International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.4040

(02/2016)

SERIES Q: SWITCHING AND SIGNALLING

Testing specifications – Testing specifications for Cloud computing

The framework and overview of cloud computing interoperability testing

Recommendation ITU-T Q.4040

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
Testing specifications for next generation networks	Q.3900–Q.3999
Testing specifications for SIP-IMS	Q.4000–Q.4039
Testing specifications for Cloud computing	**Q.4040–Q.4059**

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

Recommendation ITU-T Q.4040

The framework and overview of cloud computing interoperability testing

Summary

Recommendation ITU-T Q.4040 describes the framework and provides an overview of cloud computing interoperability testing. According to the identified target areas of testing, this framework Recommendation includes an overview of cloud computing interoperability testing with common confirmed items, infrastructure capabilities type, platform capabilities type and application capabilities type interoperability testing. This Recommendation describes the overview target areas of testing for interoperability testing of cloud computing.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.4040	2016-02-13	11	11.1002/1000/12703

Keywords

Cloud computing, interoperability.

* 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 Q.4040

The framework and overview of cloud computing interoperability testing

1 Scope

This Recommendation describes the framework and provides an overview of cloud computing interoperability testing. According to the identified target areas of testing, this framework Recommendation includes an overview of cloud computing interoperability testing with common confirmed items, infrastructure capabilities type, platform capabilities type and application capabilities type interoperability testing.

2 References

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

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T Y.1401] Recommendation ITU-T Y.1401 (2008), *Principles of interworking*.

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

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing framework and high-level requirements*.

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

[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*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 interoperability [ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

3.1.2 interworking [ITU-T Y.1401]: The term "interworking" is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication.

3.1.3 cloud service provider (CSP) [ITU-T Y.3500]: Party which makes cloud services available.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud interoperability: The capability to interact between CSCs and CSPs or between different CPSs, including the ability of CSCs to interact with cloud services and exchange information, the ability for one cloud service to work with other cloud services, and the ability for CSCs to interact with the cloud service management facilities of the CSPs.

3.2.2 cloud interoperability testing: Verifying functions and interaction that realize the cloud interoperability.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS Business Support Systems

CCRA Cloud Computing Reference Architecture

CSC Cloud Service Customer

CSP Cloud Service Provider

IaaS Infrastructure as a Service

ICT Information and Communication Technology

IT Information Technology

OSS Operational Support Systems

PaaS Platform as a Service

QoS Quality of Service

SaaS Software as a Service

SLA Service-Level-Agreement

VM Virtual Machine

5 Overview of cloud computing interoperability testing

Interoperability in the context of cloud computing includes the ability of a cloud service customer to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results. Typically, interoperability implies that the cloud service operates according to an agreed specification, one that is possibly standardized. The cloud service customer should be able to use widely available ICT facilities in-house when interacting with the cloud services, avoiding the need to use proprietary or highly specialized software. The interoperability of cloud services can be categorized by the management and functional interfaces of the cloud services. Many existing IT standards contribute to the interoperability between cloud consumer applications and cloud services, and between cloud services themselves. There are standardization efforts that are specifically initiated to address the interoperability issues in the cloud system. Interoperability also includes the ability for one cloud service to work with other cloud services, either through an inter-cloud provider relationship, or where a cloud service customer uses different multiple cloud services in some form of composition to achieve its business goals.

Interoperability stretches beyond the cloud services themselves and also includes the interaction of the cloud service customer with the cloud service management facilities of the cloud service provider. Ideally, the cloud service customer should have a consistent and interoperable interface to the cloud

service management functionality and be able to interact with two or more cloud service providers without needing to deal with each provider in a specialized way.

The main purpose of interoperability testing is to evaluate the interaction between cloud service customer and cloud service provider to obtain predictable results, collaboration among different cloud services, and consistency and interoperability of management interface across different services.

A cloud capabilities type is a classification of the functionality provided by a cloud service to the cloud service customer, based on the resources used. There are three different cloud capabilities types [ITU-T Y.3500]: infrastructure capabilities type, platform capabilities type, and application capabilities type, which are different because they follow the principle of separation of concerns, i.e., they have minimal functionality overlap between each other. The interoperability testing in different cloud capabilities type is different; there are three major interoperability testing scenarios as follows:

- infrastructure capabilities type interoperability testing
- platform capabilities type interoperability testing
- application capabilities type interoperability testing.

