International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3516

(09/2017)

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

Cloud Computing

Cloud computing – Functional architecture of inter-cloud computing

Recommendation ITU-T Y.3516

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, 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.3516

Cloud computing – Functional architecture of inter-cloud computing

Summary

Recommendation ITU-T Y.3516 specifies inter-cloud computing functional architecture, including functions and functional components, based on the inter-cloud computing framework specified in Recommendation ITU-T Y.3511. The Recommendation builds upon the functional view of the cloud computing reference architecture (Recommendation ITU-T Y.3502) and makes extensions to functional components with inter-cloud functions.

Recommendation ITU-T Y.3516 also describes the mapping between functions and functional requirements of inter-cloud computing and examples of inter-cloud related reference points.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3516	2017-09-13	13	11.1002/1000/13352

Keywords

Inter-cloud computing, functions, functional architecture, functional component.

* 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.3516

Cloud computing – Functional architecture of inter-cloud computing

1 Scope

This Recommendation specifies inter-cloud computing functional architecture, including functions and functional components, based on the inter-cloud computing framework specified in [ITU-T Y.3511]. The Recommendation builds upon the functional view of the cloud computing reference architecture [ITU-T Y.3502] and makes extensions to functional components with inter-cloud functions.

The scope of this Recommendation consists of:

– overview of inter-cloud computing functional architecture;

– functions of inter-cloud computing;

– functional components of inter-cloud computing architecture.

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 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.3514] Recommendation ITU-T Y.3514 (2017), *Cloud computing – Trusted inter-cloud computing framework and requirements*.

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 activity [ITU-T Y.3502]: A specified pursuit or set of tasks.

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

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

3.1.5 functional component [ITU-T Y.3502]: A functional building block needed to engage in an activity, backed by an implementation.

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 peer cloud service [ITU-T Y.3502]: A cloud service of one cloud service provider which is used as part of a cloud service of one or more other cloud service providers.

3.1.8 peer cloud service provider [ITU-T Y.3502]: A cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services.

3.1.9 primary cloud service provider [ITU-T Y.3511]: In inter-cloud computing, a cloud service provider which is making use of cloud services of peer cloud service providers (i.e., secondary cloud service providers) as part of its own cloud services.

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

3.1.11 secondary cloud service provider [ITU-T Y.3511]: In inter-cloud computing, a cloud service provider which provides cloud services to a primary cloud service provider.

NOTE – The primary cloud service provider can use the services of secondary cloud service providers as part of its services offered to cloud service customers.

3.1.12 sub-role [ITU-T Y.3502]: A subset of the activities of a given role.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BSS Business Support System

CSC Cloud Service Customer

CSP Cloud Service Provider

CSU Cloud Service User

KPI Key Performance Indicator

OSS Operations Support System

QoS Quality of Service

SLA Service Level Agreement

5 Conventions

None.

6 Overview

6.1 Inter-cloud functional architecture with different patterns

Inter-cloud computing describes the interworking of cloud service providers (CSPs) in order to deliver cloud services to cloud service customers (CSCs) and cloud service users (CSUs)

[ITU-T Y.3511]. One important target of inter-cloud computing for CSPs is to take benefit of the inter-cloud relationships established between peer CSPs (through inter-cloud patterns) in order to satisfy cloud service requirements of CSCs. The CSP who provides services for CSCs plays the role of primary CSP. The primary CSP is responsible for the cloud service level agreement (SLA) and interacts with peer CSP(s) within an inter-cloud relationship.

An inter-cloud relationship is bidirectional. As illustrated on Figure 6-1, CSP A plays a role of primary CSP when using the services of CSP B for providing services to its own customers, CSC A1 and CSC A2 (highlighted by black coloured arrows). CSP A plays the role of secondary CSP when providing services to CSP B, who plays the role of primary CSP and provides services to its own customers, CSC B1 and CSC B2 (highlighted by grey coloured arrows).

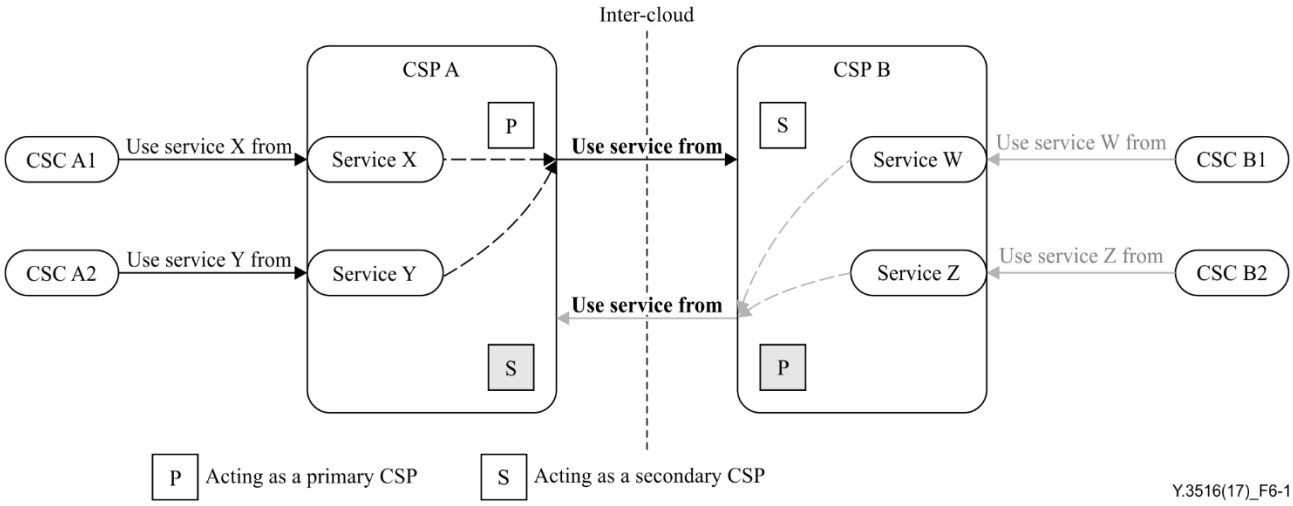

Figure 6-1 – Illustration of bidirectional relationship in inter-cloud computing

The inter-cloud computing concept is based on the relationship (pattern) among multiple CSPs as follows: peering, federation, and inter-cloud intermediary [ITU-T Y.3511]. These patterns are different in terms of business models and relationships between CSPs. However, these patterns are convergent from the viewpoint of inter-cloud computing functions and architecture.

