International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3522

(09/2016)

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

Cloud Computing

End-to-end cloud service lifecycle management requirements

Recommendation ITU-T Y.3522

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
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3522

End-to-end cloud service lifecycle management requirements

Summary

Recommendation ITU-T Y.3522 provides an overview of end-to-end (E2E) cloud service lifecycle management by specifying cloud service lifecycle metadata, the cloud service lifecycle management framework, cloud service lifecycle management stages and the relationship with cloud computing reference architecture. This Recommendation also provides E2E cloud service lifecycle management functional requirements derived from the corresponding typical use cases.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3522	2016-09-29	13	11.1002/1000/13020

Keywords

Cloud service lifecycle management, end-to-end, functional requirements, metadata, model, stage.

* 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

Recommendation ITU-T Y.3522

End-to-end cloud service lifecycle management requirements

1 Scope

This Recommendation specifies the functional requirements of end-to-end (E2E) cloud service lifecycle management. This Recommendation comprises the following:

– cloud service lifecycle metadata;

– cloud service lifecycle management framework;

– cloud service lifecycle management stages;

– relationship with cloud computing reference architecture;

– functional requirements and typical use cases of cloud service lifecycle management.

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 M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications Markup Language (tML) framework.*

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

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

[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.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

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

3.1.3 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.

3.1.4 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.

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

3.1.6 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.

3.1.7 metadata [ITU-T M.3030]: Data that describes other data.

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

3.1.9 product catalogue [ITU-T Y.3502]: A listing of all the cloud service products which cloud service providers make available to cloud service customers.

3.1.10 service catalogue [ITU-T Y.3502]: A listing of all the cloud services of a particular cloud service provider.

3.1.11 service management interface (SMI) [ITU T Y.3521]: Interface that provides a set of management capabilities exposed by a cloud service through which the cloud service can be managed.

NOTE – For additional details of SMI concepts, see [ITU T Y.3520] and [b-TMF TR198].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 functional interface: Interface that provides a set of functional capabilities exposed by a cloud service through which the cloud service can be consumed.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

CSU Cloud Service User

CT Communications Technology

E2E End-to-End

FI Functional Interface

IT Information Technology

OSS Operational Support Systems

QoS Quality of Service

SMI Service Management Interface

WSDL Web Services Description Language

5 Conventions

The keywords "**is required to**" 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 Recommendation 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.

6 Overview of E2E cloud service lifecycle management

Nowadays, cloud computing technologies are widely used in both information technology (IT) and communications technology (CT) industries. Telecommunication operators use cloud-based technologies to deliver cloud services to their users as well as to leverage their telecommunication services and network. This allows for automation and acceleration provisioning of cloud services across cloud and non-cloud facilities. Therefore, effective cloud service lifecycle management becomes one of the most important challenges from telecommunication operators' perspectives.

Cloud service lifecycle management integrates and optimizes processes such as service provisioning, service assurance, service fulfilment, service charging and service change management for particular workloads respecting relevant governance and polices.

In both telecommunication and cloud computing environments, cloud service lifecycle management has to be considered in an E2E manner which means service lifecycle management chains across cloud and non-cloud facilities. In practice, cloud service lifecycle management could be achieved by using a service management interface (SMI) based common model for E2E cloud computing management supported by operational support systems (OSS), see [ITU-T Y.3521].

The OSS encompass the set of operational related management capabilities, including service catalogue, provisioning, monitoring and reporting, service policy management, service automation, etc., in order to manage and control cloud services offered to cloud service customers (CSCs), see [ITU-T Y.3502]. OSS realize the required E2E cloud service lifecycle management functionalities by using service management interfaces (SMIs). These operational related management capabilities can help to achieve the service lifecycle management objective with the pre-defined distributed metadata in each stage.

The consistent approach to service lifecycle management includes representative definitions for the particular stages which cloud services pass through. This is based on a lifecycle management metadata model, which can hold all the data about a service throughout its lifecycle.

Cloud service lifecycle management consists of three parts:

1) service dependencies management: represents resources that are prerequisites for the service to function;
2) service lifecycle management stages: represents stages through which cloud service passes over lifecycle management;
3) additional information about the service management interface: placeholder for additional information but otherwise undefined.

