International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

**Y.3501**

(06/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Cloud Computing

# Cloud computing – Framework and high-level requirements

Recommendation ITU-T Y.3501

ITU-T Y-SERIES RECOMMENDATIONS

## GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

| | |
|---|---|
| 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 |
| Enhancements to NGN | 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** |
| INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES | |
| General | Y.4000–Y.4049 |
| Definitions and terminologies | Y.4050–Y.4099 |
| Requirements and use cases | Y.4100–Y.4249 |
| Infrastructure, connectivity and networks | Y.4250–Y.4399 |
| Frameworks, architectures and protocols | Y.4400–Y.4549 |
| Services, applications, computation and data processing | Y.4550–Y.4699 |
| Management, control and performance | Y.4700–Y.4799 |
| Identification and security | Y.4800–Y.4899 |

*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 | Unique ID[*] |
|---|---|---|---|---|
| 1.0 | ITU-T Y.3501 | 2013-05-22 | 13 | 11.1002/1000/11917 |
| 2.0 | ITU-T Y.3501 | 2016-06-13 | 13 | 11.1002/1000/12880 |

## Keywords

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

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## 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

Page

1 Scope ........ 1

2 References ........ 1

3 Definitions ........ 2

3.1 Terms defined elsewhere ........ 2

3.2 Terms defined in this Recommendation ........ 3

4 Abbreviations and acronyms ........ 4

5 Conventions ........ 4

6 General requirements for cloud computing ........ 5

7 General requirements for IaaS ........ 5

8 General requirements for NaaS ........ 6

9 General requirements for DaaS ........ 6

10 General requirements for PaaS ........ 7

11 General requirements for CaaS ........ 7

12 General requirements for BDaaS ........ 7

13 General requirements for inter-cloud computing ........ 8

14 General requirements for end-to-end cloud resource management ........ 8

15 General requirements for cloud infrastructure ........ 9

16 General requirements for trusted cloud services ........ 9

17 Security considerations ........ 10

Appendix I – Use cases of cloud computing ........ 11

I.1 Generic use case ........ 12

I.2 IaaS general use case ........ 13

I.3 NaaS general use case ........ 14

I.4 DaaS general use case ........ 15

I.5 PaaS general use case ........ 16

I.6 CaaS general use case ........ 17

I.7 BDaaS general use case ........ 19

I.8 Inter-cloud computing use case ........ 19

I.9 End-to-end cloud resource management use case ........ 21

I.10 Cloud infrastructure use case ........ 22

I.11 Trusted cloud service use case ........ 23

Appendix II – Methodology and edition plan of this Recommendation ........ 24

## Recommendation ITU-T Y.3501

# Cloud computing – Framework and high-level requirements

## 1 Scope

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

- Cloud computing;
- Infrastructure as a service (IaaS), network as a service (NaaS), desktop as a service (DaaS), platform as a service (PaaS), communication as a service (CaaS) and big data as a service (BDaaS);
- Inter-cloud computing, end-to-end cloud computing management, trusted cloud service, and cloud infrastructure.

This Recommendation addresses a set of use cases and related requirements which are included in Appendix I. Appendix II provides 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 X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*

[ITU-T Y.3503] Recommendation ITU-T Y.3503 (2013), *Requirements for desktop as a service.*

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements.*

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing.*

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service.*

[ITU-T Y.3513] Recommendation ITU-T Y.3513 (2014), *Cloud computing – Functional requirements of Infrastructure as a Service.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management.*

[ITU-T Y.3521] Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management.*

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – cloud computing based requirements and capabilities.*

# 3 Definitions

## 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 big data** [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

**3.1.2 big data as a service (BDaaS)** [ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

**3.1.3 cloud computing** [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

**3.1.4 cloud service** [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

**3.1.5 cloud service category** [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

**3.1.6 cloud service customer** [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

**3.1.7 cloud service partner** [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

**3.1.8 cloud service provider** [ITU-T Y.3500]: Party which makes cloud services available.

**3.1.9 cloud service user** [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

**3.1.10 communications as a service (CaaS)** [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

**3.1.11 desktop as a service (DaaS)** [ITU-T Y.3503]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute and deliver users' desktop functions remotely.

**3.1.12 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.

**3.1.13 infrastructure as a service (IaaS)** [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).

**3.1.14 infrastructure capabilities type** [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.

**3.1.15 inter-cloud computing** [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

**3.1.16 network as a service (NaaS)** [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

**3.1.17 party** [ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

**3.1.18 platform as a service (PaaS)** [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

**3.1.19 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.

**3.1.20 role** [ITU-T Y.3502]: A set of activities that serves a common purpose.

**3.1.21 service level agreement (SLA)** [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

**3.1.22 virtual desktop** [ITU-T Y.3503]: An environment for accessing end user's desktop functions remotely.

NOTE – Examples of end user's desktop functions can include desktop interface functions for applications, data access functions for multimedia data, and control functions for input/output (I/O) devices.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

**3.2.1 trusted cloud service**: A cloud service that satisfies a set of requirements such as transparency for governance, management and security so that a cloud service customer (CSC) can be confident in using the cloud service.

NOTE 1 – The set of requirements will vary depending on the involved cloud service customer, the nature of the cloud service and the governing jurisdiction.

NOTE 2 – The set of requirements could also be related to additional cross-cutting aspects [ITU-T Y.3502] such as performance, resiliency, reversibility, SLAs, etc.

