International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3514

Corrigendum 1

(12/2018)

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

Cloud Computing

Cloud computing – Trusted inter-cloud computing framework and requirements

Corrigendum 1

Recommendation ITU-T Y.3514 (2017) – Corrigendum 1

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.3514

Cloud computing – Trusted inter-cloud computing framework and requirements

Corrigendum 1

Summary

Recommendation ITU-T Y.3514 specifies a framework of trusted inter-cloud computing and relevant use cases. It provides general requirements for trusted inter-cloud and specific ones related to governance, management, resiliency, security and confidentiality of trusted inter-cloud.

Corrigendum 1 replaces the definition of dependability.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3514	2017-05-22	13	11.1002/1000/13254
1.1	ITU-T Y.3514 (2017) Cor. 1	2018-12-14	13	11.1002/1000/13813

Keywords

Cloud computing, confidentiality, governance, inter-cloud, management, resiliency, security, trust.

[*] 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.3514

Cloud computing – Trusted inter-cloud computing framework and requirements

Corrigendum 1

Editorial note: This is a complete-text publication. Modifications introduced by this corrigendum are shown in revision marks relative to Recommendation ITU-T Y.3514 (2017).

1 Scope

This Recommendation specifies a framework of trusted inter-cloud computing and relevant use cases, based on the framework of inter-cloud computing [ITU-T Y.3511]. The scope of this Recommendation includes:

- an overview of trusted inter-cloud computing;
- general requirements for trusted inter-cloud;
- requirements for governance of trusted inter-cloud;
- requirements for management of trusted inter-cloud;
- requirements for resiliency of trusted inter-cloud;
- requirements for security and confidentiality of trusted inter-cloud.

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 (2014), *Security framework for cloud computing.*

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

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

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

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

[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 availability [ITU-T Y.3500]: Property of being accessible and usable upon demand by an authorized entity.

3.1.2 confidentiality [ITU-T Y.3500]: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

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

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

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

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

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

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

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

3.1.8 dependability [ITU-T L.1202], [ITU-T E.800]: The collective term used to describe the availability performance and its influencing factors on reliability performance, maintainability performance and maintenance support performance.

3.1.9 governance [b-ISO/IEC 38500:2015]: System of directing and controlling.

3.1.~~9~~10 information security [b-ISO/IEC 27000:2016]: Preservation of confidentiality, integrity and availability of information.

NOTE – In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

3.1.11~~0~~ integrity [ITU-T Y.3500]: Property of accuracy and completeness.

3.1.12~~1~~ 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.

3.1.13~~2~~ service level agreement [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

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

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

3.1.14~~3~~ service management interface [ITU-T Y.3521]: Interface that provides a set of management capabilities exposed by a cloud service through which the cloud service can be managed.

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

3.1.15~~4~~ trusted cloud service [ITU-T Y.3501]: A cloud service that satisfies a set of requirements such as transparency for governance, management and security so that a cloud service customer (CSC) can be confident in using the cloud service.

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

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

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

~~**3.2.1 dependability**: The availability performance and its influencing factors on reliability performance, maintainability performance and maintenance support performance.~~

3.2.~~2~~1 inter-cloud governance: System by which the use of inter-cloud is directed and controlled.

3.2.2~~3~~ reliability: The ability of a system, product or component to perform and maintain under stated conditions as required for a specified period of time.

3.2.3~~4~~ resiliency: The ability of a system, product or component to provide, maintain, or return to an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
BSS	Business Support System
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
KPI	Key Performance Indicator
MSA	Master Service Agreement
NaaS	Network as a Service
NAT	Network Address Translation
NFV	Network Functions Virtualization
OSS	Operations Support System
PaaS	Platform as a Service
PII	Personally Identifiable Information
QoS	Quality of Service
SaaS	Software as a Service
SDN	Software-Defined Networking
SLA	Service Level Agreement
SMI	Service Management Interface
vFW	Virtual Firewall

vHGW	Virtual Home Gateway
vLB	Virtual Load Balancer
vNAT	Virtual Network Address Translation

5 Conventions

In this Recommendation:

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

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

6 Overview of trusted inter-cloud

The inter-cloud computing concept is based on the relationship (pattern) among multiple cloud service providers (CSPs). This pattern (peering, federation or intermediary) allows the CSP to interwork with one or more peer CSPs to assure intermediation and security of services provided by these CSPs.

The trusted inter-cloud relationship among multiple CSPs relies on confidence between cloud service customer (CSC) and CSP, or between CSPs. One of them has to delegate physical control over application, service, resource and data to the others. The appropriate security mechanisms (e.g., security access control, security of network connectivity between the CSPs) are needed during peer CSPs interactions to achieve trusted inter-cloud computing.