The inter-cloud peering pattern contains only two CSPs and is the fundamental pattern, which may exist on its own or can be used in the other two patterns. The inter-cloud federation pattern involves a group of peer CSPs who mutually combine their service capabilities in order to provide the set of cloud services required by CSCs. The involved peer CSPs forming the inter-cloud federation establish and share common agreement which may range from service related policies, service level agreements (SLAs). The inter-cloud intermediary pattern refers to one and provides intermediation, aggregation and arbitrage of services provided by these peer CSPs.

The roles of the three patterns are also the same, the CSC, the primary CSP, and the secondary CSP. Among the multiple peer CSPs, the one that directly provides cloud services to its CSCs is called the primary CSP, while the one which indirectly provides its cloud service is called the secondary CSP. The secondary CSP treats the primary CSP as a CSC. Cloud services provided by the secondary CSP to the primary CSP are used by the primary CSP to offer services to its own customers (cf. the "perform peering, federation, intermediation, aggregation, arbitrage" activity defined in clause 8.3.2.16 of [ITU-T Y.3502]). For resource handling, the primary CSP negotiates to use the resources of secondary CSPs as an inter-cloud service.

NOTE – This Recommendation uses the term *inter-cloud service* instead of *abstracted resources* employed in [ITU-T Y.3511].

From the architecture point of view, the functions and functional components, as well as reference points for inter-cloud are the same, no matter which inter-cloud patterns are used.

6.2 Relationship with cloud computing reference architecture

The high-level interaction between CSPs for an inter-cloud relationship is described in the cloud computing reference architecture [ITU-T Y.3502]. Two functional components are defined to support inter-cloud computing [ITU-T Y.3502]: peer service integration (shown in Figure 6-2) and peer service management (shown in Figure 6-3 and Figure 6-4). As shown in Figure 6-2, a peer service integration functional component is used by a primary CSP to integrate services from peer CSP(s) (available through service access functional component in access layer) with its own services.

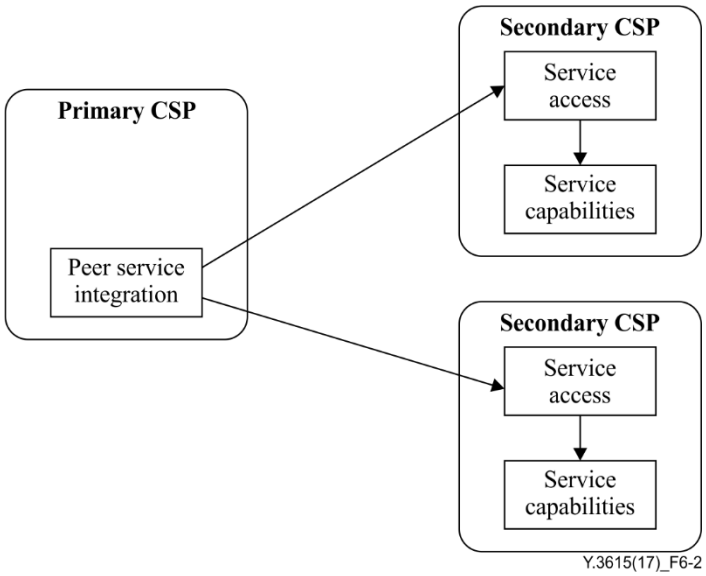

Figure 6-2 – Primary CSP using cloud services provided by secondary CSPs

Figure 6-3 and Figure 6-4 indicate primary CSP use peer service management functional component to make access to the secondary CSPs' operational support systems and business support systems (BSSs) through business access functional component and business capabilities, administration access functional component and business capabilities respectively.

This Recommendation describes additional extensions to [ITU-T Y.3502] for the support of inter-cloud, in particular extensions to functions and the definition of reference points necessary to support interactions between relevant functional components.

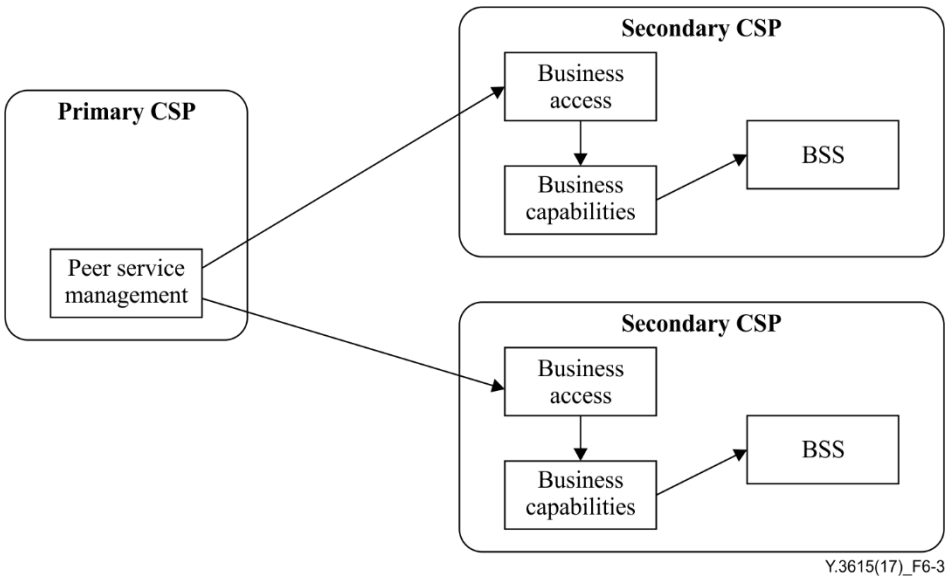

Figure 6-3 – Primary CSP using business capabilities provided by secondary CSPs

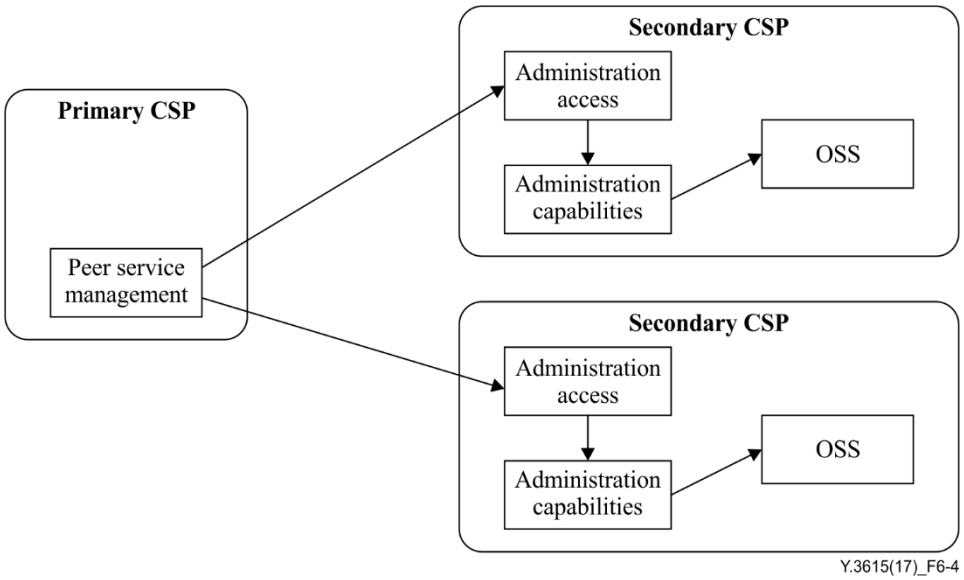

Figure 6-4 – Primary CSP using administration capabilities provided by secondary CSPs