As shown in Figure 1, there are three different target areas of cloud computing interoperability testing as follows:

- "CSC – CSP", dealing with interaction between CSC and CSP
- "CSP – CSP", dealing with collaboration among different CSPs
- "CSP – management", dealing with CSP management functions.

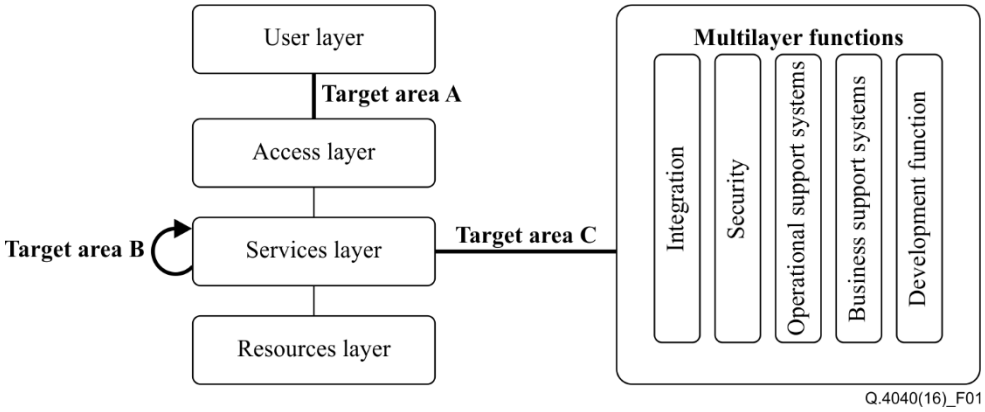

Figure 1 – Target areas of cloud computing interoperability testing

Also, the cloud architecture in terms of the common set of cloud computing functional components are described in [ITU-T Y.3502]. Figure 2 presents a high level overview of the CCRA functional components organized by means of the layering framework.