The relevant CSPs form a common trusted inter-cloud to establish a trust relationship between them. In particular, the multiple CSPs involved in inter-cloud may be administered by different parties. In case of an inter-cloud federation, the involved CSPs may establish trust relationships among them prior to any interactions between them or during inter-cloud interactions (e.g., service requests between CSPs).

The specifics of trusted inter-cloud computing are different depending on the technologies used by CSC or CSP. Therefore, the management of trusted inter-cloud takes into account different levels of security.

Trusted inter-cloud relationships can be expressed through cross-cutting aspects (identified in [ITU-T Y.3502]), such as the **governance, management, resiliency** and **security** of inter-cloud.

Trusted inter-cloud computing covers security threats for CSC and threats for CSP. The specific threats depend on the level of responsibilities and control between the CSC and CSP, or between CSPs (such as those identified in [ITU-T X.1601]). In trusted inter-cloud systems, the control can be exchanged between CSC and CSP or between CSPs to achieve security continuum. The **security** of inter-cloud can be realized based on:

a) self-service security which enables self-service management of security in heterogeneous cloud infrastructures and provides flexible mechanisms to let CSC or CSP control the security of their cloud computing resources in a fine-grained manner;

b) self-managed security which enables full automation of security management in order to reduce operational costs while adding more flexibility and providing a unified view of security in heterogeneous cloud computing environments;

c) end-to-end security which implements a distributed security abstraction layer between endpoints defined by the CSC to overcome the heterogeneity of security technologies across multi-cloud environments and to manage trust relationships between different layers and across CSPs, to provide a unified user experience of security.

The **governance** of inter-cloud means the system by which inter-cloud is directed and controlled. A governance system has to monitor and to control usage of cloud computing system in both horizontal (cross-provider) and vertical (cross-layer) dimensions with a high level of automation.

The **resiliency** of inter-cloud means the ability of multi-cloud environment to provide and to maintain an acceptable quality level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operations.

6.1 Governance of trusted inter-cloud

One of the main challenges in inter-cloud computing is to respect security, confidentiality, and compliance requirements of cloud services hosted in a multi-cloud environment. The governance aspects become key parts of service level agreements (SLAs) for cloud services as they allow for usage of cloud services in a transparent manner over all their lifecycle. The governance roles guarantee security and appropriate treatment of cloud applications and cloud data independently of the deployment model. They are specified and targeted for an operational area of cloud computing.

The governance of trusted inter-cloud is based on specific policies and principles which allow for the use of particular cloud services in a trustworthy manner. This needs strongly isolated (physically or logically) instances of cloud services for aspects including identity management, geographic redundancy, support for hybrid scenarios, and effective inter-cloud data (workloads) management. The CSPs establishing a trusted inter-cloud relationship are obliged to determine their policies of decision-making roles, and implement these policies in their management systems.

The governance of trusted inter-cloud can be expressed as a system of directing and controlling an inter-cloud environment to reach objectives for trust. It can be spread over the governance body and governance executive. The governance body consists of a set of representatives of CSPs (person or group of people) who are accountable for the performance and conformance of the trusted inter-cloud environment. The governance executive represents the system by which current and future use of trusted inter-cloud is directed and controlled. The governance executive also provides plans, builds and runs trusted inter-cloud enabled business.

The governance of trusted inter-cloud is a continuous process to monitor particular indicators from systems (e.g., performance, conformance), evaluate proposals and plans, and direct strategy and policies between the governance body and governance executive. The governance body takes into account external trusted inter-cloud conditions related to business pressures, regulatory obligations, source of authority, stake-holders' expectations and business needs.

The trusted inter-cloud governance is based on the following principles:

– responsibility, which indicates clearly defined roles for demand and support of the environment;

– strategy, which is strongly related to phase of plans, builds and runs trusted inter-cloud enabled business;

– acquisition of inter-cloud data, which depends on the business case;

– performance, which has to be realized according to SLAs for cloud services;

– compliance, which covers the necessary respect of laws and regulations;

– human behaviour, which addresses the dynamics of interaction in the governance process.

The governance of trusted inter-cloud can be considered with respect to internal or external aspects. Internal cloud governance allows a CSP to control its own processes in a way that it can give assurance and transparency to other CSPs participating in a trusted inter-cloud environment according to specified expectations in terms of cloud computing cross-cutting aspects [ITU-T Y.3502].

External cloud governance spans processes of monitoring and controlling the inter-cloud environment to reach objectives of trust. This can refer to a service level agreement which provides detailed information about functional and non-functional aspects of cloud services.