The inter-cloud functional components in the functional architecture represent sets of functions that are required to perform inter-cloud computing activities for various roles and sub-roles. There are two types of relationship between peer CSPs:

- the use of cloud services of secondary CSPs by a primary CSP;
- the use of business and administration capabilities of secondary CSPs by a primary CSP.

The secondary CSP provides inter-cloud services to the primary CSP. From the secondary CSP point of view, the primary CSP plays the role of CSC. As a result, there is no difference in terms of service access and service capabilities for inter-cloud, compared to the case of cloud services provided by a CSP to a CSC.

The primary CSP utilizes a peer service integration functional component to connect to a secondary CSP. The primary CSP manages inter-cloud services by using a peer service management functional

component along with the integration, BSSs, operations support system (OSS) and security systems functional components of a secondary CSP.

No functional extensions are needed for the user layer, access layer, service layer, resource layer and development function. As highlighted by the dark grey colour in Figure 6-5, this Recommendation identifies inter-cloud specific extensions to functional components [ITU-T Y.3502] that are part of integration, security systems, OSS and BSSs. Functional components in other parts of the architecture, i.e. user layer, access layer service layer, resource layer and multi-layer development functions, are reused without modification in the inter-cloud functional architecture.

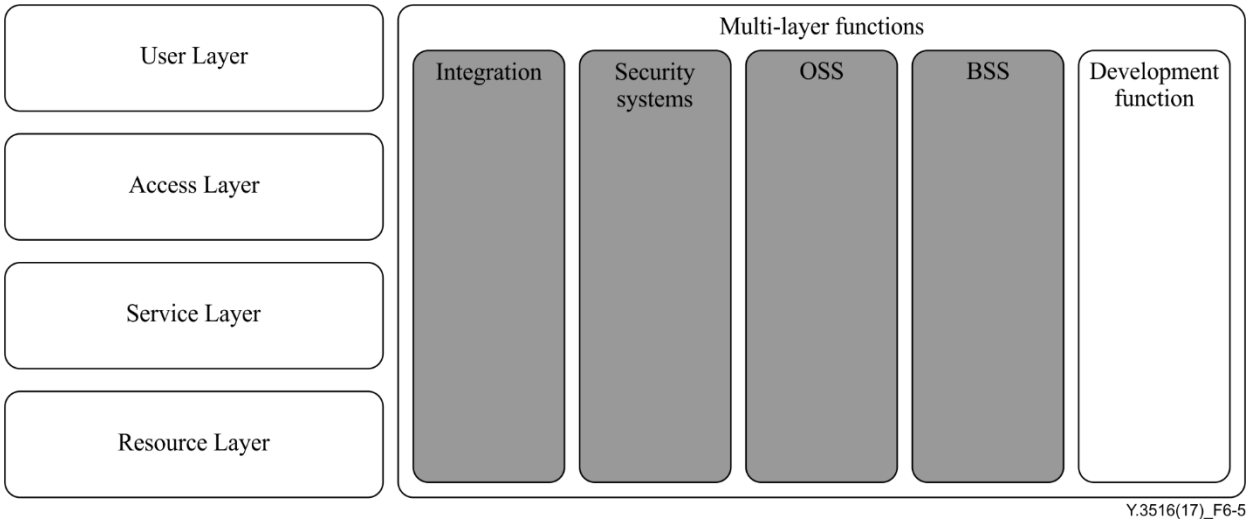

Figure 6-5 – Functional components extended with inter-cloud computing functions

7 Functions of inter-cloud computing

As shown in Figure 6-5, the inter-cloud functions only cover extensions to BSSs, OSS, integration and security systems. The inter-cloud functions are as follows:

– BSS functions, including service subscription management and billing.

– OSS functions, including service catalogue, service provisioning, monitoring and reporting, service policy management, service level management, incident and problem management and peer service management.

– Integration functions, including peer CSP management, inter-cloud service negotiation, inter-cloud service discovery, inter-cloud service selection, inter-cloud service reservation, inter-cloud service release and inter-cloud capabilities adaptation.

– Security systems functions, including authentication and identity management, authorization and security policy management and encryption management.

7.1 Business support systems

7.1.1 Service subscription management

The service subscription management function handles the subscription of the CSP to services provided by peer CSPs as well as subscription of peer CSPs to its own services.

This function includes the following.

– Service subscription management. This allows for managing, e.g., creating, modifying, updating, deleting and querying inter-cloud service subscription between peer CSPs.

7.1.2 Billing

The billing function generates service charging and invoice for inter-cloud services.

This function includes the following.

– Service charging. This allows for rating the usage of an inter-cloud service based on metering data of the particular inter-cloud service.

– Service invoice generation. This allows generating inter-cloud service invoice and delivering the invoices to peer CSPs.

7.2 Operational support systems

7.2.1 Service catalogue

The service catalogue function includes service catalogue synchronization and life-cycle management with peer CSPs.

This function includes the following.

– Service catalogue synchronization. This allows for periodically or on-demand exchange of service catalogue information for inter-cloud services.

– Service catalogue lifecycle management. This allows managing, e.g., creating, modifying, deleting and querying content of the service catalogue of the peer CSP for inter-cloud services. Service catalogue life-cycle management includes publishing catalogue content information allowing peer CSPs to consult and select inter-cloud services.

7.2.2 Service provisioning

The provisioning function allows for the provisioning of inter-cloud services provided by peer CSPs.

This function includes the following.

– Service deployment. This allows creating inter-cloud service instances based on the inter-cloud service template defined in the service catalogue, and delivery of inter-cloud service instances deployment requests to related peer CSPs.

– Service configuration and lifecycle management. This allows accessing and configuring deployed inter-cloud service instances as well as managing the lifecycle of deployed inter-cloud service instances.

NOTE – Service lifecycle management includes inter-cloud service creation, scaling, update and termination. For more details about end-to-end cloud service lifecycle management, refer to [ITU-T Y.3522].