NOTE 3 – Transparency means that the cloud service provider (CSP) should commit to the CSC that they have appropriate and clear control and reporting mechanisms for governance, management and security, such as SLA commitments, online announcements, data handling policies, etc.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| API | Application Programming Interface |
| BDaaS | Big Data as a Service |
| CaaS | Communication as a Service |
| CPU | Central Processing Unit |
| CSC | Cloud Service Customer |
| CSN | Cloud Service Partner |
| CSP | Cloud Service Provider |
| DaaS | Desktop as a Service |
| HD | High Definition |
| IaaS | Infrastructure as a Service |
| NaaS | Network as a Service |
| PaaS | Platform as a Service |
| PII | Personally Identifiable Information |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| SaaS | Software as a Service |
| SDK | Software Development Kit |
| 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.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its appendixes, 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 clause I.1 are as follows:

- **Service life-cycle management**: It is required that the cloud service provider (CSP) supports automated service provisioning, modification and termination during the service life-cycle;
- **Regulatory**: It is required that all applicable laws and regulations be respected, including those related to the protection of personally identifiable information (PII);
- **Security**: It is required that the cloud computing systems provided by the CSP be appropriately secured to protect the interests of all involved parties (e.g., persons and organizations);
- **Accounting and charging**: It is recommended that cloud service provided by the CSP supports various accounting and charging models and policies;
- **Efficient service deployment**: It is recommended that cloud service provided by the CSP enables efficient use of resources for service deployment;
- **Interoperability**: It is recommended that cloud service provided by the CSP complies with appropriate specifications and/or standards for allowing these systems to work together;
- **Portability**: It is recommended that cloud service provided by the CSP supports the portability of software assets and the data of cloud service customers (CSCs) with minimum disruption;
- **Service access**: The CSP 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 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 infrastructure as a service (IaaS) derived from the use cases in clause I.2 are as follows:

- **Configuration, deployment and maintenance of resources**: The IaaS CSP is recommended to configure, deploy and maintain processing, storage and/or networking resources with specific SLAs and charging models to CSCs;
- **Use and monitoring of resources**: The IaaS CSP is recommended to provide the capability for CSCs to use and monitor processing, storage and/or networking resources so that they are able to deploy and run arbitrary software.

NOTE – Functional requirements for IaaS are provided in [ITU-T Y.3513].

## 8 General requirements for NaaS

The general requirements for network as a service (NaaS) derived from the use cases in clause I.3 are as follows:

– **On-demand network configuration**: It is required that the NaaS CSP provides the network capability, which can be configured on demand by the CSC;

– **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 NaaS CSP supports network connectivity through heterogeneous networks.

NOTE – Functional requirements for NaaS are provided in [ITU-T Y.3512].

## 9 General requirements for DaaS

The general requirements for desktop as a service (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 central processing unit (CPU), memory, storage, network, etc.;

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

– **QoE**: 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 to get all DaaS functionality with appropriate security requirements through a single sign-on mechanism.

The following DaaS general requirements are described in [ITU-T Y.3503] as follows:

– **Support for high-definition (HD) and three-dimensional (3D) applications**: DaaS can optionally support execution of HD applications on virtual desktops for CSCs;

– **Extensible storage**: It is recommended that a CSP support the storage extension requested by a CSC;

– **Response time**: It is recommended that DaaS provide CSCs with acceptable QoE;

– **High availability**: It is recommended that high availability in terms of delivery and operation of DaaS be assured by a CSP;

– **Resiliency to disaster**: In the case of a disaster, DaaS is recommended to provide and maintain an acceptable level of service;

– **Service continuity**: It is recommended that in the case of temporarily unavailable resource access, a CSP provides the capability to preserve the state of the user session;

– **System scalability**: It is recommended that DaaS supports elastic scalability of:

  - Storage for DaaS user account information, virtual desktop environment settings and active and inactive virtual desktop environments;
  - Processing and network capacity for the number of concurrent DaaS user connections and total DaaS users;
  - Underlying DaaS resources.

– **DaaS developer environments**: It is recommended to provide a developer environment for the service and contents regarding DaaS;

- **Diversity of DaaS clients**: It is recommended that the CSP support a wide selection of DaaS clients.

NOTE – Functional requirements for DaaS are provided in clause 8 of [ITU-T Y.3503].

## 10 General requirements for PaaS

The general requirements for platform as a service (PaaS) derived from the use cases in clause I.5 are as follows:

- **Application hosting**: It is required that the PaaS CSP provides an application hosting environment, where the application can be rapidly deployed, reliably executed, flexibly expanded and isolated from other applications;
- **Services delivery platform**: It is recommended that the PaaS CSP provides the capabilities of service presence, orchestration, billing, mash-up and tools for associated development and testing by CSCs through a unified application programming interface (API);
- **Integrated development environment**: The PaaS CSP can optionally provide comprehensive capabilities to CSCs for software development such as coding, debugging, compiling and distribution;
- **Development tools**: PaaS CSP can optionally provide development tools as a service to CSCs, who can use it on-demand.

## 11 General requirements for CaaS

The general requirements for communication as a service (CaaS) derived from the use cases in clause I.6 are as follows:

- **Communication capabilities openness**: It is recommended that the CSP provides APIs for accessing communication capabilities of CSNs to enhance their own services by using communication enablers;
- **Communication software development support**: It is recommended that the CSP provides support for communication software development, which is a group of communication building blocks, to CSNs in order to develop communication applications;

  NOTE – Examples of communication building blocks are protocol stacks, codecs, authentication, etc.
- **Unified communication**: It is recommended that the CSP provides to CSCs a consistent unified user interface and user experience of communications applications, such as voice, messaging, audio, video conferencing, etc., across multiple devices and media-types.

## 12 General requirements for BDaaS

The general requirements for big data as a service (BDaaS) derived from the use cases in clause I.7 are as follows:

- **Resource clustering**: It is recommended for the CSP to cluster resources for processing of extensive data;

  NOTE 1 – Resources includes processing, storage and networks, etc.
- **Data collection**: It is recommended for the BDaaS CSP to collect data from CSCs, CSNs and CSPs;

  NOTE 2 – Data includes various types, different formats, real time streaming/static data and CSC data including users' behaviour data.
- **Data storing**: It is recommended for the BDaaS CSP to store data with sufficient storage and fulfil performance demands;

- **Data analysing**: It is recommended for the BDaaS CSP to analyse data with various kinds of analysis algorithms;

  NOTE 3 – Data analysis algorithms include classification, clustering, regression, association, ranking, etc.

- **Data visualizing**: It is recommended for the BDaaS CSP to provide reporting tools with multiple styles of data visualization;

  NOTE 4 – Visualization styles include statistical graphics, forms, diagrams, charts, etc.

- **Data managing**: It is recommended for the BDaaS CSP to support management of data lifecycle and resources monitoring.

  NOTE 5 – Functional requirements for BDaaS are provided in clause 8 of [ITU-T Y.3600].

## 13 General requirements for inter-cloud computing

The general requirements for inter-cloud computing derived from the use cases in clause I.8 are as follows:

- **On-demand assignment of cloud computing resources among CSPs**: For assigning cloud computing 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 an 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 changes in the cloud service user environment, 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 1 – These actions are to be performed for all cloud service users.