The development of an E2E cloud service lifecycle management process is based on the following elements interacting with each other:

1) service catalogue, see [ITU-T Y.3502], [ITU-T Y.3521];

2) service inventory, see [ITU-T Y.3521];

3) SMI, see [ITU-T Y.3521].

6.1 Cloud service lifecycle metadata

The cloud service capabilities are exposed and consumed through the functional interfaces (FIs) of the service while the management or operations of the service are available through the SMI.

The cloud service capabilities may participate/contribute in many different product offerings that are delivered to CSCs. They may also have different configuration constraints and policies due to constraints from distinct implementation technologies and CSCs' devices that the service is delivered through. These complicated re-design, re-configuration and re-deployment problems can be addressed through the cloud service lifecycle metadata, which represents all of the lifecycle aspects of the virtualized elements, as expressed in the form of logical objects within a defined model space.

The alignment between elements in the defined model and the real world can be achieved by tools which can address service dependency and drive the required actions based on the metadata associated with the modelled elements. This approach allows a new service to be created with changes only in metadata and minimal modifications. Therefore, the lifecycle metadata can be regarded as the linkage between design time and execution time. From the point of view of cloud service developers (see [ITU-T Y.3502]), FIs and SMIs may only be described in common service languages such as web services description language (WSDL) or web service implementation environment. The aim of this is to define the SMI operations that all services can understand. Therefore, cloud service lifecycle metadata can be designed to capture the cloud service dependencies and service properties to support multi-cloud management.

In order to support consistent management, business process automation and CSC experience, cloud services should understand a set of operations requirements. The word "understand" means that, for example if there is a request for a SMI to configure a service, then the SMI may:

1) intelligently perform the steps required to configure the service per its operation environment, or

2) transfer the request to other applications/services to perform the request, or

3) simply return to the management application that there is no operation or capability to support this function.

Therefore the cloud service compatibility can be provided in any of the following forms:

1) new service component that is implemented by supporting the SMI specification and metadata to be defined;

2) cloud service wrapper on existing service components;

3) cloud service proxy where it transfers the actual operation tasks to other application/service components.

6.2 Cloud service lifecycle management framework

E2E cloud computing management is the capability to manage services and resources (addressing fulfilment, assurance and repositories) of single or multiple cloud services spanning across one or more cloud service providers (CSPs), see [ITU-T Y.3521]. The common model for E2E cloud computing management is based on SMIs. The SMI based approach provides a means to allow consistent E2E management of cloud computing services exposed by and across, different domains of CSPs. Figure 6-1 depicts a conceptual framework of E2E cloud service lifecycle management.