7.2.3 Monitoring and reporting

The monitoring and reporting functions monitor inter-cloud services and provide monitoring reports to peer CSPs.

This function includes the following.

– Service monitoring. This allows for providing inter-cloud service metrics to peer CSPs periodically or on a request basis.

  NOTE – Inter-cloud service metrics are tracked for the purpose of meeting the inter-cloud service availability contributing to SLAs.

– Monitoring information exchanging and reporting. This allows for exchanging, recording and reporting of inter-cloud services monitoring information for peer CSPs.

7.2.4 Service policy management

The service policy management function includes lifecycle management and provisioning policy negotiation.

This function includes the following.

– Service policy lifecycle management. This allows for defining, modifying, storing and retrieving of inter-cloud service policies.

  NOTE – Inter-cloud service policy refers to an inter-cloud SLA, disaster recovery mechanism, auto-scale, inter-cloud service switchover and switchback.

– Service provisioning policy negotiation. This allows for inter-cloud service provisioning policy comparison, transformation and confirmation between peer CSPs.

7.2.5 Service automation

The service automation function delivers inter-cloud services automatically, including the management and execution of service templates and the orchestration of services.

This function includes the following.

– Service provisioning automation. This allows automation of workflows to realize inter-cloud service deployment between peer CSPs, without manual operations.

  NOTE 1 – Typical use cases of service provision automation include: automatic recovery, scale-in and scale-out, switchover and switchback of cloud services with peer CSPs.

– Service configuration automation. This allows automation of workflows to realize automated inter-cloud service configuration, without manual operations.

  NOTE 2 – Service provisioning and configuration automation allows for policy-based automated workflows for inter-cloud services.

7.2.6 Service level management

The service level management function manages the service levels of a particular inter-cloud service to meet the requirements of the SLA.

This function includes the following.

– SLA negotiation. This allows for negotiating inter-cloud service level information, e.g., capacity, performance, between peer CSPs.

– Service level tracking. This allows for measuring and recording of key performance indicators (KPIs) of inter-cloud service between peer CSPs according to the monitoring results.

– Service performance management. This allows for adjusting of particular inter-cloud service performance based on service performance tracking results to meet the requirements of the SLA.

– Service capacity management. This allows for identifying of current or potential capacity bottlenecks by comparing the allocated inter-cloud service capacity with KPIs, and planning inter-cloud service capacity to meet the requirements of the SLA.

7.2.7 Incident and problem management

The incident and problem management function detects and reports inter-cloud incidents and problems.

This function includes the following.

– Incident and problem detection. This allows for capturing of inter-cloud incidents or problems between peer CSPs.

– Incident and problem reporting. This allows for providing and exchanging of inter-cloud incident or problem reports to peer CSPs.

7.2.8 Peer service management

The peer service management function allows for connecting of OSS and BSSs of a peer CSP, by adapting an inter-cloud management application programming interface (API).

This function includes:

– Inter-cloud connection management. This allows for managing of connectivity with peer CSPs involved in an inter-cloud relationship.

– Access of the BSSs of a peer CSP. This allows for accessing to the inter-cloud BSSs of peer CSP with appropriate identity and credentials to provide business capabilities. The identity and credentials are provided by inter-cloud security (see clause 7.4). The functions of inter-cloud BSSs can be found in clause 7.1.

– Access to the OSS of a peer CSP. This allows for accessing to the inter-cloud OSS of a peer CSP with appropriate identity and credentials to provide administration capabilities. The identity and credentials are provided by inter-cloud security (see clause 7.4). The functions of an inter-cloud OSS can be found in clause 7.2.

– Inter-cloud management API adaptation. This allows for adapting of an inter-cloud BSS- and OSS-related API from a peer CSP.

7.3 Peer service integration

7.3.1 Peer CSP management

The peer CSP management function supports discovery of peer CSPs, negotiation with peer CSPs, primary CSP role delegation, primary CSP switchover and switchback.

This function includes the following.

– Peer CSP discovery. This allows for exchanging of available inter-cloud service and resource information between peer CSPs with peering, federation and intermediary patterns.

– Negotiation with peer CSPs. This allows for performing of API negotiation, SLA negotiation and policy negotiation between peer CSPs.

NOTE 1 – API negotiation mainly deals with the API format, protocol, and content.

NOTE 2 – SLA negotiation deals with the different inter-cloud service quality between peer CSPs.

NOTE 3 – Policy negotiation with peer CSPs deals with policies that apply to inter-cloud services. Policies can include business, technical, security, privacy and certification policies that apply to inter-cloud services and their usage by peer CSPs.

– Primary CSP role delegation. This allows for identifying of peer CSPs that are capable of inheriting the primary CSP role with peering, federation and intermediary inter-cloud patterns. This allows negotiating with the peer CSPs identified as to whether they can accept the inheritance and also allows for delegating of one of the peer CSPs identified to take the role of primary CSP.

– Primary CSP switchover and switchback. This allows for switchover of CSC access to a peer CSP (acting as primary CSP) without service interruption for that CSC. This allows the CSC to use services in a similar manner to the way they did before the access was switched over. This also allows for switching back on CSC access to the primary CSP when this CSP has recovered from the reasons that led to the switchover (e.g., a fault or load distribution).

NOTE 4 – Switchover conditions include load distribution between CSPs, in which the primary CSP role is maintained as it is; and fault cases, in which the primary CSP role is delegated to the peer CSP (see clause 9.6 of [ITU-T Y.3511]).

NOTE 5 – The mechanism of switchover and switchback of a primary CSP can be a policy-based process.

7.3.2 Inter-cloud service negotiation

The inter-cloud service negotiation function negotiates inter-cloud service information, quality of service (QoS), and performance estimation and selection policy between peer CSPs.

This function includes the following.

– Inter-cloud service information negotiation. This allows for negotiation of inter-cloud service information between peer CSPs. Inter-cloud inter-working can only start when inter-cloud service information negotiation is finalized and the inter-cloud service is available.

NOTE – The inter-cloud service information includes: inter-cloud service provider, inter-cloud service identifier, inter-cloud service type, inter-cloud service status (available, reserved, allocated, released), inter-cloud service priority (high, medium, normal, low).

– Inter-cloud service performance negotiation. This allows a primary CSP to negotiate with peer CSPs in order to guarantee inter-cloud service performance that satisfies inter-cloud service SLAs.

– Inter-cloud service performance estimation and selection policy negotiation. This allows for negotiating of inter-cloud service performance estimation and selection policies associated with peer CSPs.

7.3.3 Inter-cloud service discovery

The inter-cloud service discovery function discovers available particular inter-cloud services between peer CSPs.