- **Inter-cloud service intermediation**: Inter-cloud service intermediation enables the CSP to select the most suitable cloud services and to create new cloud services by integrating cloud services offered by other CSPs. It is recommended that the CSP engages in support of intermediation for multiple cloud services of various cloud service categories such as IaaS, NaaS, PaaS and SaaS;
- **Large-scale migration**: A CSP in an inter-cloud federation is recommended to be able to guarantee continuity of all the cloud services in the 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 cloud services when migrating.

  NOTE 2 – For more information on functional requirements for inter-cloud computing, see clause 9 of [ITU-T Y.3511].

## 14 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 clause I.9 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 the cloud computing systems used for providing cloud services 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 service providers, requiring the need for multi-cloud, end-to-end management data.

NOTE – For more information on end-to-end cloud computing management, refer to [ITU-T Y.3520] and [ITU-T Y.3521].

## 15 General requirements for cloud infrastructure

The general requirements for cloud infrastructure derived from the use cases in clause I.10 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 processing, storage and network resources to cloud services and supporting functions.

NOTE – Functional requirements for cloud computing infrastructure are provided in [ITU-T Y.3510].

## 16 General requirements for trusted cloud services

The general requirements for trusted cloud services are derived from the use case in clause I.11. The following requirements are important for CSCs in order to be able to select a trusted cloud service. These requirements do not specify the levels and abilities of the cloud services, but require that the cloud services which are treated as trusted cloud services should satisfy the following:

– **Governance for trusted cloud service**: It is recommended for trusted cloud services to comply with appropriate or local standards and best practices of corporate governance and include appropriate mechanisms by which policies affecting the provision and use of cloud services are directed and controlled;

NOTE 1 – Part of this requirement refers to [ITU-T Y.3502].

– **Management for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for administration, reporting, location of stored data, privacy, de-identification of data, etc.

– **Resiliency for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms by which an acceptable level of service can be maintained in the face of faults (unintentional, intentional or naturally caused) affecting normal operation;

NOTE 2 – Part of this requirement refers to [ITU-T Y.3502].

– **Security for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for cryptography, attack resistance, intrusion detection, security incident handling and reporting, etc.

NOTE 3 – Part of this requirement refers to [ITU-T X.1601].

– **Availability for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for ensuring the appropriate level of access to the service and usability by the CSC;

– **Auditability for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for collecting and making available necessary evidential information related to the operation and use of a cloud service, for the purpose of conducting an audit;

NOTE 4 – Part of this requirement refers to [ITU-T Y.3502].

- **Service agreement for trusted cloud service**: It is recommended for trusted cloud services to have appropriate service agreements or contracts for commitments to CSC on terms of their requirements and considerations.

## 17 Security considerations

The security framework from cloud computing [ITU-T X.1601], analyses security threats and challenges in the cloud computing environment, describes security capabilities that could mitigate these threats and addresses security challenges.

[ITU-T X.1631] provides guidelines supporting the implementation of information security controls for CSCs and CSPs. Many of the guidelines guide the CSPs to assist the CSCs in implementing the controls and guide the CSCs to implement such controls. Selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment as well as any legal, contractual, regulatory or other cloud-sector specific information security requirements.

Regarding the protection of PII, ISO/IEC 27018 is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for organizations for implementing commonly accepted PII protection controls.

# 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. Table I.1 shows the template used for the description of the use cases.

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

| **Use case** | |
|---|---|
| **Name** | Title of the use case |
| **Abstract** | Overview and features of the use case |
| **Roles** | Roles relating to/appearing in the use case |
| **Figure** | Figure to present the use case.<br>(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.<br>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 for pre-conditions, 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:<br>– Large-scale migration |

Table I.2 lists the use cases described in this appendix.

**Table I.2 – List of use cases**

| **Domains** | **Use cases** |
|---|---|
| **Generic use case** | – General CSC-CSP-CSN use case<br>– Use case publish service<br>– Use case consult service<br>– Use case use service |
| **IaaS** | – IaaS general use case |
| **NaaS** | – NaaS general use case |
| **DaaS** | – DaaS general use case |
| **PaaS** | – PaaS general use case |
| **CaaS** | – CaaS general use case |
| **BDaaS** | – BDaaS general use case |
| **Inter-cloud computing** | – Inter-cloud computing use case for federation<br>– Inter-cloud computing use case for intermediation |
| **Cloud resource management** | – End-to-end cloud resource management use case |
| **Cloud infrastructure** | – Cloud infrastructure use case |
| **Trusted cloud service** | – Trusted cloud service 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)<br>– UC-CS (Use case consult service)<br>– UC-PS (Use case publish service) |

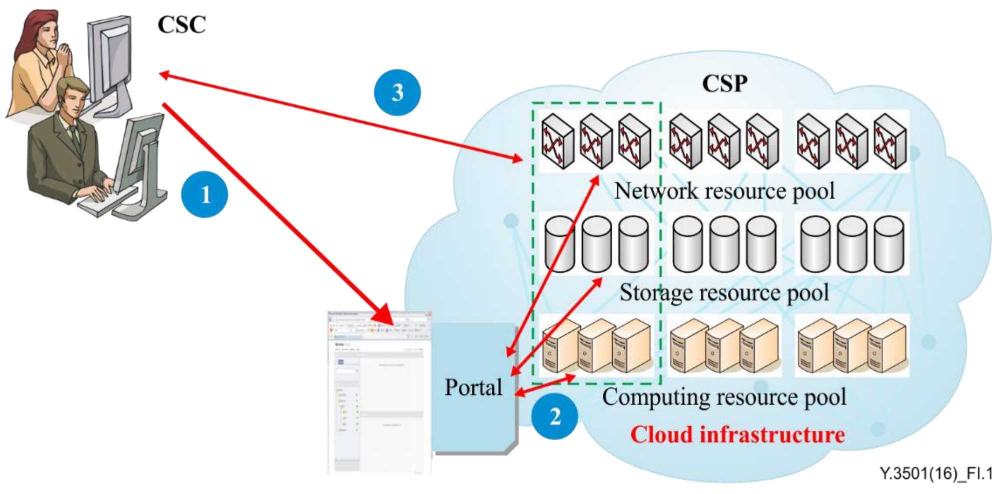
| Use case | |
|---|---|
| **Name** | Use case publish service |
| **Abstract** | A CSP publishes cloud service information to the public so that any users including a CSP, CSC or CSN can use the published cloud service. In terms of service publishing, the CSP adds the service to a service catalogue which will be accessible to 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<br>– Security<br>– Efficient service deployment<br>– Portability<br>– Regulatory aspects<br>– Service availability, service reliability and quality assurance<br>– Service access<br>– 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).<br>– The CSC, CSP or CSN has been authenticated. |
| **Post-conditions (optional)** | – A given service should be accessible. |
| **Requirements** | – Security<br>– Service availability, service reliability and quality assurance |

| Use case | |
|---|---|
| | – Service access<br>– Interoperability<br>– Regulatory aspects<br>– Accounting and charging |