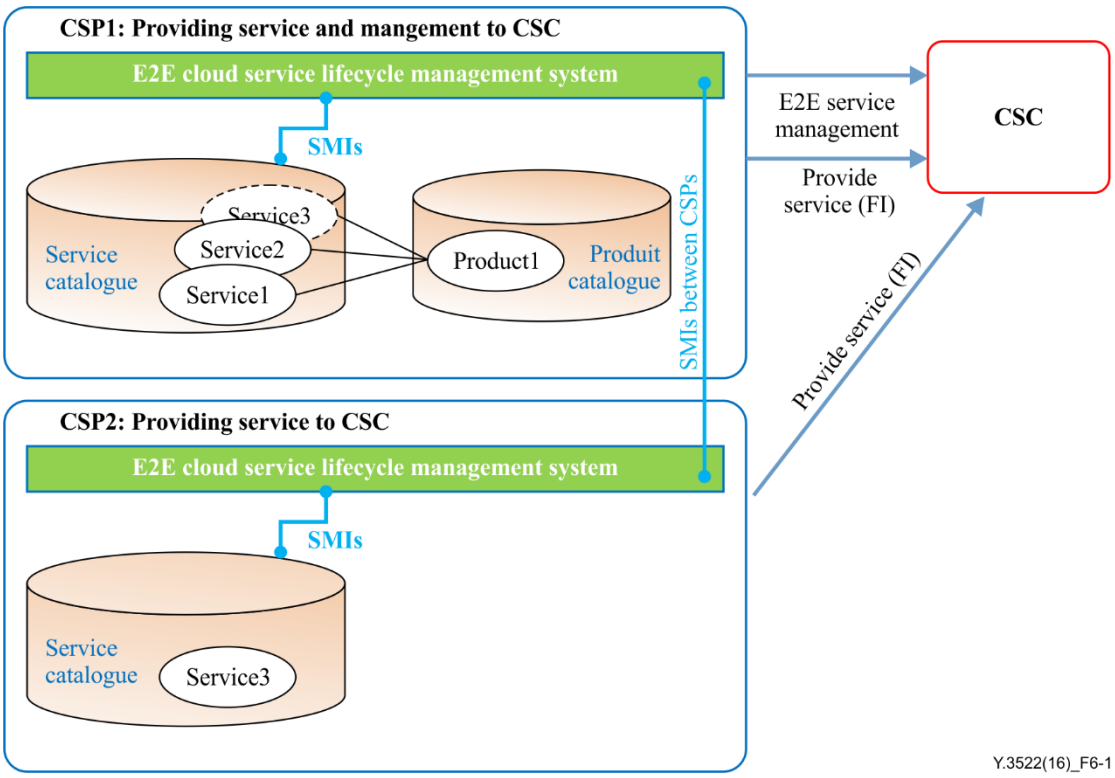


Figure 6-1 – E2E cloud service lifecycle management framework

As the Figure 6-1 shows, the E2E cloud service lifecycle management system interacts with CSC and other E2E cloud service lifecycle management systems as follows:

1) CSC can take an action (function) to search for a product (see "Product1" in Figure 6-1) in a self-service fashion (see clause 7.2). In fact, "Product1" is provided by CSP1 and it consists of three services: "Service1", "Service2" and "Service3". The "Service1" and "Service2" are provided by CSP1 while "Service3" is provided by CSP2. After the provisioning process, the CSC can access the E2E service management functions provided by CSP1 and the function of the services can be accessed through the FI provided by CSP1 and CSP2 respectively.

2) The E2E cloud service lifecycle management system performs cloud service lifecycle management through SMIs in domains as follows:

   a) Defining services: all services need to be defined according to their role and what they offer.

   b) Building cloud service catalogue: the cloud service catalogue contains a list of services of a particular CSP. Besides the definition of the service, many attributes such as who can use this service, resource configurations, service levels, processes, networking options, constraints, etc. can be defined and provided through a service catalogue.

   c) Management of policy: CSCs require the ability to set policies for which cloud services are configured and managed i.e., controls over who has access to cloud assets, periodic and on-demand logging and reporting.

   d) Managing self-service portal: a self-service portal can be managed by a CSP to provide a product catalogue and to take CSCs' requests and offer a degree of control.

   e) Configuring: cloud services can be configured for provisioning and use.

   f) Provisioning service: cloud service should be provisioned automatically according to CSCs' requests.

g) Composition/orchestration of services: multiple cloud services may need to be composed into a single cloud service.

h) Service decommissioning: for the best utilization of resources, when a cloud service (or resource) is suspended, it should be managed by freeing the associated resources. Decommissioning can be achieved on-demand, when a request from a CSC occurs or according to a schedule.

i) Charging: according to the policy, time of use and service type, charging information can be provided.

3) E2E cloud service lifecycle management system implemented by CSP1 can interact with E2E cloud service lifecycle management system implemented by CSP2 through the SMIs between CSPs as shown in Figure 6-1.

6.3 Cloud service lifecycle management stages

A cloud service is managed differently in the various stages of its lifecycle. At a high level view, the lifecycle of the cloud service includes four stages: design, deployment, operation and retirement. The term stage is used to designate the various steps in this overall process. Particular tasks in each stage and how to control the level of independence or interaction from one stage to another stage vary from one organization to another.

The tasks in each stage depend on development process considerations (e.g., software development, testing, deployment, etc.) and operational or business considerations (e.g., how a software component becomes a service in the organization and what are the resulting constraints that are then imposed on the software). Such considerations are part of CSP operational style. This clause presents the basic stages description below but in reality, the involved roles and implementation will vary based on the actual conditions.

