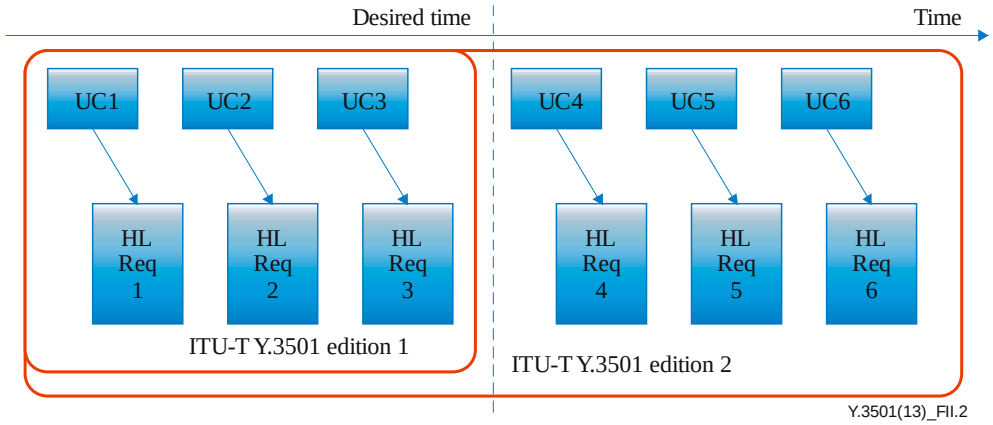


Figure II.1 – Methodology including mapping of use cases and requirements

The use-case-driven approach may also ease the preparation of future editions of this Recommendation. As explained in the next figure, a new edition will include new use cases with derived new requirements.



UC: Use case
HL Req: High-level requirement

Figure II.2 – Editions of this Recommendation

NOTE – For the sake of readability, this Recommendation describes the requirements with short titles. Exact description of short titles is provided in relevant clauses of this Recommendation.

The following table presents the edition plan of this Recommendation based on the progress of the corresponding content.

Table II.1 – Edition plan of this Recommendation

Scope		Edition 1	Edition2
General requirements for cloud computing		O	Extended
General requirements for architecture			O
General requirements for NaaS		O	Extended
General requirements for IaaS		O	Extended
General requirements for PaaS			O
General requirements for SaaS/CaaS			O
General requirements for DaaS		O	Extended
General requirements for Inter-cloud		O	Extended
General requirements for end-to-end cloud resource management		O	Extended
General requirements for cloud infrastructure		O	Extended
Others general requirements			O
Security consideration		O	Extended
Use case	Generic use cases	O	Extended
	NaaS general use case	O	Extended
	IaaS general use case	O	Extended
	PaaS general use case		O
	SaaS/CaaS general use case		O
	DaaS general use case	O	Extended
	Inter-cloud general use case	O	Extended
	End-to-end cloud resource management use case	O	Extended
	Cloud infrastructure use case	O	Extended
	Other use cases		O
NOTE – The mark "O" indicates initial requirements and use cases are prepared, "extended" indicates additional requirements and use cases will be provided.			

Bibliography

[b-ITU-T Q.1231] Recommendation ITU-T Q.1231 (1999), *Introduction to Intelligent Network Capability Set 3.*

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN.*

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[b-ITU-T FG Cloud TR] ITU-T FG Cloud TR (2012), Focus Group Cloud Computing Technical Report, Version 1, *Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014