This function includes the following.

– Inter-cloud service discovery. This allows for discovering of available particular inter-cloud services provided by peer CSPs that meet the requirements of an inter-cloud service SLA.

7.3.4 Inter-cloud service selection

The inter-cloud service selection function allows a primary CSP to match and identify a specified inter-cloud service.

This function includes the following.

– Inter-cloud service matching. This allows a primary CSP to find out about available inter-cloud services by matching inter-cloud service SLAs and inter-cloud service monitoring information.

– Inter-cloud service identification. This allows for selecting of appropriate inter-cloud services based on the matching result. The identification of the inter-cloud service selected, as the acknowledgement of the inter-cloud selection, is used to reserve an inter-cloud service by a primary CSP.

7.3.5 Inter-cloud service reservation

The inter-cloud service reservation function allows a primary CSP to create, update and release reserved inter-cloud service and its attached resource.

This function includes the following.

– Inter-cloud reserved service creation. This allows a primary CSP to reserve an inter-cloud service and its attached resources from other peer CSPs. The acknowledgement is sent between peer CSPs as confirmation of the creation.

– Inter-cloud reserved service updated. This allows a primary CSP to update the inter-cloud reserved service and its attached resources from other peer CSPs. The acknowledgement is sent between peer CSPs as confirmation of the update.

– Inter-cloud reserved service released. This allows a primary CSP to release an inter-cloud reserved service and its attached resources from other peer CSPs. The acknowledgement is sent between peer CSPs as confirmation of the release.

7.3.6 Inter-cloud service release

The inter-cloud service release function allows for releasing of a reserved and allocated inter-cloud service and return of its attached resources to peer CSPs.

This function includes the following.

– Inter-cloud reserved service release. This allows for releasing of an issued inter-cloud service reservation and return of its attached resources to peer CSPs.

– Inter-cloud allocated service release. This allows for de-allocating and terminating of the allocated inter-cloud service and return of its attached resources to peer CSPs.

7.3.7 Inter-cloud capabilities adaptation

The inter-cloud capabilities adaptation function allows for adapting inter-cloud service API from peer CSPs.

This function includes the following.

– Inter-cloud service API adaptation. This allows for adapting of an inter-cloud service API from peer CSPs. The format of an inter-cloud service API provided by peer CSPs is transformed into a primary CSP's own API by utilizing inter-cloud capabilities adaptation.

7.4 Security systems

7.4.1 Authentication and identity management

The authentication and identity management function provides authentication of and identities for peer CSPs.

This function includes the following.

– Federated identity management. This allows for using of federated identity management to permit peer CSPs to employ the same identity and credentials to access inter-cloud services.

7.4.2 Authorization and security policy management

The authorization and security policy management function controls and applies authorization for peer CSPs to access a specific inter-cloud service.

This function includes the following.

– Authorization management. This allows for implementing of permissions and authorization for particular peer CSPs and related inter-cloud services.

– Federated authorization and security policy management. This allows for providing of federated authorization and security policy management between peer CSPs.

– Trust management. This allows for encapsulating and verifying of the policies for trusted inter-cloud.

NOTE – For more information about trusted inter-cloud please refer to [ITU-T Y.3514].

7.4.3 Encryption management

The encryption management function provides data encryption, API encryption, as well as network connectivity encryption.

This function includes the following.

– Data encryption. This allows for encrypting of data exchanged through inter-cloud services.

– API encryption. This allows for encrypting of inter-cloud service and management APIs for peer CSPs.
– Network connectivity encryption. This allows for utilizing of security keys to secure the network connectivity between CSPs.

8 Functional components of inter-cloud

Figure 8-1 illustrates the mapping of inter-cloud functions and functional components.

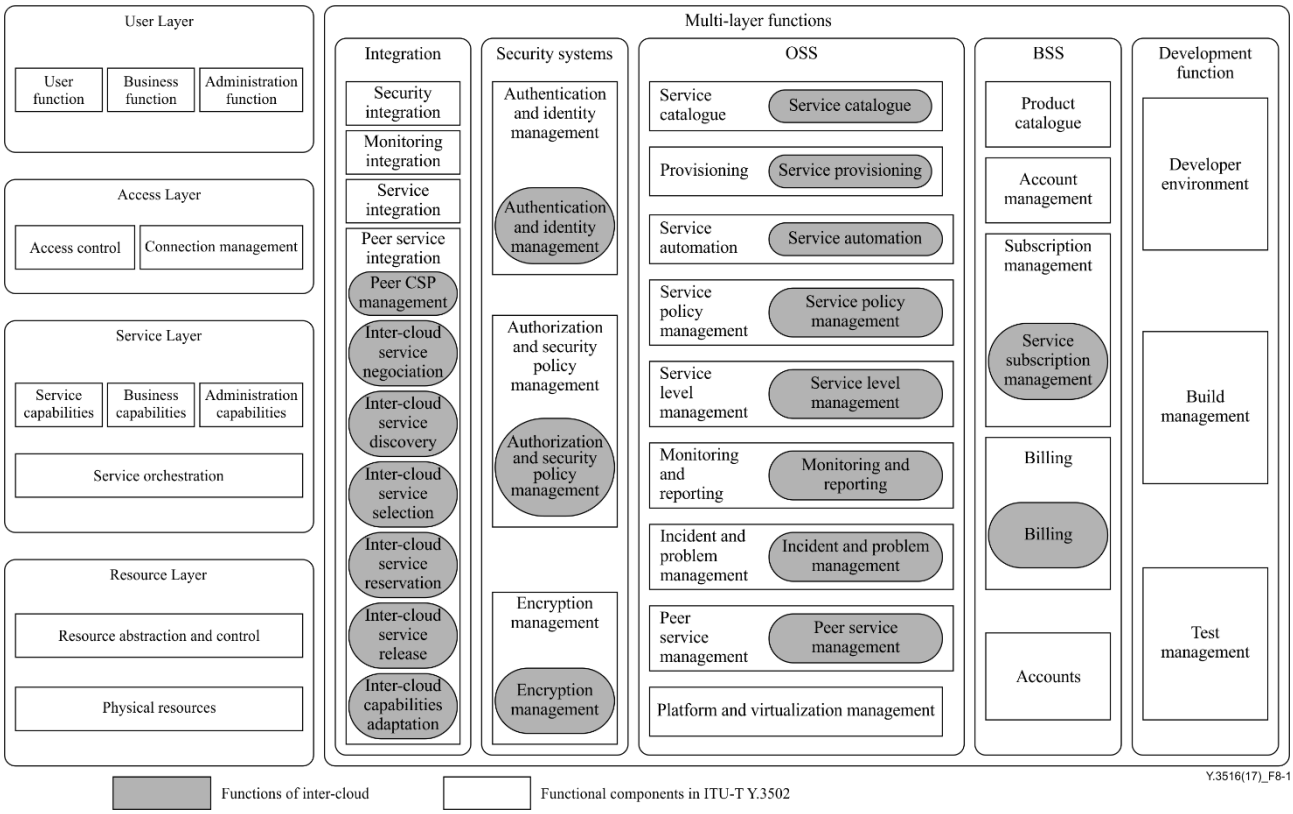

Figure 8-1 – Mapping of inter-cloud functions and functional components

The inter-cloud functions identified in clause 7 are mapped to functional components in [ITU-T Y.3502]. No new functional components are defined. However, functions of some functional components are extended for inter-cloud as follows.