The cloud service lifecycle management stages are as follows:

1) Stage 1: Design

The service design metadata is built or the existing one is modified by creating new versions or variants in order to capture at the service level the necessary artefacts to support the business considerations.

During the design stage, the necessary service process specification, template, rules, etc. are created and developed for the operation stage. Policies and their enforcement points are also defined for different service conditions.

2) Stage 2: Deployment

The more specific service deployment metadata specialized from the same service design metadata is built. It is typically done by associating specific values or value ranges for each invariant non-functional characteristic. Several sets of service deployment metadata associated with the same service design metadata constitute in a sense a specific family of related service deployment metadata. These service deployment metadata sets will be mapped to different product offerings and will be used as essential entry points during the fulfilment process.

3) Stage 3: Operation

This stage covers all the activities related to the actual instantiation, monitoring, analysis and feedback to design stage of each service. The management tasks of this stage actually involve two aspects:

a) the cloud service itself (seen as a coordinated set of resources in the execution environment from one or several domains);

b) the cloud service operation metadata, which is the unique representation of the service in the management infrastructure of the CSP.

The operation stage includes the service instantiation and delivery process, during which, the designed templates and policies are distributed to the involved roles. The service is instantiated based on CSC's request and CSP's infrastructure condition. The monitoring control mechanism is set up along with the service instantiation.

The automation of configuration is also provided in this stage, including the initial and subsequent changes. To achieve automation, the inventory, monitoring and control functions are activated.

During the whole operation stage, the monitoring activities are performed via event listening; computing analysis is enforced based on data collection. The event, requiring healing and/or scaling, is published, based on pre-defined policies. The actions (healing and/or scaling) are preformed to implement the changed demands.

Based on the analytical data obtained during the operation stage, the patterns governing usage, thresholds, events, policy effectiveness, etc., are discerned and the feedback necessary to effect changes in the design stage is enabled.

4) Stage 4: Retirement

Triggered by the end of the contractual agreement between CSC and CSP, this stops the monitoring and usage activities and releases the resources and components associated with the cloud service resulting in its disappearing. Note that the retirement process does not necessarily mean that the associate service instance is removed from the service inventory. The CSP may want to keep the service operation metadata in "unconfigured" state in its management infrastructure.

A conceptual cloud service will therefore evolve throughout stages such as those described above. This may affect the service lifecycle metadata as structure (e.g., adding a new element), or as value (e.g., modifying the current value of an element or attribute in the metadata associated with the service). Hence cloud service lifecycle metadata representation evolves with cloud service lifecycle stages while the stages essentially represent the different steps a service would be subject to, from design stage to retirement stage.

6.4 Relationship with cloud computing reference architecture

The cloud computing reference architecture, see [ITU-T Y.3502] provides an architectural framework that is effective for describing the cloud computing roles, sub-roles, cloud computing activities, cross-cutting aspects, as well as the functional architecture and functional components of cloud computing. Although the cloud computing reference architecture does not mention the cloud service lifecycle management in the activities and functional architecture, some of its functional components can be used in different cloud service lifecycle management stages. For example, the subscription management functional component in cloud computing reference architecture handles subscriptions from CSC to particular cloud services, aiming to record new or changed subscription information from CSC and ensure the delivery of the subscribed service(s) to CSC. In addition the operation stage in the cloud service lifecycle covers all the activities related to the actual creation and monitoring of each service, which includes service subscription. Therefore the subscription management functional component can be used in operation stage.

Figure 6-2 illustrates the relationship between E2E cloud service lifecycle stages and functional components of cloud computing reference architecture.