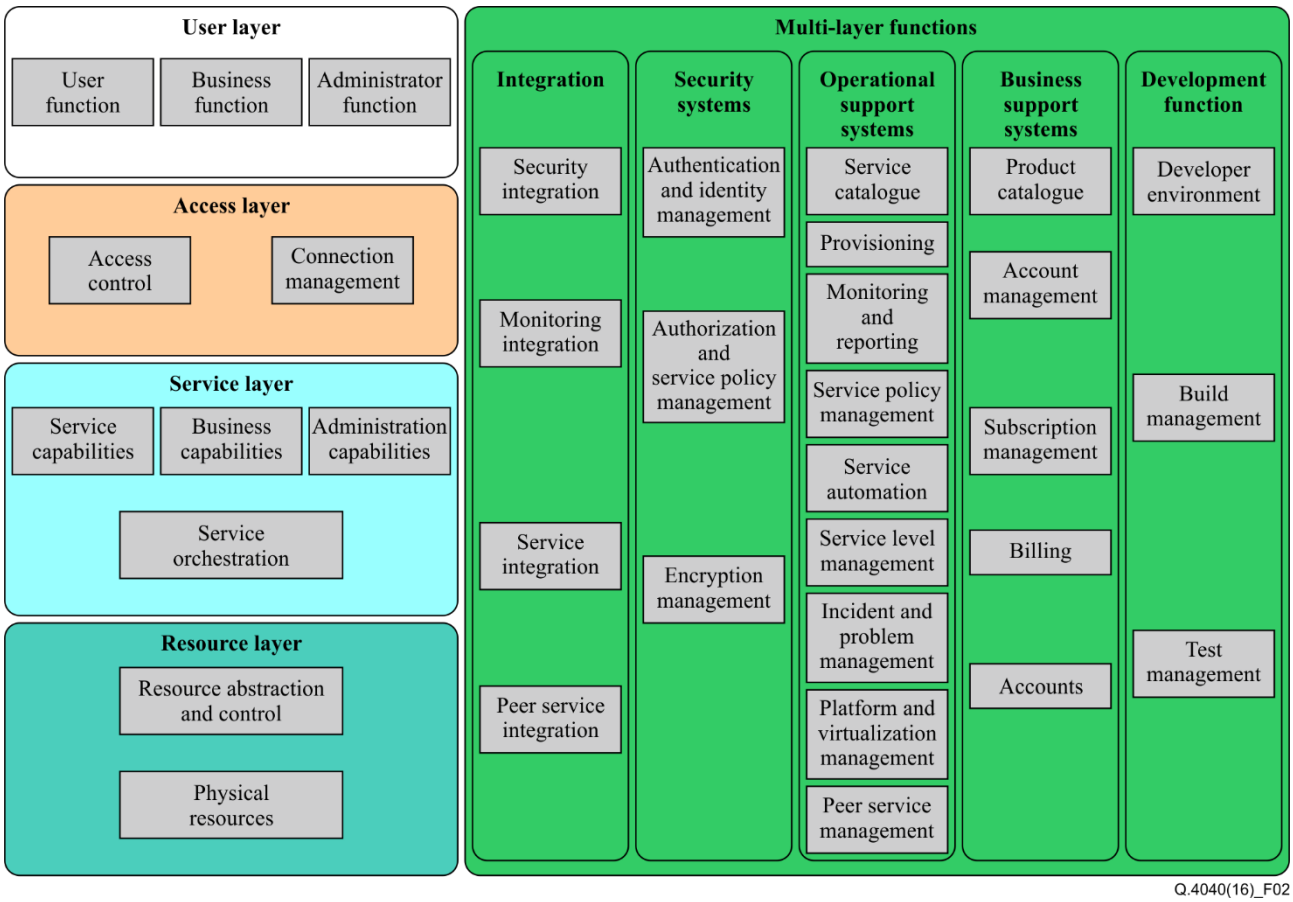

Figure 2 – Functional components of the CCRA

This Recommendation covers the typical functional components, not all components, and interworking among them in clauses 7, 8 and 9.

5.1 Common aspects to be considered in cloud computing interoperability testing

The aspects which should be considered for the testing of cloud computing interoperability need to be prescribed according to the requirements described in [ITU-T Y.3501]. The following items, picked up from the general requirements for cloud computing [ITU-T Y.3501], indicate common aspects to be considered in cloud computing interoperability testing:

- Service life-cycle management

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

- Regulatory aspects

It is required that all applicable laws and regulations be respected, including those related to privacy protection.

- Security

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

- Accounting and charging

It is recommended that cloud computing supports various accounting and charging models and policies.

- Efficient service deployment

It is recommended that cloud computing enables efficient use of resources for service deployment.

- Interoperability

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

- Portability

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

- Service access

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

- Service availability, service reliability and quality assurance

It is recommended that the cloud service provider (CSP) provides end-to-end quality of service assurance, high levels of reliability and continued availability.

5.2 Infrastructure capabilities type interoperability testing

Cloud infrastructure includes compute, storage, network and other hardware resources, as well as software assets. Abstraction and control of physical resources are essential means to achieve on-demand and elastic characteristics of cloud infrastructure. This way, physical resources can be abstracted into virtual machines (VMs), virtual storage and virtual networks. The abstracted resources are controlled to meet cloud service customers' (CSC) needs. [ITU-T Y.3510]

The goal for cloud infrastructure capabilities type interoperability is to devise and implement testing methods and conduct a basic set of functional tests for infrastructure capabilities type (IaaS) Interoperability in a hybrid cloud environment using both private and public clouds.

Ideally, cloud subscribers would like to be able to select any cloud provider based on the basis of service cost, performance and capabilities. In order to make this feasible for the cloud consumer, the various hypervisor platforms and infrastructure components involved will need to be interoperable and enable portability, leveraging defined industry standards.

Reliability and reproducibility of a change such as a VM migration involved in IaaS are based on pre-defined standards, specifications, frameworks, scenarios, and processes. This need exists in their organizations too for reasons such as being able to demonstrate the ability to move between internal private clouds, being able to move between cloud providers if necessary, and if for no other reason, to demonstrate that the service is not locked in to that environment with no relocation options once it has been established there.