– Business support systems
  - Service subscription management functional component is extended with service subscription management function for inter-cloud as described in clause 7.1.1.
  - Billing functional component is extended with billing function for inter-cloud as described in clause 7.1.2.
– Operational support systems
  - Service catalogue functional component is extended with service catalogue function for inter-cloud as described in clause 7.2.1.
  - Provisioning functional component is extended with service provisioning function for inter-cloud as described in clause 7.2.2.
  - Monitoring and reporting functional component is extended with monitoring and reporting function for inter-cloud as described in clause 7.2.3.

- Service policy management functional component is extended with service policy management function for inter-cloud as described in clause 7.2.4.
- Service automation functional component is extended with service automation function for inter-cloud as described in clause 7.2.5.
- Service level management functional component is extended with service level management function for inter-cloud as described in clause 7.2.6.
- Incident and problem management functional component is extended with incident and problem management function for inter-cloud as described in clause 7.2.7.
- Peer service management functional components is extended with peer service management function for inter-cloud as described in clause 7.2.8.

– Peer service integration
  - Peer service integration functional component is extended with peer CSP management function as described in clause 7.3.1.
  - Peer service integration functional component is extended with inter-cloud service negotiation as described in clause 7.3.2.
  - Peer service integration functional component is extended with inter-cloud service discovery function as described in clause 7.3.3.
  - Peer service integration functional component is extended with inter-cloud service selection function as described in clause 7.3.4.
  - Peer service integration functional component is extended with inter-cloud service reservation function as described in clause 7.3.5.
  - Peer service integration functional component is extended with inter-cloud service release function as described in clause 7.3.6.
  - Peer service integration functional component is extended with inter-cloud capabilities adaptation function as described in clause 7.3.7.

– Security systems
  - Authentication and identity management functional component is extended with authentication and identity management function for inter-cloud as described in clause7.4.1.
  - Authorization and security policy management functional component is extended with authorization and security policy management function for inter-cloud as described in clause 7.4.2.
  - Encryption management functional component is extended with encryption management function for inter-cloud as described in clause 7.4.3.

9 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. In addition, clause 7 of this Recommendation identifies the inter-cloud security related functions.

Appendix I

Mapping of inter-cloud computing functional requirements and functions

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

This appendix aims to describe the mapping of inter-cloud computing functional requirements specified in [ITU-T Y.3511] and inter-cloud functions in clause 7 of this Recommendation.

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		**Inter-cloud functions in this Recommendation**
9.1 SLA and policy negotiation	The SLA and policy negotiation capability is required to be aware of the SLA information related to the QoS and performance aspects of the CSPs involved in the inter-cloud using standard formats.	– 7.3.1 Peer CSP management – 7.2.4 Service policy management – 7.2.6 Service level management – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow describing and expressing of the resource information (e.g., resource type, configuration and status) in a standard manner in order to be able to monitor these resources across multiple CSPs.	– 7.2.8 Peer service management – 7.3.2 Inter-cloud service negotiation – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow updating of the resource information across multiple CSPs in synchronization with the events (e.g., reserve or release of resources) involving the CSPs.	– 7.2.8 Peer service management – 7.2.3 Monitoring and reporting – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow periodically, or on a request basis, collecting of information about the usage and performance status of the resources of multiple CSPs.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.2 Inter-cloud service negotiation – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow periodically, or on a request basis, collecting of information about the resource availability (e.g., dead or alive status of machines) of multiple CSPs.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow exchange of monitoring information in commonly defined ways across multiple CSPs.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.3 resource performance estimation and selection	The resource performance estimation and selection capability deals with the selection of resources from the candidate resources that have already been reserved in peer CSPs. This capability estimates the achievable performance of available reserved	– 7.2.8 Peer service management – 7.3.4 Inter-cloud service selection – 7.3.7 Inter-cloud capabilities adaptation

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		Inter-cloud functions in this Recommendation
	resources and assists the CSP in the selection of resources to be effectively used.	
9.4 resource discovery and reservation	Allow finding of available resources in the peer CSPs based on different priorities. Allow reservation of available resources in the peer CSPs on the basis of different priorities	– 7.3.2 Inter-cloud service negotiation – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Enable discovery of resources available in the peer CSPs.	– 7.3.3 Inter-cloud service discovery – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow the reservation of discovered resources in the peer CSPs.	– 7.3.5 Inter-cloud service reservation – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow provisional reservation of discovered resources, i.e., to keep the resources to be used (as candidates), for later acknowledgement (for some of them) or release (for others).	– 7.3.5 Inter-cloud service reservation – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow finding of available resources in the peer CSPs based on different priorities.	– 7.3.3 Inter-cloud service discovery – 7.3.4 Inter-cloud service selection – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow reservation of available resources in the peer CSPs on the basis of different priorities	– 7.3.5 Inter-cloud service reservation – 7.3.4 Inter-cloud service selection – 7.3.7 Inter-cloud capabilities adaptation
9.5 resource set-up and activation	The resource set-up and activation capability deals with the set up and activation of reserved resources in the peer CSPs. This includes connecting to the peer CSPs via networks, remotely activating (i.e., invoking) software and transferring or copying data to enable the use of resources in the peer CSPs.	– 7.2.2 Service provisioning – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.5 resource set-up and activation	Allow the establishment of reserved resources in a peer CSP.	– 7.2.2 Service provisioning – 7.3.7 Inter-cloud capabilities adaptation
9.5 resource set-up and activation	Allow accessing to the configuration and policy settings of reserved resources in the peer CSPs.	– 7.2.2 Service provisioning – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		Inter-cloud functions in this Recommendation
9.6 cloud services switchover and switchback	Allow switching over of CSC end-user access to a peer CSP (acting as primary CSP) without manual operation from the CSC, in order to allow the CSC end user to use services in a similar manner to the way they did before the access was switched over. Allow switching back of CSC end-user access to the primary CSP when this CSP has recovered from the reasons that led to the switchover (e.g., a disaster or load distribution between peer CSPs is no longer needed).	– 7.3.1 Peer CSP management – 7.2.7 Incident and problem management – 7.2.5 Service automation – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.7 resource release	Allow updating of the peer CSP resource configuration information.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.7 resource release	Allow releasing by the CSP of resources reserved, activated or set up in the peer CSPs.	– 7.3.6 Inter-cloud service release – 7.3.7 Inter-cloud capabilities adaptation
9.8 CSC information exchange	Be able to manage CSC profiles and associated information. Be able to exchange CSC profiles and associated information 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.	– 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.9 primary CSP role delegation	Allow a CSP to discover peer CSPs that are capable of inheriting the primary CSP role, and enable the CSP to negotiate with these peer CSPs as to whether they can accept the inheritance.	– 7.3.1 Peer CSP management – 7.3.7 Inter-cloud capabilities adaptation
9.9 primary CSP role delegation	Allow a CSP to transfer its management information associated with the primary CSP role in a reliable manner (e.g., periodically) to the peer CSPs that have accepted the permission transfer with that CSP.	– 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.9 primary CSP role delegation	Allow the controllability of the information associated with the primary CSP role to be transferred to the secondary CSPs with minimum interruptions.	– 7.1.1 Service subscription management – 7.1.2 Billing – 7.3.1 Peer CSP management