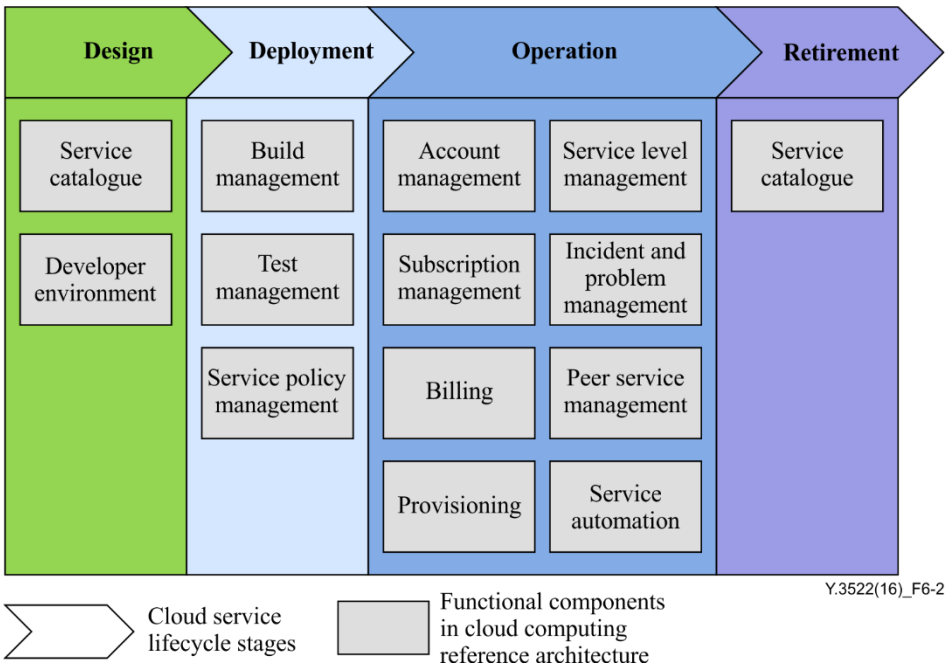


Figure 6-2 – Relationship E2E cloud service lifecycle stages and functional components of cloud computing reference architecture

7 E2E cloud service lifecycle management functional requirements

This clause provides requirements of E2E cloud service lifecycle management derived from the use cases described in Appendix I.

7.1 Service management interface

It is recommended that the CSP provides SMI between cloud services and an E2E cloud service lifecycle management system.

It is recommended that the CSP provides management functionalities of its own cloud service to others CSPs through SMI between CSPs.

7.2 Self-service

It is recommended that the CSP provides an easy method (web portal or other automated approaches) to discover, purchase, configure, deploy, activate and deactivate a service and to check service status to the CSC.

7.3 Service maintenance

It is recommended that the CSP provides automated software enabled cloud services for continuous service maintenance to manage stability and availability of its service.

7.4 Reporting

It is recommended that the CSP provides functions to report (according to local laws and regulations) service health condition, performance, security, geo-location of services, events and other related activities which affect E2E cloud service performance.

7.5 Composite applications or mash-ups

It is recommended that the CSP provides functions to support the rapid delivery of cloud services that are delivered as composite apps, or mash-ups built from multiple services implemented by multiple cloud providers residing in different domains.

7.6 Traditional business processes

It is recommended that the CSP provides functions to support the application of traditional business processes associated with administration, provisioning/configuration, service assurance and charging /billing/settlement involved across inter-clouds residing in different domains.

7.7 Decommissioning

It is recommended that the CSP provides automatic de-commissioning of service resources either based on original service request expiration date or CSC decommission request initiated while the service is running.

7.8 Policy

It is recommended that the CSP provides a set of policies for cloud service access and control.

7.9 Lifecycle stage management

It is required that the CSP provides the ability to run the given service through its lifecycle stages and offers the needed functionality at every step of the process.

7.10 Service automation and continuous delivery

It is required for the CSP to enable automated response to deal with the demand variations and offer necessary feedback to effect changes in the iterative design, by monitoring the service during its operation in order to provide the necessary service automation and continuous delivery without human intervention.

7.11 Metadata management

It is required that the CSP provides metadata schema to support the dynamicity of the services by capturing the service dependencies and service properties at a per-instance level.

8 Security considerations

Security aspects for consideration within the cloud computing environment are addressed by security challenges for the CSPs as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges and describes security capabilities that could mitigate these threats and meet the security challenges.