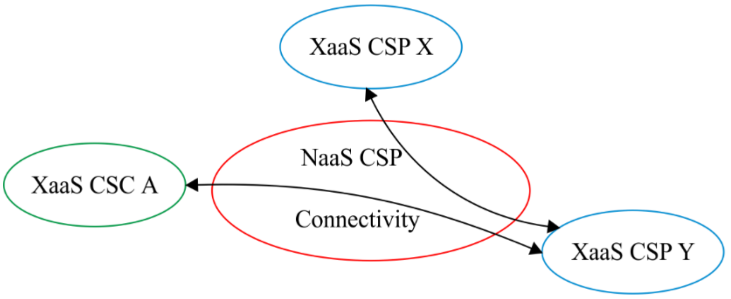
| Use case | |
|---|---|
| **Name** | Use case use service |
| **Abstract** | A CSC or a CSN uses a published service. According to the agreement of the SLA, the user invokes the cloud service. |
| **Actors** | CSC, CSN |
| **Pre-conditions (optional)** | – The service to be used has already been published by a CSP (UC-PS).<br>– The CSC or the CSN has been authenticated. |
| **Post-conditions (optional)** | – The used service should be kept available during the whole invocation.<br>– The SLA should be met for service use. |
| **Requirements** | – Service life-cycle management<br>– Security<br>– Portability<br>– Interoperability<br>– Regulatory aspects<br>– Service availability, service reliability and quality assurance<br>– Service access<br>– 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** |  CSC<br>CSP<br>3<br>1<br>2<br>Network resource pool<br>Storage resource pool<br>Computing resource pool<br>Portal<br>Cloud infrastructure<br>Y.3501(16)_FI.1 |
| **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.<br>– 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.<br>– 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.<br>– 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.<br>– ③ The CSP configures, deploys and maintains hypervisors and storage resources.<br>– ③ The CSP establishes, configures, delivers and maintains network connectivity to the CSC.<br>– ③ The CSP provides security infrastructure to the CSC. |
| **Requirements** | – Configuration, deployment and maintenance of resources<br>– Use and monitoring of resources |

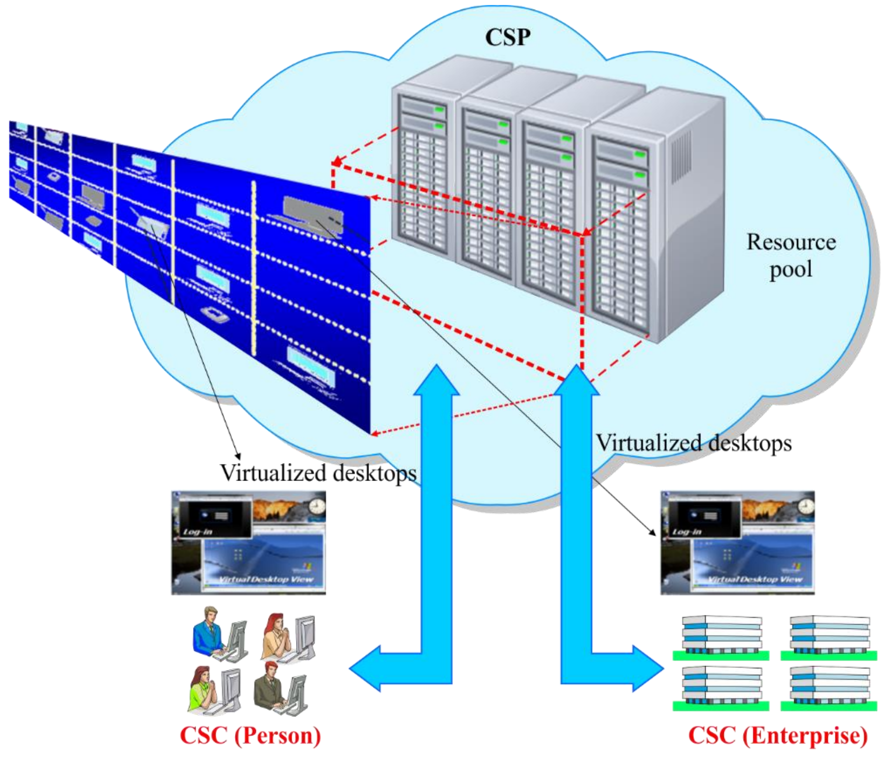
## I.3 NaaS general use case

| **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** |   XaaS CSP X<br>NaaS CSP<br>XaaS CSC A<br>Connectivity<br>XaaS CSP Y Y.3501(16)_FI.2 |
| **Pre-conditions (optional)** | – There is no connectivity between XaaS CSC A and XaaS CSP Y.<br>– There is no connectivity between XaaS CSP X and XaaS CSP Y.<br>– 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.<br>– 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.<br>– XaaS CSC X and XaaS CSP Y can communicate with each other. |
| **Requirements** | – On-demand network configuration |

| Use case | |
|---|---|
| | – Heterogeneous networks compatibility<br>– QoS-guaranteed connectivity<br>– Secured connectivity |