For both internal governance and external governance of trusted inter-cloud, these refer to matters that are decided by the governing board of a CSP, such as how policy decisions are made, and how these are converted into policies that can be implemented in the CSP's management system.

6.2 Management of trusted inter-cloud

Management in trusted inter-cloud computing environments is based on access control mechanisms and a trust management system. They are complementary to each other. Appropriate access control mechanisms guarantee a level of confidentiality and trust between a CSC and CSPs or between CSPs.

Access control mechanisms determine authorization of shifting physical control over applications, services, resources and data. An authorization, authentication and accounting (AAA) module to control the access to cloud computing resources relies on a customisable access control policy model and its implementation requirements. The specification of the access control mechanism is usually predefined in an access control policy. This specification is used to specify permissions and access control to cloud computing resources and cloud services.

The traditional access control mechanisms (e.g., identity-based, lattice-based, role-based, organisation-based, attribute-based) cannot be successfully used in trusted inter-cloud computing due to high dynamics in cloud computing environments. Therefore, new mechanisms based on mixing traditional functionality can be used to control cross-tenant at the policy administration level.

The objectives of access control mechanisms in trusted inter-cloud environment are as follows:

– expressivity as the ability to provide appropriate mechanisms of access control policies. This depends on the implementation;

– granularity as the ability to decompose an access control mechanism into smaller size components. This is in line with granularity of the cloud computing resources and cloud services as well as the SLA established between the CSC and CSP or between CSPs;

– context-awareness as the ability of an authorization mechanism to take context information into consideration when making access decisions. Context awareness is significant in trusted inter-cloud environments due to their distributed nature: access to inter-cloud from different locations, during different time periods, etc.

Appropriate policy language implemented in the trusted inter-cloud environment provides expressiveness beyond the boundary of access control. This should respect security mechanisms of trust management systems to fulfil specified requirements.

Trust management in inter-cloud environments (as an interaction enabler in situations of risk and uncertainty) is considered in cross-provider and cross-layer dimensions. Decisions of the trust management system are typically taken based on the prediction of cloud computing actors' behaviours and are based on the SLA established between CSC and CSP or between CSPs. According to particular needs, trust management can either be CSC-related or CSP-related.

The trust management functionalities are supported by the "Authorisation and security policy management" functional component within the multi-layer functions of the cloud computing reference architecture [ITU-T Y.3502]. The positioning of trust management functionalities across the CSPs which provide inter-cloud services is presented in Figure 6-1.