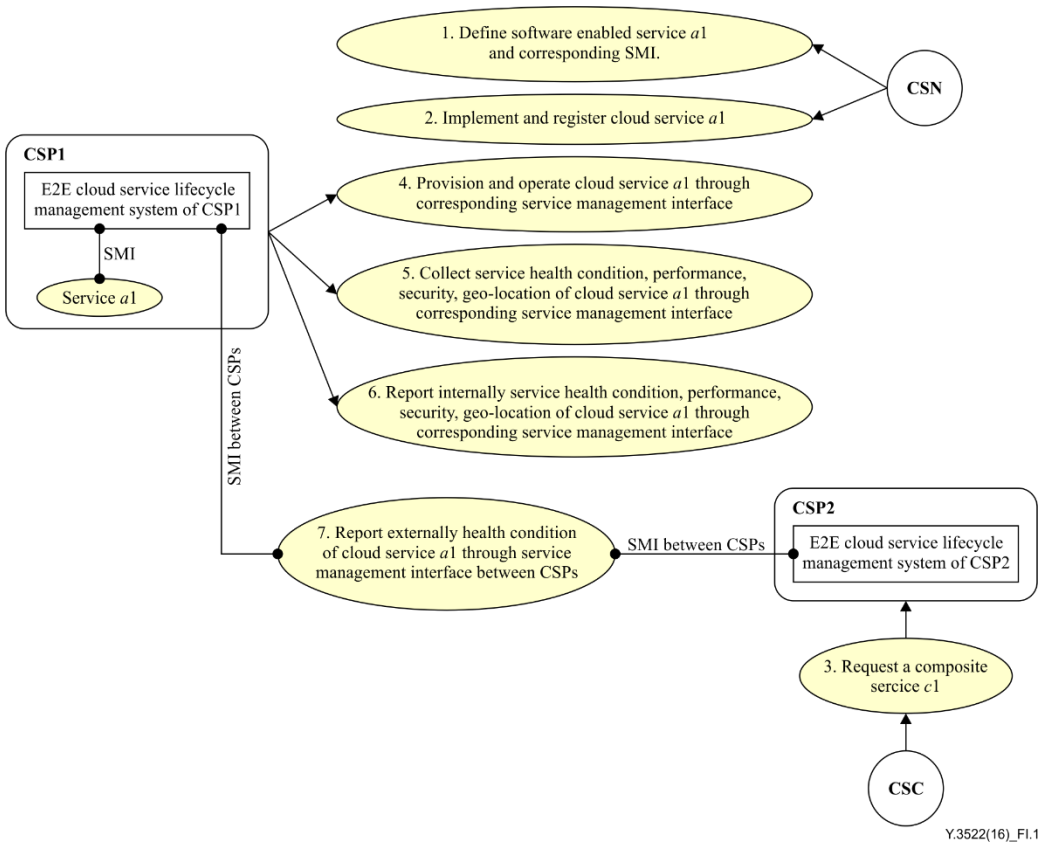
Appendix I

E2E cloud service lifecycle management use cases

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

I.1 Service management interface

Title	Service management interface
Description	CSP1 and CSP 2 established an inter-cloud relationship. Each of them has their own E2E cloud service lifecycle management system inside. CSP1 defines a software enabled service and provides the corresponding service management interface (SMI). CSN makes use of the SMI capabilities provided by CSP1 and develops a new implementation of cloud service *a1*. CSN registers the developed cloud service *a1*. The status, availability, performance and/or delay time of a service *a1* can be collected through SMI. The CSP1 provides his cloud service *a1* to CSP2. CSC requests a composite service *c1* to CSP2. This composite service includes the *a1* service offered by CSP1 which provides a service and management to CSC. The E2E cloud service lifecycle management system of CSP1 provisions and operates service *a1* through its SMI. The E2E cloud service lifecycle management system of CSP1 collects (according to local laws and regulations) service health condition, performance, security, geo-location and events results of the service *a1*through its SMI. The E2E cloud service lifecycle management system of CSP1 reports (according to local laws and regulations) service health condition, performance, security, geo-location of the service *a1* events results internally to CSP1. The E2E cloud service lifecycle management system of CSP1 can report the service health condition of service *a1* externally to CSP2 through SMI between CSPs .
Roles	CSP, CSC, CSN

Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	– The status, availability, performance and/or delay time of cloud service can be collected through SMI. – The E2E cloud service lifecycle management system of CSP1 reports internally service health condition, performance, security, geo-location of cloud service *a1* through corresponding SMI. – The E2E cloud service lifecycle management system of CSP1 reports externally service health condition of cloud service *a1* o CSP2 through SMI between CSPs.
Derived requirements	– Service management interface (refer to clause 7.1) – Service Management Interface between CSPs (refer to clause 7.1) – Reporting (refer to clause 7.4)

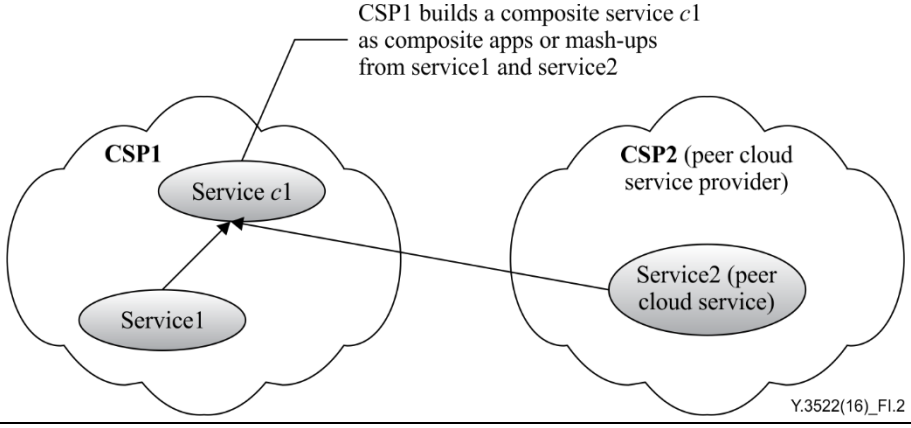
I.2 Self-service use case

Title	Self-service use case
Description	CSP provides cloud services to the market. For improvement of CSC experiences, the CSP provides self-service method to CSCs (e.g., web portal or other automated approaches) to discover, purchase, configure, deploy, activate and deactivate cloud service and to check cloud service status.
Roles	CSP, CSC
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	– The self-service method is provided to CSCs to discover, purchase, configure, deploy, activate and deactivate cloud service and to check cloud service status.
Derived requirements	– Self-service (refer to clause 7.2)

I.3 Service maintenance use case

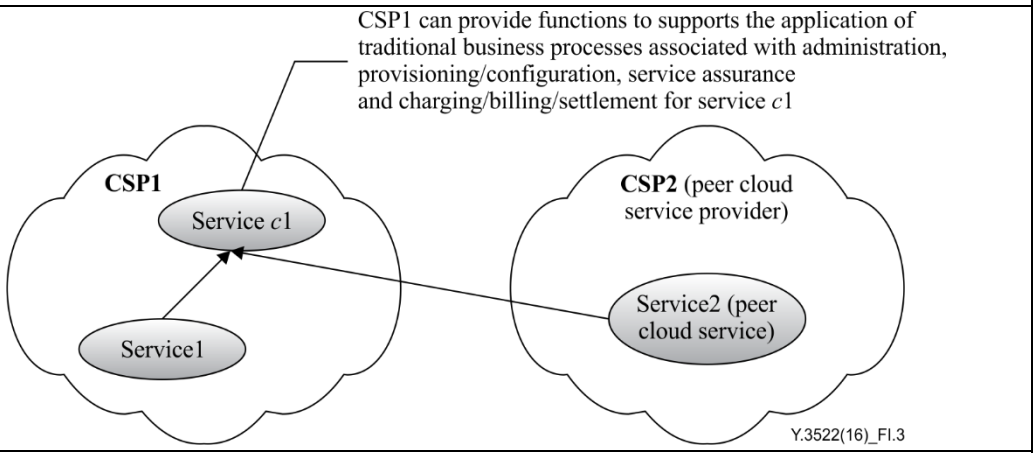
Title	Service maintenance use case
Description	A CSP provides cloud services to the market. For the stability and availability of its service, periodic maintenance is needed. For a good customer experience, the maintenance cannot result in a long suspension and deactivation of a service. Therefore it is required that CSP can provide automated software enabled cloud services to shorten the maintenance time.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	– The CSP can provide automated software enabled cloud services.
Post-conditions (optional)	– The duration of suspension and deactivation is reduced markedly.
Derived requirements	– Service maintenance (refer to clause 7.3)