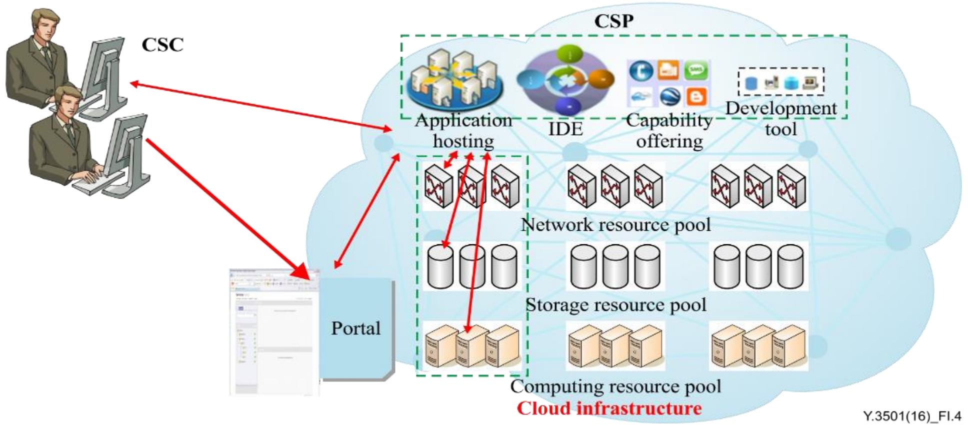
## I.4 DaaS general use case

| 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.<br>– 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.<br>– 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 |

| Use case | |
|---|---|
| **Figure** |  CSP<br>Resource pool<br>Virtualized desktops<br>Virtualized desktops<br>Log-in<br>Virtual Desktop View<br>Log-in<br>Virtual Desktop View<br>CSC (Person)<br>CSC (Enterprise)<br>Y.3501(16)_FI.3 |
| **Pre-conditions (optional)** | – A CSP offers the configuration menu of the virtual desktop to CSCs.<br>– A CSC specifies parameter-settings shown in the configuration menu. |
| **Post-conditions (optional)** | – A CSC uses DaaS service. |
| **Requirements** | – QoE<br>– Fast boot-up time<br>– Configurability of the virtual environment<br>– Single sign-on access control<br>– Support for high-definition (HD) and three dimensional (3D) applications<br>– Extensible storage<br>– Response time<br>– High availability<br>– Resiliency to disaster<br>– Service continuity<br>– System scalability<br>– DaaS developer environments<br>– Diversity of DaaS client |

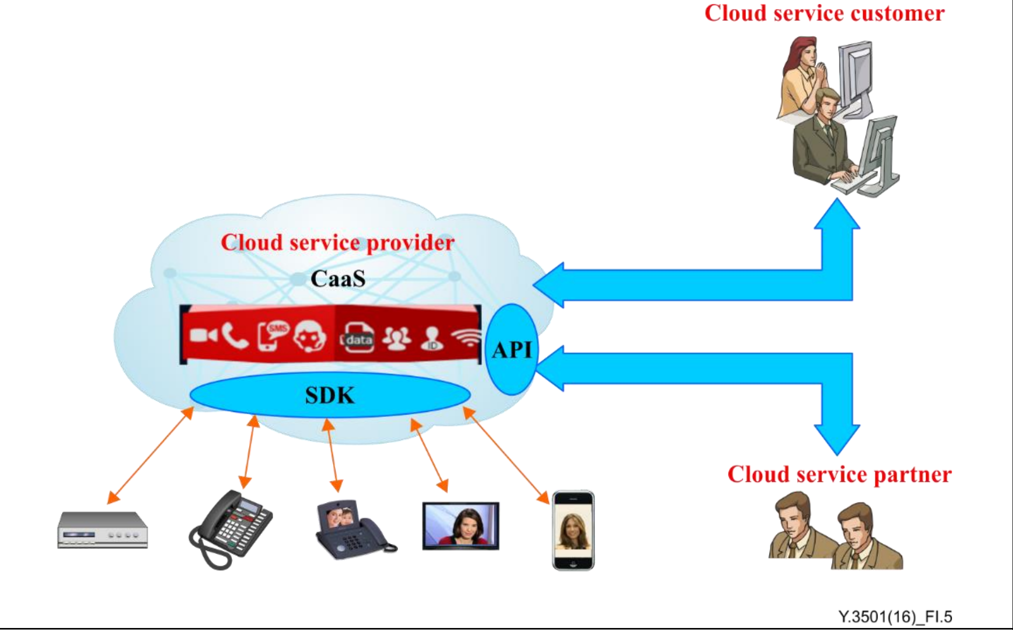
## I.5 PaaS general use case

| Use case | |
|---|---|
| **Name** | PaaS general use case |
| **Abstract** | A PaaS CSP provides application hosting, capabilities offering, integrated development environment and development tools to CSC. |
| **Roles** | CSC, CSP |

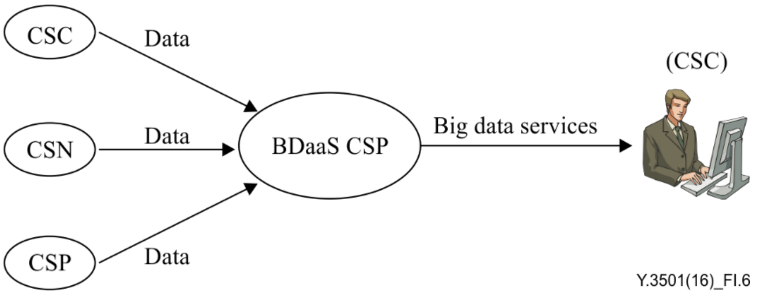
| Use case | |
|---|---|
| **Figure** |  CSC<br>CSP<br>Application hosting<br>IDE<br>Capability offering<br>Development tool<br>Network resource pool<br>Storage resource pool<br>Computing resource pool<br>Cloud infrastructure<br>Portal<br>Y.3501(16)_FI.4 |
| **Pre-conditions (optional)** | – CSC requests PaaS service from CSP1 to develop an application.<br>– CSP1 provides a cloud-based integrated development environment to CSC as well as some development tools.<br>– CSC requests PaaS service from CSP2 to use a service delivery platform provided by CSP.<br>– CSP2 provides service presence, orchestration, billing, mash-up and associated development and testing tools.<br>– CSC requests PaaS service from CSP3 to an application hosting environment provided by CSP.<br>– CSP3 provides application hosting service to CSC to deploy and execute the application. |
| **Post-conditions (optional)** | – CSC develops an application using an integrated development environment to be more productive by reducing the configuration necessary to piece together multiple development utilities and setup time.<br>– CSC uses development tools without deploy and maintain.<br>– CSC uses capabilities sets, such as location and SMS to develop an application.<br>– CSC deploys and runs an application on the application hosting environment without concerning the underlying resources. |
| **Requirements** | – Application hosting<br>– Services delivery platform<br>– Integrated development environment<br>– Development tools |