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		Inter-cloud functions in this Recommendation
	Allow a CSP to cancel the permission transfer arrangements.	– 7.2.5 Service automation – 7.3.7 Inter-cloud capabilities adaptation
9.10 inter-cloud service handling	Support service intermediation, i.e., conditioning or enhancing the cloud service of a peer CSP. Support service aggregation, i.e., providing the composition of a set of services provided by the CSPs. Support service arbitrage, i.e., selecting one service offering from a group offered by the peer CSPs.	– 7.2.8 Peer service management – 7.2.1 Service catalogue – 7.2.5 Service automation – 7.3.7 Inter-cloud capabilities adaptation

Appendix II

Reference points of inter-cloud computing

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

As described in this Recommendation, inter-cloud functional architecture reuse the functional components of [ITU-T Y.3502] and extends BSS, OSS, integration and security system functional components with inter-cloud functions. Given no detailed interactions and reference points have been defined in [ITU-T Y.3502] between functional components, this appendix provides examples of inter-cloud related reference points for informative purposes.

The reference points of inter-cloud computing architecture are shown in Figure II.1.

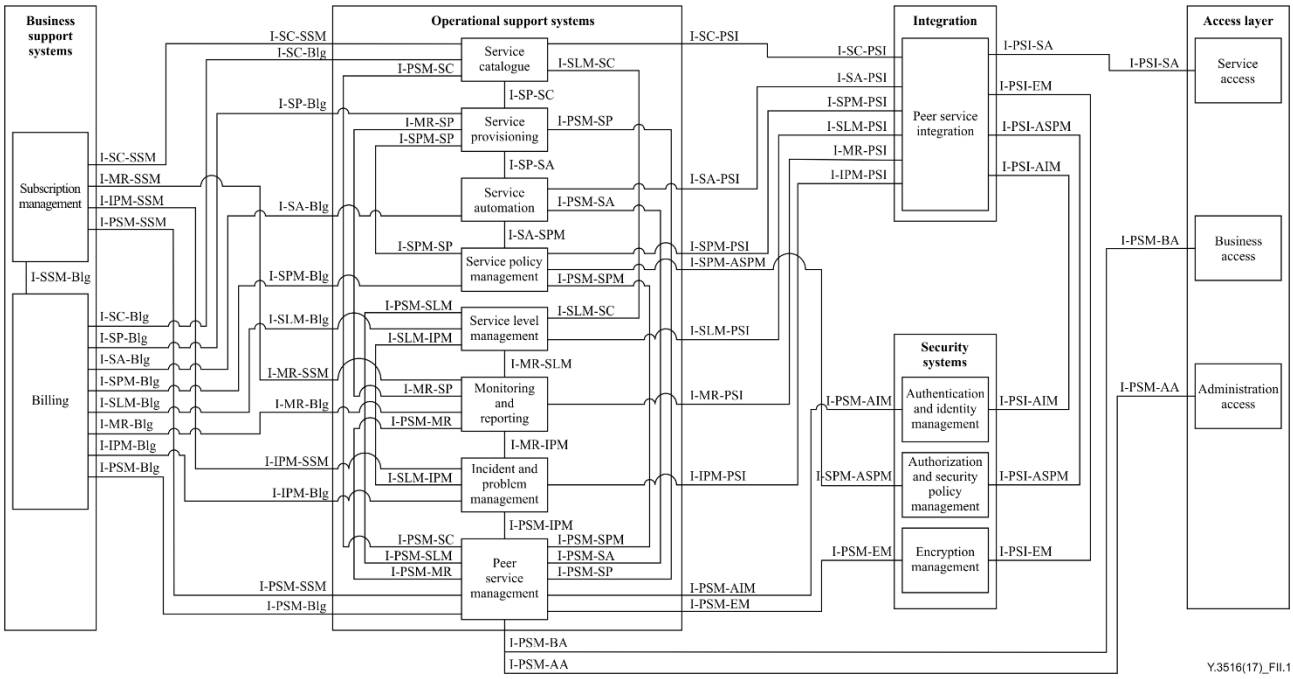

Figure II.1 – Reference points of inter-cloud computing architecture

II.1 Reference point: I-SSM-Blg

The subscription management functional component interacts with billing functional component through I-SSM-Blg to provide inter-cloud service subscription information for billing.

II.2 Reference point: I-SSM-IPM

The subscription management functional component interacts with incident and problem management functional component through I-SSM-IPM to synchronize inter-cloud incident- and problem-detecting and reporting information.

II.3 Reference point: I-SSM-MR

The subscription management functional component interacts with monitoring and reporting functional component through I-SSM-MR to get the monitoring information of inter-cloud services of different inter-cloud service subscriptions.

II.4 Reference point: I-SSM-SC

The subscription management functional component interacts with service catalogue functional component through I-SSM-SC to synchronize inter-cloud service catalogue information.

II.5 Reference point: I-SSM-PSM

The subscription management functional component interacts with peer service management functional component through I-SSM-PSM to access the BSSs of a peer CSP for subscription.

II.6 Reference point: I-Blg-IPM

The billing functional component interacts with incident and problem management functional component through I-Blg-IPM to get inter-cloud incident and problem information for billing.