I.4 Composite applications or mash-ups use case

Title	Composite applications or mash-ups use case
Description	CSP1 builds cloud service c1 as composite apps, or mash-ups from service1 delivered by CSP1 and sevice2 delivered by CSP2.
Roles	CSP
Figure (optional)	

Pre-conditions (optional)	– Service1 delivered by CSP1. – Service2 delivered by CSP2.
Post-conditions (optional)	– A composite service c1 is built from service1 and service2.
Derived requirements	– Composite applications or mash-ups (refer to clause 7.5)

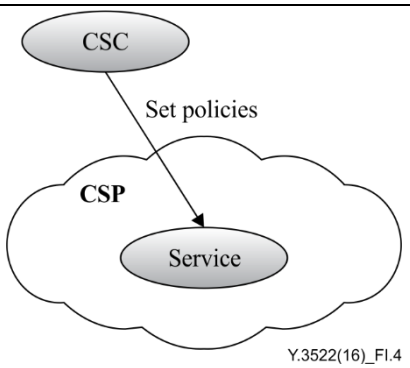
I.5 Traditional business processes use case

Title	Traditional business processes use case
Description	CSP1 builds a composite service c1 from service1 delivered by CSP1 and sevice2 delivered by CSP2. CSP1 can provide functions to support the application of traditional business processes associated with administration, provisioning/configuration, service assurance and charging /billing/settlement for service c1.
Roles	CSP
Figure (optional)	
Pre-conditions (optional)	– CSP1 builds a composite service c1 from service1 delivered by CSP1 and sevice2 delivered by CSP2.
Post-conditions (optional)	– CSP1 can provide functions to support the application of traditional business processes associated with administration, provisioning/configuration, service assurance and charging /billing/settlement for service c1.
Derived requirements	– Traditional business processes (refer to clause 7.6)

I.6 Decommissioning use case

Title	Service decommissioning use case
Description	A CSP provides cloud services to the market. When an original service request passes its expiration date or a user decommission request initiated while the service is running, the resources of this service should be decommissioned automatically.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	– An original service request passes its expiration date or a user decommission request initiated while the service is running.
Post-conditions (optional)	– The service resources have been decommissioned automatically.
Derived requirements	– Decommissioning (refer to clause 7.7)

I.7 Policy use case

Title	Policy use case
Description	A CSP provides some kind of cloud services to the market. The CSC of its service want to have the abilities to control who can access to cloud assets, plus both periodic and on-demand logging and reporting. Therefore the CSP is required to provide functions to support the CSC's ability to set policies for doing this.
Roles	CSP, CSC
Figure (optional)	
Pre-conditions (optional)	CSC can set policies on the service.
Post-conditions (optional)	The policies of the service have been set successfully.
Derived requirements	– Policy (refer to clause 7.8)

I.8 Lifecycle stage management use case

Title	Lifecycle stage management use case
Description	A CSP provides some kind of cloud services to the market. For a better management for its services, the CSP is required to provide the ability to run the given service through its lifecycle stages and offers the needed functionality at every step of the process.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	/
Derived requirements	– Lifecycle stage management (refer to clause 7.9)

I.9 Service automation and continuous delivery use case

Title	Service automation and continuous delivery use case
Description	A CSP provides cloud services to the market. Because of the continuous changing of the market and CSC's requirements, the design of the cloud service should be an iterative process. By monitoring the service during its operation, the demand variations should be responded to automatically and the necessary feedback to effect changes should be offered to the service designer.
Roles	CSP, CSC
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	/
Derived requirements	– Service automation and continuous delivery (refer to clause 7.10)

I.10 Metadata management use case

Title	Metadata management use case
Description	A CSP provides cloud services to the market. According to market requirement changes, it is needed to adjust the already existing cloud services. Therefore, a robust schema like metadata which can be distributed in each stage needs to be provided.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	CSP can support new cloud service creation with minimal modifications.
Derived requirements	– Metadata management (refer to clause 7.11)

Bibliography

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer and Code Pack, Release 2.2*. https://www.tmforum.org/?s=TR198

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