## I.6 CaaS general use case

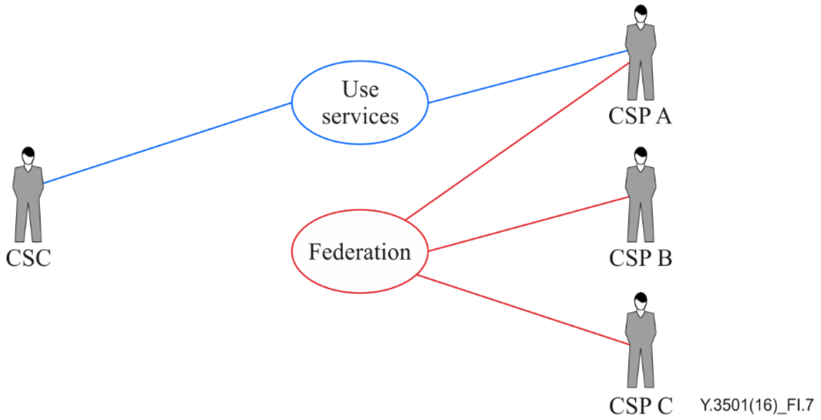
| Use case | |
|---|---|
| **Name** | CaaS general use case |
| **Abstract** | A CaaS CSP provides API and/or software development support such as a software development kit (SDK) to enable building of a communication platform and services by a CSN, or in addition to build communication services offered to CSC directly by CaaS CSP. This involves both platform capabilities type and application capabilities type. |
| **Roles** | CSC, CSP,CSN |

| Use case | |
|---|---|
| **Figure** | <br> Cloud service customer<br>Cloud service provider<br>CaaS<br>SMS<br>data<br>ID<br>API<br>SDK<br>Cloud service partner<br>Y.3501(16)_FI.5 |
| **Pre-conditions (optional)** | With platform capabilities type:<br>– CSN wants to develop some product or service, using communication features such as video call capability. For example, a non-cloud video game developer could include CaaS-based voice and video calling between players of their game.<br>– CSP provides carrier-grade video call capabilities to a CSN through CaaS API.<br>– CSN wants to enhance a device (such as an IP-connected camera) with a remote control feature, while the original device only has connectivity capabilities but no communication capabilities.<br>– CSP provides the SDK to a CSN, in this case, the CSN can add communication capabilities to the device.<br>With application capabilities type:<br>– CSC wants to use communication applications on different kinds of devices, such as wire-line telephone, mobile phone, IMS device, tablet and PC. |
| **Post-conditions (optional)** | With platform capabilities type:<br>– CSN develops a product or service with carrier-grade video call capabilities provided by the CaaS CSP.<br>– CSC can call the device and control it remotely by using SDK provided by the CSP.<br>With application capabilities type:<br>– CSC can access all kinds of communications applications with consistent unified user-interface and user-experience over multiple devices, such as wire-line telephone, mobile phone, IMS device, tablet and PC. |
| **Requirements** | – Communication capabilities openness<br>– Communication software development support<br>– Unified communication |

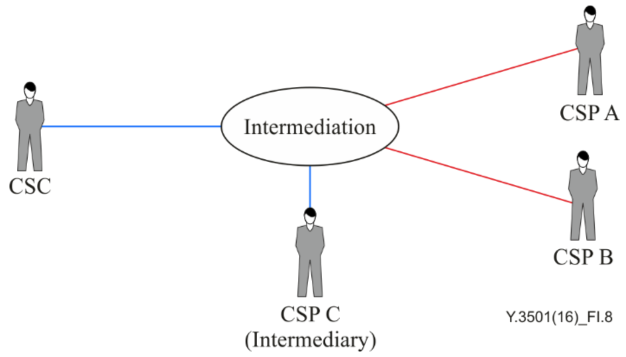
## I.7 BDaaS general use case

| Use case | |
|---|---|
| **Name** | BDaaS general use case |
| **Abstract** | A BDaaS CSP provides big data services through cloud computing. The BDaaS CSP uses the cloud computing capabilities to implement various big data capabilities such as collecting data, managing data storage, managing data privacy, managing data pre-processing, providing data integration, managing data provenance, analyzing data and visualizing data. |
| **Roles** | CSC, CSP, CSN |
| **Figure** |   CSC<br>Data<br>CSN<br>Data<br>CSP<br>Data<br>BDaaS CSP<br>Big data services<br>(CSC)<br>Y.3501(16)_FI.6 |
| **Pre-conditions (optional)** | – The CSN provides appropriate access methods of data to the BDaaS CSP. |
| **Post-conditions (optional)** | |
| **Requirements** | – Resource clustering<br>– Data collection<br>– Data storing<br>– Data analysing<br>– Data visualizing<br>– Data managing |

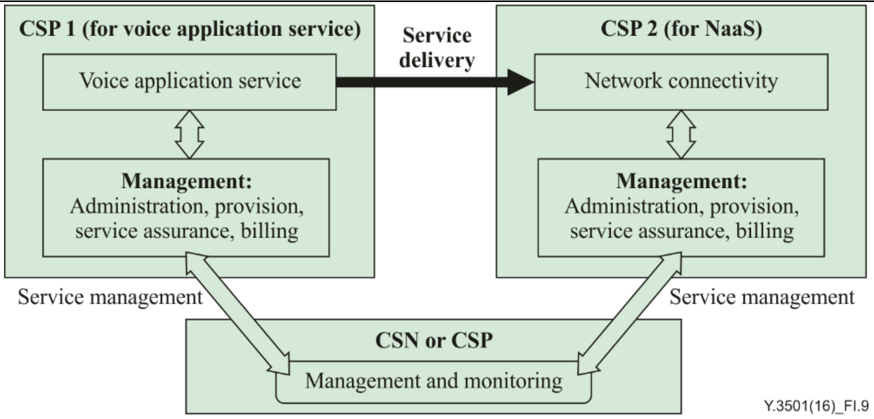
## I.8 Inter-cloud computing use case

| Use case | |
|---|---|
| **Name** | Inter-cloud computing use case for federation |
| **Abstract** | CSPs federate to provide a service to the CSC |
| **Roles** | CSC, CSP |
| **Figure** |   Use services<br>CSC<br>Federation<br>CSP A<br>CSP B<br>CSP C<br>Y.3501(16)_FI.7 |