5.3 Platform capabilities type interoperability testing

Platform capabilities type (PaaS) interoperability encourages seamless operation of cloud applications across providers, rapid integration with consumer orchestration engines, and automatable configuration and operation of both the PaaS container and the execution of the application itself. This provides the combined benefits of rapid application deployment and linear scalability without the overhead of directly managing the underlying infrastructure for the application, all while avoiding PaaS lock-in.

The business drivers for PaaS Interoperability are as follows:

- Rapid application deployment: Enable subscribers to quickly deploy new business applications. Reduce the overhead of ongoing application deployments.

- Application scalability: Ability to quickly scale applications up and back based on the real-time demand for those applications.
- Application migration: Ability to move applications from one discrete PaaS to another PaaS available from the same or different cloud provider with minimal effort.
- Business continuity: Migrate or replicate applications among PaaS services to address outages, security breaches, or other disruptions. This is intended to encompass both disaster recovery and disaster avoidance.

Interoperability perspectives follow:

- Interconnectability: The parallel process in which two coexisting environments communicate and interact.
- Portability: The serial process of moving a system from one cloud environment to another.

5.4 Application capabilities type interoperability testing

In portability and interoperability of application capabilities (SaaS) environments, business process functionality offered through SaaS solutions can be initially connected, transferred, or interconnected. SaaS interoperability allows organizations to create mash-ups from multiple SaaS and non-SaaS applications. This is an issue that primarily concerns data exchange, which includes metadata, and interface compatibility.

6 Cloud computing interoperability testing between CSC and CSP

CSC is a party in a business relationship for the purpose of using cloud services. The interoperability between CSC and CSP supports the CSC to interact with CSP according to a prescribed method and obtain predictable results. Enabled by interworking between CSC and CSP, CSC can use the capabilities provided by CSP, such as using the processing, network and storage capability. For example, CSC can use virtual machine provide by the CSP.

CSC can also perform business administration tasks such as subscribing to cloud service and administering use of cloud service through the interaction with CSP.

Based on the reference architecture described in [ITU-T Y.3502], the interworking involved in CSC-CSP relationship and corresponding test objective can be identified as follows:

- Interworking between CSC and CSP's service integration component.

  Test objective is to verify that CSP can provide connections to CSP's services for CSC.
- Interworking between CSC and CSP's authentication and identities management component

  Test objective is to verify that CSP can provide capabilities relating to user identities and the credentials required to authenticate users are provided when CSC access cloud services and related administration and business capabilities.
- Interworking between CSC and CSP's authorization and security policy management component

  Test objective is to verify that CSP can provide capabilities for the control and application of authorization for CSC to access specific capabilities or data.
- Interworking between CSC and CSP's product catalogue component

  Test objective is to verify that the CSP can provide capabilities for browsing available service list, and capabilities for management of the content of catalogue.
- Interworking between CSC and CSP's account management CSC

  Test objective is to verify that the CSP can provide capabilities for managing cloud service relationships, including management of contracts, subscription to cloud service, entitlements, service pricing and policies that apply to the treatment of CSC data.

- Interworking between CSC and CSP's subscription management component

  Test objective is to verify that the CSP can handle subscriptions from CSC to particular cloud services, aiming to record new or changed subscription information from the customer and ensure the delivery of the subscribed service(s) to the customer.

- Interworking between CSC and CSP's monitoring and report component

  Test objective is to verify that CSP can provide capabilities monitoring the cloud computing activities of other functional components throughout the CSP's system and providing reports on the behaviour of the cloud service provider's system.

- Interworking between CSC and CSP's service access

  Test objective is to verify that CSP can provide service access capabilities that provide access offered by CSP, perform authentication of the CSC and establish authorization to use particular capabilities of the cloud service. If authorized, the service access capabilities invoke the cloud service implementation which performs the request.

- Interworking between CSC and CSP's service capabilities

  Test objective is to verify that CSP can provide service capabilities which consist of the necessary software required to implement the service offered to CSC.

- Interworking between CSC and CSP's resource abstraction and control

  Test objective is to verify that CSP can provide access to the physical computing resources through software abstraction and to offer qualities such as rapid elasticity, resource pooling and on-demand self-service.

- Interworking between CSC and CSP's physical resources

  Test objective is to verify that the operational support systems can manage all the elements of the physical resources (e.g., computing resources, storage resources, and network resources).