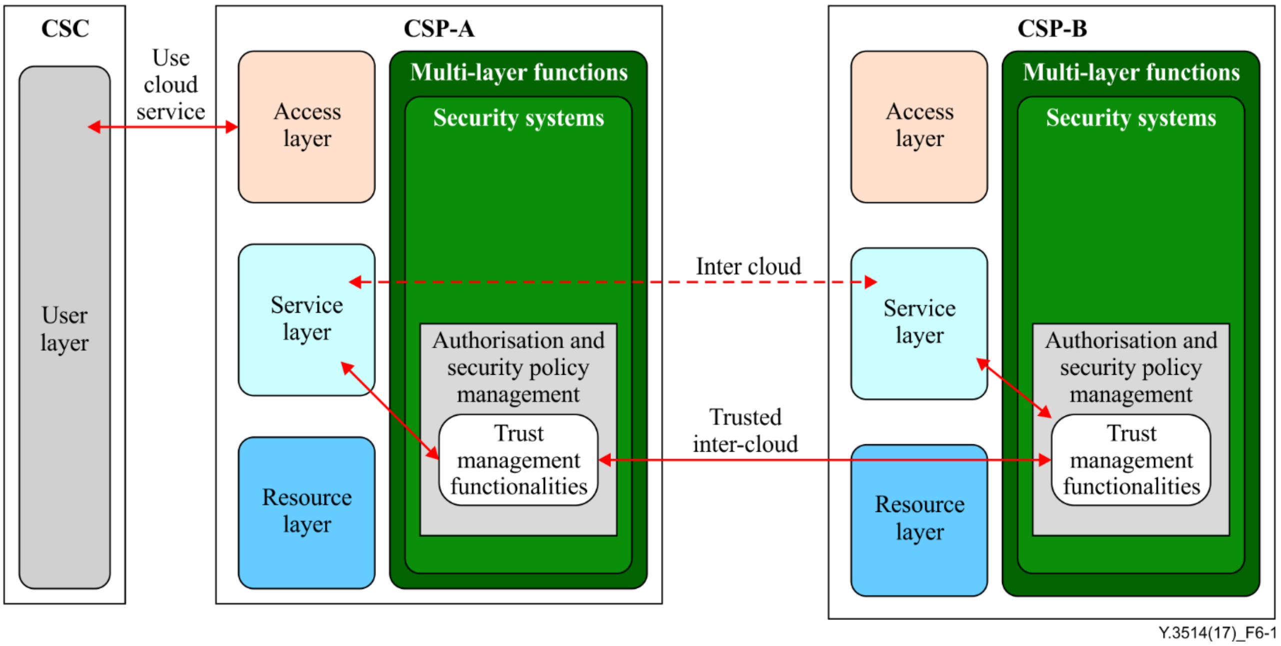


Figure 6-1 – The positioning of trust management functionalities over CSP in inter-cloud

The inter-cloud relation is realised over the particular service layers of CSP-A and CSP-B (dashed line in Figure 6-1). The trusted inter-cloud relation is realised over trust management functionalities of CSP-A and CSP-B located in the "Authorisation and security policy management" functional component, which is located within functionalities of inter-cloud security among CSPs (solid lines in Figure 6-1). The trust management functionalities play an intermediary role between service layers of CSP-A and CSP-B in inter-cloud relations.

The operational model of trust management identifies four modes as follows:

– Mode 1 – the trust management system produces simple answers (i.e., trust or no trust) that states whether the credentials provided by the CSP satisfy the policy;

– Mode 2 – extended Mode 1, with justification when the request is denied, that states which conditions in the policy the provided credentials were unable to satisfy;

– Mode 3 – the trust management system provides an answer with justifications and explanation when the policy is satisfied. The explanation contains all credentials that satisfy the policy;

– Mode 4 – extended Mode 3, with detailed explanation. The detailed explanation is obtained by providing all subsets of credentials that satisfy the policy.

The trust management functionalities are built upon elements as follows:

– **Feedback analyser** which is responsible for the collection and analysis of feedbacks and opinions from a CSC or CSP about another CSC or CSP;

– **SLA analyser** which is responsible for extracting and evaluating SLA metrics;

– **Credential analyser** which verifies chains of trust and evaluates the validity of credentials;

– **Trust requirement handler** which parses and extracts trust requirements;

– **Trust analyser** which encapsulates the policies used to compute trust;

– **Trust requests handler** which orchestrates and coordinates the collaboration of the aforementioned components.

For an overview of cloud SLA, cloud SLA metrics and the relationship between the cloud service agreement and the cloud SLA please refer to [b-ISO/IEC 19086-1].

The relationships between particular elements of trust management functionalities are presented in Figure 6-2.

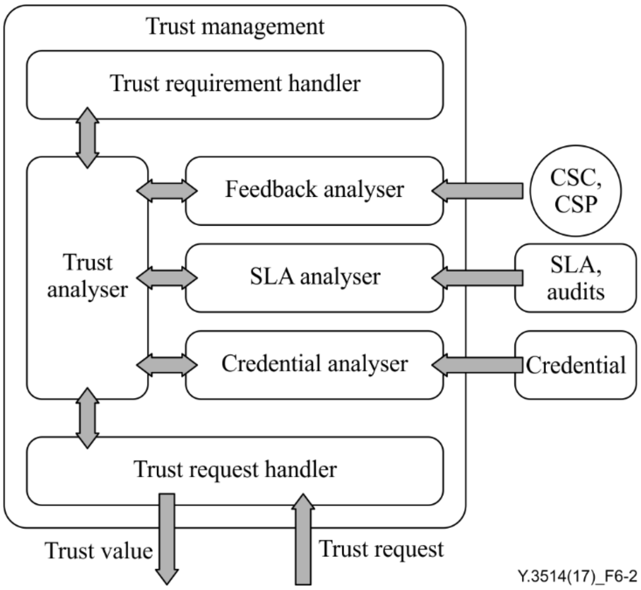


Figure 6-2 – The relationship between particular elements of trust management functionalities

Trust management relies on components for managing isolation and security mechanisms. The components managing isolation ensure cross-layer trust, while components managing security mechanism establish a chain of trust satisfying both horizontal (cross-provider) and vertical (cross-layer) dimensions.