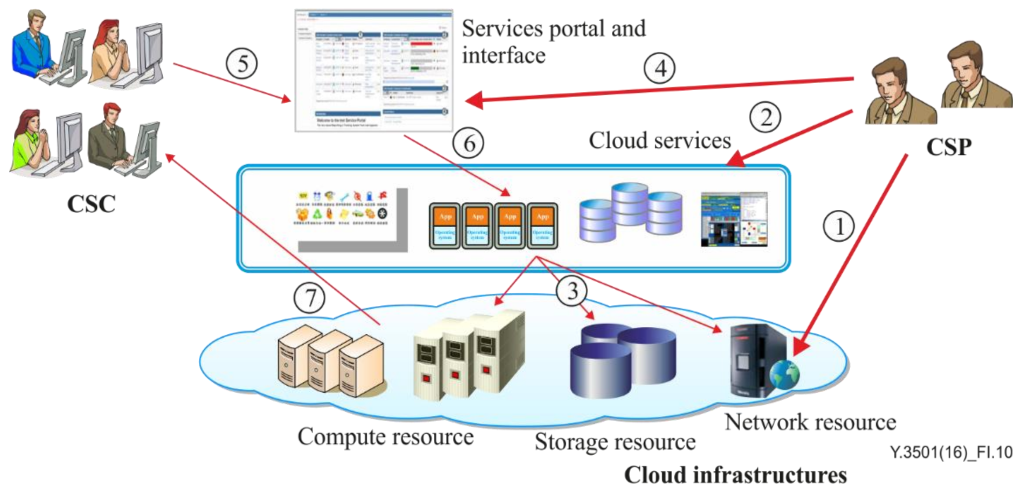
| Use case | |
|---|---|
| **Pre-conditions (optional)** | – CSPs federate with each other by establishing a trust relationship and policy settlement.<br>– A CSC uses a service provided by one of the federated CSPs.<br>– Case-A: The CSP that offers the service to the CSC is going to spend all resources due to overload, or has lost the resources due to disaster.<br>– 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).<br>– 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<br>– Resource and load distribution<br>– Large-scale migration<br>– User environment adaptation |

| Use case | |
|---|---|
| **Name** | Inter-cloud computing use case for intermediation |
| **Abstract** | A CSP intermediates services from other CSPs to provide a service to the CSC. |
| **Actors** | CSP, CSC |
| **Figure** |   Intermediation<br>CSC<br>CSP A<br>CSP B<br>CSP C<br>(Intermediary)<br>Y.3501(16)_FI.8 |
| **Pre-conditions (optional)** | |
| **Post-conditions** | – A CSP selects a service from other CSPs' services and intermediates them to a CSC.<br>– 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<br>– Inter-cloud computing service intermediation |

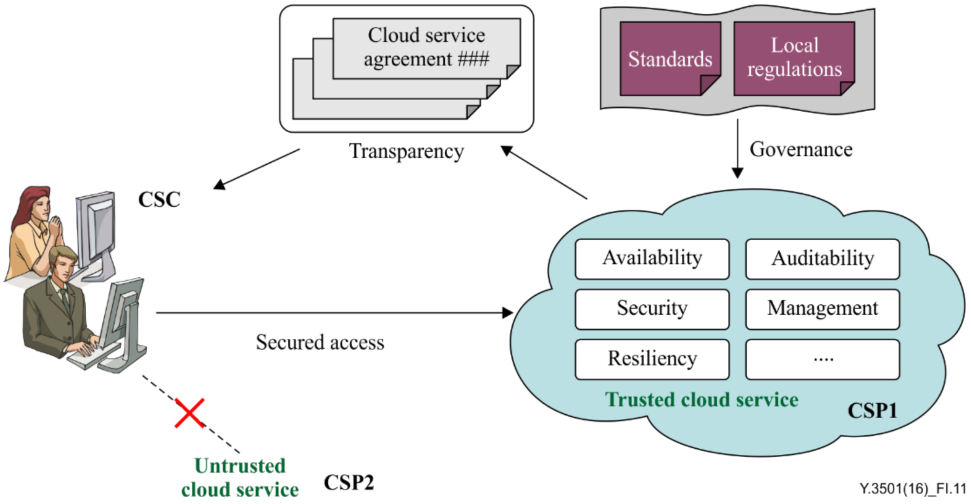
### I.9 End-to-end cloud resource management use case

| 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 |
| **Figure** |   CSP 1 (for voice application service)<br>Voice application service<br>Management:<br>Administration, provision, service assurance, billing<br>Service delivery<br>CSP 2 (for NaaS)<br>Network connectivity<br>Management:<br>Administration, provision, service assurance, billing<br>Service management<br>Service management<br>CSN or CSP<br>Management and monitoring<br>Y.3501(16)_FI.9<br>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.<br>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.<br>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.<br>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<br>– Manageability for multiple cloud services |

## I.10 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 kinds of cloud services.<br>The CSC accesses and uses cloud services deployed in and delivered by cloud infrastructure. |
| **Roles** | CSC, CSP |
| **Figure** |  Services portal and interface<br>⑤<br>④<br>②<br>CSP<br>CSC<br>⑥<br>Cloud services<br>①<br>⑦<br>③<br>Compute resource<br>Storage resource<br>Network resource<br>Cloud infrastructures<br>Y.3501(16)_FI.10 |
| **Pre-conditions (optional)** | – ① A CSP builds a cloud infrastructure with cloud resources including compute, storage and network resources.<br>– 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.<br>– ④ The CSP publishes the deployed cloud services in the catalogue of the cloud service portal.<br>– ⑤ A CSC accesses the cloud services published by the CSP through service portals or service interfaces which are protected by appropriate security mechanisms.<br>– 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<br>– Resource abstraction and control |