For interoperability testing between CSC and CSP, the interoperability testing target should cover the interworking between CSC and CSP described above. A set of functional test cases need to be developed based on the corresponding test objectives, and perform functional test to determine if CSC interoperate with CSP. Figure 3 shows the relationships among functional components and functions for the "use cloud service" activity between CSC and CSP according to clause A.1.1 of [ITU-T Y.3502].

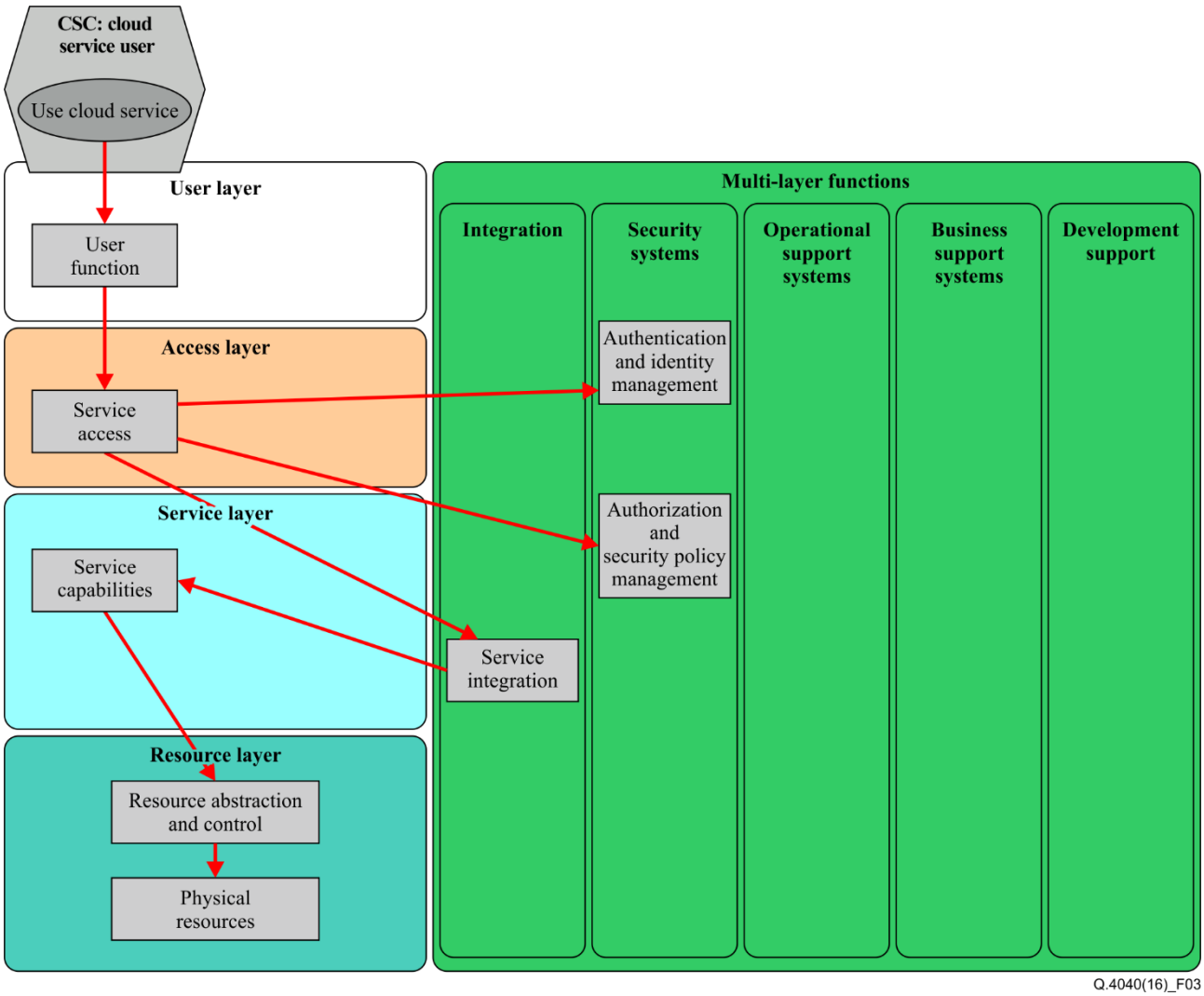

Figure 3 – Relationships among functional components and functions for the "use cloud service" activity between CSC and CSP