II.7 Reference point: I-Blg-MR

The billing functional component interacts with monitoring and reporting functional component through I-Blg-MR to get inter-cloud service monitoring information for billing.

II.8 Reference point: I-Blg-SC

The billing functional component interacts with service catalogue functional component through I-Blg-SC to get inter-cloud service catalogue information for billing.

II.9 Reference point: I-Blg-SP

The billing functional component interacts with service provisioning functional component through I -Blg-SP to get inter-cloud service provisioning information for billing.

II.10 Reference point: I-Blg-SA

The billing functional component interacts with service automation functional component through I-Blg-SA to get inter-cloud service automation information for billing.

II.11 Reference point: I-Blg-SPM

The billing functional component interacts with service policy management functional component through I-Blg-SPM to get inter-cloud service policy information for billing.

II.12 Reference point: I-Blg-SLM

The billing functional component interacts with service level management functional component through I-Blg-SLM to get inter-cloud service level information for billing.

II.13 Reference point: I-Blg-PSM

The billing functional component interacts with service level management functional component through I-Blg-PSM to exchange with peer CSP's billing.

II.14 Reference point: I-SP-SC

The service catalogue functional component interacts with service provisioning functional component through I-SP-SC to provision inter-cloud service by using inter-cloud service templates.

II.15 Reference point: I-SLM-SC

The service catalogue functional component interacts with service level management functional component through I-SLM-SC to exchange service level information.

II.16 Reference point: I-PSM-SC

The service catalogue functional component interacts with peer service management functional component through I-PSM-SC to access the inter-cloud service catalogue of a peer CSP.

II.17 Reference point: I-SC-PSI

The service catalogue functional component interacts with peer service integration functional component through I-SC-PSI to provide inter-cloud service integration information.

II.18 Reference point: I-SPM-SP

The service provisioning functional component interacts with service policy management functional component through I-SPM-SP to get inter-cloud service provisioning policy information.

II.19 Reference point: I-SP-SA

The provisioning functional component interacts with service automation functional component through I-SP-SA to provision inter-cloud service automatically.

II.20 Reference point: I-PSM-SP

The provisioning functional component interacts with peer service management functional component through I-PSM-SP to access the OSS of a peer CSP in order to provision inter-cloud service among peer CSPs.

II.21 Reference point: I-MR-SP

The provisioning functional component interacts with monitoring and reporting functional component through I-MR-SP to exchange inter-cloud monitoring and provision information.

II.22 Reference point: I-PSM-SA

The service automation functional component interacts with peer service management functional component through I-PSM-SA to access peer CSP's OSS in order to delivers inter-cloud service automatically.

II.23 Reference point: I-SA-SPM

The service automation functional component interacts with service policy management functional component through I-SA-SPM to get inter-cloud service provisioning policies and configuration policies.

II.24 Reference point: I-SA-PSI

The service automation functional component interacts with peer service integration functional component through I-SA-PSI to provide automation processing of primary CSP switchover and switchback.

II.25 Reference point: I-PSM-SPM

The service policy management functional component interacts with peer service management functional component through I-PSM-SPM to access the OSS of a peer CSP to manage inter-cloud service policy and negotiated provisioning policy.

II.26 Reference point: I-SPM-PSI

The service policy management functional component interacts with peer service integration functional component through I-SPM-PSI to negotiate inter-cloud service policy with peer CSPs.

II.27 Reference point: I-SPM-ASPM

The service policy management functional component interacts with authorization and security policy management functional component through I-SPM-ASPM to exchange inter-cloud security policy information.

II.28 Reference point: I-SLM-IPM

The service level management functional component interacts with incident and problem management functional component through I-SLM-IPM to get inter-cloud incident and problem information for inter-cloud service level tracking, performance and capacity management.

II.29 Reference point: I-PSM-SLM

The service level management functional component interacts with peer service management functional component through I-PSM-SLM to access the OSS of a peer CSP to manage the service levels of a particular inter-cloud service to meet the requirements of the inter-cloud SLA.

II.30 Reference point: I-MR-SLM

The service level management functional component interacts with monitoring and reporting functional component through I-MR-SLM to get inter-cloud monitoring information.

II.31 Reference point: I-SLM-PSI

The service level management functional component interacts with peer service integration functional component though I-SLM-PSI to negotiate inter-cloud service SLA with peer CSPs.

II.32 Reference point: I-MR-IPM

The monitoring and reporting functional component interacts with incident and problem management functional component through I-MR-IPM to exchange inter-cloud monitoring information for inter-cloud incident and problem management.

II.33 Reference point: I-PSM-MR

The monitoring and reporting functional component interacts with peer service management functional component through I-PSM-MR to access the OSS of a peer CSP for monitoring and reporting.

II.34 Reference point: I-MR-PSI

The monitoring and reporting functional component interacts with peer service integration functional component through I-MR-PSI to get inter-cloud services negotiation, discovery, selection, reservation and release information for monitoring.

II.35 Reference point: I-PSM-IPM

The incident and problem management functional component interacts with peer service management functional component through I-PSM-IPM to access the OSS of a peer CSP for inter-cloud incidents and problems management.

II.36 Reference point: I-IPM-PSI

The incident and problem management functional component interacts with peer service integration functional component through I-IPM-PSI to get inter-cloud integration information for incident and problem management.

II.37 Reference point: I-PSM-AIM

The peer service management functional component interacts with authentication and identity management functional component through I-PSM-AIM for peer CSP and inter-cloud service authenticate and identities.

II.38 Reference point: I-PSM-EM

The peer service management functional component interacts with encryption management functional component through I-PSM-EM to get data encryption and API encryption for peer CSPs.

II.39 Reference point: I-PSM-BA

The peer service management functional component interacts with the business access functional component of a peer CSP through I-PSM-BA to access the business capabilities of a peer CSP.

II.40 Reference point: I-PSM-AA

The peer service management functional component interacts with the administration access functional component of a peer CSP through I-PSM-AA to access the administration capabilities of a peer CSP.

II.41 Reference point: I-PSI-AIM

The peer service integration functional component interacts with authentication and identity management functional component through I-PSI-AIM to provide authentication and identities for inter-cloud service integration.

II.42 Reference point: I-PSI-ASPM

The peer service integration functional component interacts with authorization and security policy management functional component through I-PSI-ASPM to apply authorization for peer CSPs to access inter-cloud services.

II.43 Reference point: I-PSI-EM

The peer service integration functional component interacts with encryption management functional component through I-PSI-EM to get API encryption function for peer CSPs.

II.44 Reference point: I-PSI-SA

The peer service integration functional component interacts with peer CSP's service access functional component through I-PSI-SA to access the services of a peer CSP.

Bibliography

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

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017