## I.11 Trusted cloud service use case

| Use case | |
|---|---|
| **Name** | Trusted cloud service use case |
| **Abstract** | The CSP provides trusted cloud service which satisfies a set of requirements and transparency for governance, management and security to provide CSC confidence in using the cloud service. |
| **Roles** | CSC, CSP |
| **Figure** |   Cloud service agreement ###<br>Standards<br>Local regulations<br>Transparency<br>Governance<br>CSC<br>Availability<br>Auditability<br>Security<br>Management<br>Resiliency<br>....<br>Trusted cloud service<br>CSP1<br>Secured access<br>Untrusted cloud service<br>CSP2<br>Y.3501(16)_FI.11 |
| **Pre-conditions (optional)** | – The CSC requests a trusted cloud service:<br>• The CSP1 offers the same cloud services as CSP2, but CSP2 does not meet trusted cloud service requirements.<br>• The CSC gets effective cloud service information from CSP1.<br>• The CSC does not have effective cloud service information from CSP2.<br>– The CSP1 negotiates a cloud service agreement with the CSC before providing a cloud service, while CSP2 does not. |
| **Post-conditions (optional)** | – The CSP 1 provides a trusted cloud service which meets the needs of the CSC.<br>– The CSP 1 ensures PII protection of the CSC.<br>– The CSP 1 ensures that the CSC can control and manage their application and data.<br>– The CSP 1 provides a secure access to the CSC.<br>– The CSC uses the trusted cloud service from CSP 1.<br>– The CSC no longer uses the cloud service from CSP 2. |
| **Requirements** | – Governance for trusted cloud service<br>– Management for trusted cloud service<br>– Resiliency for trusted cloud service<br>– Availability for trusted cloud service<br>– Auditability for trusted cloud service<br>– Security<br>– Service agreement for trusted cloud service. |

# 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 Figure II.1, one use case may derive multiple requirements.

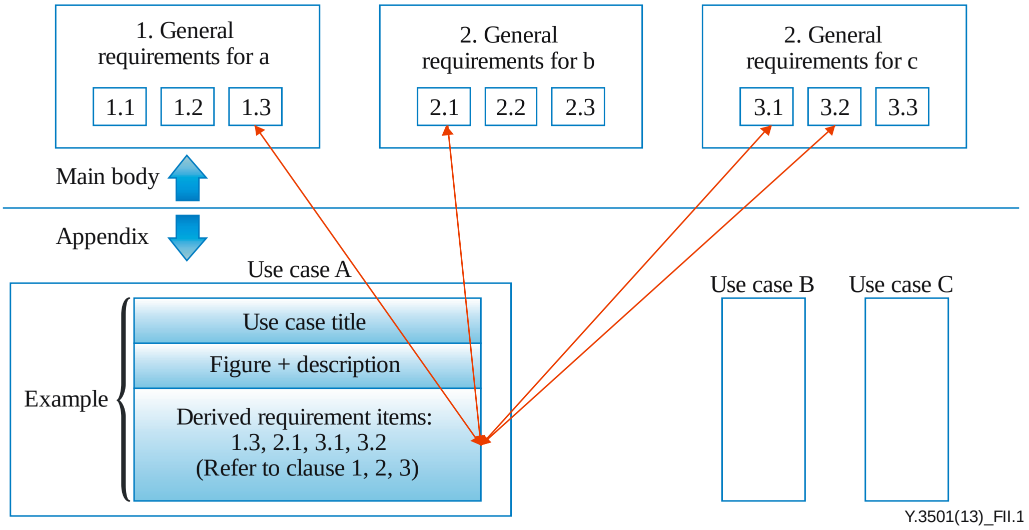
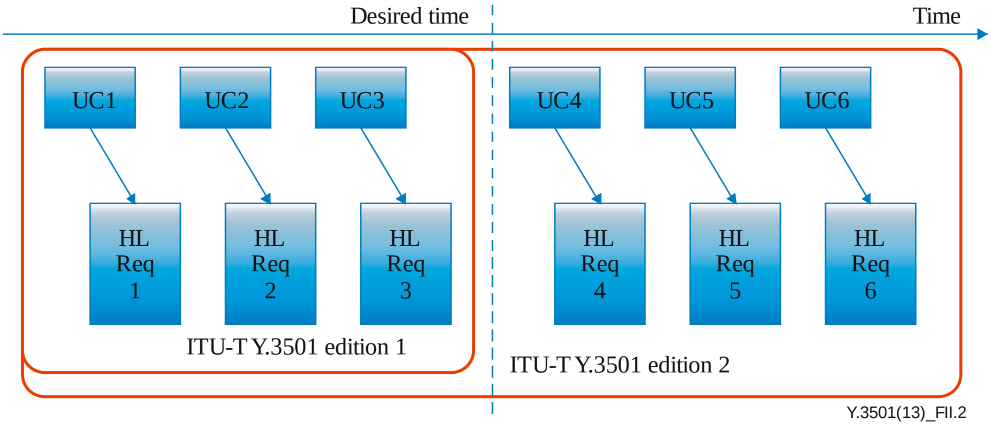


**Figure II.1 – Methodology including mapping of use cases and requirements**

The use-case-driven approach may also ease the preparation of future editions of this Recommendation. As explained in Figure II.2, 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.

Table II.1 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 | Edition3 |
|---|---|---|---|---|
| General requirements for cloud computing | | O | Extended | Extended |
| General requirements for IaaS | | O | Extended | Extended |
| General requirements for NaaS | | O | Extended | Extended |
| General requirements for DaaS | | O | Extended | Extended |
| General requirements for PaaS | | | O | Extended |
| General requirements for CaaS | | | O | Extended |
| General requirements for BDaaS | | | O | Extended |
| General requirements for SaaS | | | | O |
| General requirements for Inter-cloud | | O | Extended | Extended |
| General requirements for end-to-end cloud resource management | | O | Extended | Extended |
| General requirements for cloud infrastructure | | O | Extended | Extended |
| General requirements for Trusted cloud service | | | O | Extended |
| Others general requirements | | | | O |
| Security consideration | | O | Extended | Extended |
| Use case | Generic use cases | O | Extended | Extended |
| | IaaS general use case | O | Extended | Extended |
| | NaaS general use case | O | Extended | Extended |
| | DaaS general use case | O | Extended | Extended |
| | PaaS general use case | | O | Extended |
| | CaaS general use case | | O | Extended |
| | BDaaS use case | | O | Extended |
| | SaaS general use case | | | O |
| | Inter-cloud general use case | O | Extended | Extended |
| | End-to-end cloud resource management use case | O | Extended | Extended |
| | Cloud infrastructure use case | O | Extended | Extended |
| | Trusted cloud service 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. | | | | |

## 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 | Environment and ICTs, climate change, e-waste, energy efficiency; 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, Internet of Things and smart cities** |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2016