7 Cloud computing interoperability testing between CSP and CSP

Ideally, multiple interoperable CSPs could interact in different patterns of inter-cloud: peering, federation, and intermediary patterns, as defined in [ITU-T Y.3511]. In inter-cloud peering pattern, two CSPs interwork directly with each other, and one CSP can use the services provided by the peer CSP. In inter-cloud federation pattern, a group of peer CSPs mutually combine their service capabilities in order to provide the set of cloud services required by CSCs. In inter-cloud intermediary pattern, CSP interworks with one or more peer CSPs and provides intermediation, aggregation and arbitrage of services provided by these CSPs.

The functions which should be tested for inter cloud computing interoperability need to be prescribed according to the functional requirements described in [ITU-T Y.3511]. The following bullet items indicate aspects to be considered in the cloud computing interoperability testing of the CSP-CSP interworking.

- SLA and policy negotiation should be confirmed as follows:
  - the SLA and policy information that is aware of the SLA information related to the QoS and performance aspects of the CSPs involved is exchanged among multiple CSPs using standard formats;
  - the SLA and policy information comparing, negotiating and settling down service provisioning policies is exchanged among multiple CSPs using standard formats.

- Resource monitoring should be confirmed as follows:
  - resource information is exchanged in a standard manner among multiple CSPs;
  - updated resource information is exchanged among multiple CSPs in synchronization with the events involving the CSPs;
  - collecting information about the usage and performance status of the resources is exchanged among multiple CSPs periodically or on a request basis;
  - collecting information about the resource availability is exchanged among multiple CSPs periodically or on a request basis;
  - monitoring information in commonly defined ways is exchanged among multiple CSPs.
- Resource performance estimation and selection should be confirmed as follows:
  - the achievable resource performance that is available reserved resources in the secondary CSPs is exchanged between secondary CSPs.
- Resource discovery and reservation should be confirmed as follows:
  - CSP can discover available resources of the peer CSPs;
  - discovered resources in the peer CSPs are reserved;
  - discovered resources in the peer CSPs are reserved provisionally;
  - available resources in the peer CSPs are found based on different priorities;
  - available resources in the peer CSPs are reserved on the basis of different priorities.
- Resource set-up and activation should be confirmed as follows:
  - reserved resources in a peer CSP are established;
  - the configuration and policy settings of reserved resources in the peer CSPs are accessed.
- Cloud services switchover and switchback should be confirmed as follows:
  - the CSC's end-user is switched over access to a peer CSP without manual operation from the CSC, in order to allow the CSC's end user to use services in a similar manner to the way he/she did before the access was switchover;
  - the CSC's end-user access is switched back to the primary CSP when this CSP has recovered from the switchover
- Resource release should be confirmed as follows:
  - resources reserved, activated and/or set up in the peer CSPs are released by the CSP;
  - the peer CSP's resource configuration information are updated;
  - received cloud application data are erased and/or transferred back during the resource reservation.
- CSC information exchange should be confirmed as follows:
  - CSC information is activated only with the prior agreement of the CSC;
  - CSC profiles and associated information can be managed;
  - CSC profiles and associated information can be exchanged among multiple CSPs according to a pre-determined protocol and format, with the condition that the CSC is informed of and agrees to the exchange.
- Primary CSP role delegation should be confirmed as follows:
  - a CSP is activated only with the prior agreement of the CSC;
  - a CSP is able to discover peer CSPs that are capable of inheriting the primary CSP role, and to negotiate with these peer CSPs as to whether they can accept the inheritance;

  - a CSP is able to transfer its management information associated with the primary CSP role in a reliable manner to the peer CSPs that have accepted the permission transfer with that CSP;
  - the controllability of the information associated with the primary CSP role can be transferred to the secondary CSPs with minimum interruptions;
  - a CSP is able to cancel the permission transfer arrangements.
- Inter-cloud service handling should be confirmed as follows:
  - service intermediation is supported;
  - service aggregation is supported;
  - service arbitrage is supported.

A CSP can make use of one or more cloud services which are provided by other CSP. In every patterns of inter-cloud, there are two roles of CSP – primary CSP and secondary CSP. The provider making use of the services is termed a primary CSP while a provider whose services are being used is termed a secondary CSP. There are two types of relationship between a primary CSP and a secondary CSP:

- the use of secondary CSP's cloud services by a primary CSP;
- the use of secondary CSP's business and administration capabilities by the primary CSP's cloud service operations manager and CSP's cloud service manager to establish and control the use of the secondary CSP's cloud services.

Based on the reference architecture, the interworking involved in CSP-CSP relationship and corresponding test objectives can be identified as follows:

- interworking between primary CSP and CSC

  test objective is to verify that CSC can use cloud service, administer use of cloud service and perform business administration to the cloud services, in peering, federation or intermediary pattern;
- interworking between primary CSP's peer service integration component and secondary CSP

  test objective is to verify that primary CSP can connect to services of secondary CSP with appropriate security and with appropriate accounting for the usage;
- interworking between primary CSP's peer service management component and secondary CSP

  test objective is to verify that the primary CSP's operational support systems and business support systems can be connected to the administration capabilities and business capabilities of secondary CSP;
- interworking between CSPs to form and maintain inter-cloud pattern

  test objective is to verify that multiple CSP can interact to form and maintain the peering, federation or intermediary pattern.

8 Cloud computing interoperability testing between CSP and its management system

The interface of management system is used to interact with cloud services to provide supporting capabilities, such as monitoring and provisioning of cloud service. As described in [ITU-T Y.3502], management functional components are implemented in multi-layer functions in reference architecture. Interoperability testing is done to verify the following test objective:

- Operational support test

  Test objective is to verify that CSP can perform OSS related operation that required managing and controlling the cloud services offered to CSC, including runtime administration, monitoring, provisioning and maintenance.

- Business support test

  Test objective is to verify that CSP can provide a set of business-related management capabilities dealing with customers and supporting processes, including product catalogue, billing and financial management.

- Security test

  Test objective is to verify that security related controls can be applied to mitigate the threats in cloud computing environment, including authentication, authorization, auditing, validation, and encryption.

- Integration test

  Test objective is to verify that functional components can be connected to achieve the required functionality.

- Development support test

  Test objective is to verify that CSP can provide development support capabilities involving the creation, testing and life-cycle management of services and service components and support the cloud computing activities of the cloud service developer.

Appendix I

Cloud interoperability testing scenarios

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

ITU-T, ETSI and NIST have been considering wide technical areas related to cloud computing and also developing several use case documents which are generally recognised by cloud computing industry. Since the use case documents are like a framework document for cloud usage and involve wide technical areas, the documents shown below are useful reference documents in order to develop cloud interoperability testing specifications.

1) ITU-T Y.3500 series

   [ITU-T Y.3501] – Cloud computing framework and high-level requirements

      Appendix I – Use cases of cloud computing

   [ITU-T Y.3511] – Framework of inter-cloud computing for network and infrastructure

      Appendix I – Use cases from the inter-cloud perspective

      Appendix II – Use cases from telecom and non-telecom providers' views

      Appendix III – Abstract service offering models for inter-cloud computing

2) ETSI Cloud Standards Coordination Final Report (November 2013)

      Section 3 – Use cases analysis (especially cloud bursting)

3) NIST cloud computing program technical efforts

      NIST cloud computing test scenario use cases – Version 1

4) ODCA usage model for IaaS, PaaS, SaaS

   ODCA has published many usage models:

      ODCA SAAS_Interop_UM_Rev1.0 Software as service (SaaS) interoperability

      ODCA PAAS_Interop_UM_Rev1.0 Platform as a service (PaaS) interoperability

      ODCA VM_Interoperability_in_a Hybrid_Cloud_Enviroment_rev1.2 Virtual machine (VM) Interoperability in a hybrid cloud environment

      ODCA VM_Interop_PoC_White_Paper Implementing the Open Data Center Alliance Virtual Machine Interoperability Usage Model

NOTE – The detail contents are described in [b-ITU-T Q-Sup.65].

Bibliography

[b-ITU-T Q-Sup. 65] ITU-T Q-series Recommendations – Supplement 65 (2014), *Cloud computing interoperability activities*.

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