6.3 Resiliency of trusted inter-cloud

Resiliency includes the set of monitoring, preventive and responsive processes that enable a cloud service to provide near-continuous operations, or predictable and verifiable outages (such as scheduled maintenance), through appropriate failure and recovery actions. These include hardware failures, communications and software malfunctions, and can occur as isolated incident or in combination, including cascade of failures. These processes might include both automated and manual actions, usually spanning multiple systems, and thus their description and realisation are part of the overall cloud infrastructure, and not an independent function. Inherent in resiliency is the realisation of risk management – since resiliency is determined by the least resilient component in the system, performance or other factors may limit the extent to which resiliency is achievable or effective. The association of risk to value is realised in the implementation choices to provide resiliency.

Inter-cloud resiliency is interpreted as persistence under uncertainty of performance among multiple CSPs in the face of some set of disturbances that are likely to occur during a specified timeframe.

Trusted inter-cloud resiliency is a set of technical procedures (rely on shifting control and security mechanisms) to:

– monitor CSC or CSP's environment and collect relevant data;

– analyse monitored data;

– predict faults and;

– mitigate or restore the cloud service parameters after service failure (related to certain equipment or software functionality, laws and regulations, local policies, service contracts, etc.) and availability (related to technical systems functionality).

Complementary to trusted inter-cloud resiliency is the reliability of trusted inter-cloud. This means the ability of the trusted inter-cloud environment to perform and maintain under stated conditions as required for a specified period of time.

6.4 Security and confidentiality of trusted inter-cloud

The security and confidentiality of trusted inter-cloud is the main challenge of integrating multiple CSP platforms. This is necessary to provide self-service, self-managed and end-to-end security services for the CSC, and for the CSP to guarantee a level of confidentiality, integrity, as well as availability of services and resources hosted on CSP's cloud computing environments. To establish and specify trust between different cloud computing environments as well as trust between CSC and CSPs, a dedicated security and confidentiality terminology, together with a master service agreement (MSA) is needed.

The security and confidentiality of trusted inter-cloud is based on distributed cloud management. It enables the primary CSP to provide end-to-end dynamic deployment, configuration and unified control of security and confidentiality of cloud services across multiple CSPs. In implementation, distributed cloud management supported trust can be realised by combining specialised protocol design with smart interaction with the underlying cloud network fabric (e.g., using software-defined networking (SDN) traffic engineering and cloud-tailored smart queue management).

To increase security and confidentiality of trusted inter-cloud computing, it is necessary to define a terminology (language) to annotate (or tag) workloads and data with security requirements (such as permissible storage locations). These annotations will be processed by the system during scheduling and migration to ensure that workload constraints are maintained. Additionally, annotation of workloads allows the use of appropriate network data plane mechanisms (e.g., SDN) for strong security protection and traffic isolation in order to ensure that the above constraints are reached when workloads are practically placed, executed (data accessed and stored) and migrated. Such annotation of workloads and data sets might be based on standards for data categorisation.

The security and confidentiality of trusted inter-cloud is realized based on a two dimensional (vertical and horizontal) model as follows. The vertical axis is based on the layers of the cloud computing reference architecture [ITU-T Y.3502]:

– in the higher layers focussed on user-centric security and confidentiality through a unified distribution layer for cloud resources (independently from their type and from underlying CSP), such as user identity management, authentication and authorization;

– in the lower layers focused on provider-independent control, security and confidentiality over the whole distributed inter-cloud infrastructure, such as disk and network encryption.

The horizontal axis is based on the interconnection of CSPs based on the inter-cloud framework [ITU-T Y.3511].

Consequently, security and confidentiality of trusted inter-cloud are based on satisfying both horizontal (cross-provider) and vertical (cross-layer) dimensions.

6.5 Relationship between trusted inter-cloud and the cloud computing reference architecture

The cloud computing reference architecture [ITU-T Y.3502] provides an architectural framework which defines cloud computing roles, sub-roles, cloud computing activities and cross-cutting aspects. It also describes the functional layers and functional components of a cloud computing system. According to this framework, the trusted inter-cloud relationships can be expressed by cross-cutting aspects like security, governance and resiliency that span over cloud computing multi-layer functionality. The conceptual view of cloud computing management is based on cloud computing management layers and the service management interface (SMI) approach [ITU-T Y.3520] and [ITU-T Y.3522].

Trust management in inter-cloud environments can be realized based on the common model for end-to-end cloud computing management [ITU-T Y.3521]. In particular, the operations support system (OSS) functional components encompass the set of management capabilities that are required in order to manage and control trust in an inter-cloud environment. The role of business support system (BSS) functional components remains to encompass the set of business-related management capabilities dealing with customers and supporting processes in a trusted manner (see clause 9.2.5.4 of [ITU-T Y.3502]). Therefore, in a trusted inter-cloud environment, the cloud computing management functionalities [ITU-T Y.3521] can be used to reach objectives of trust satisfying governance, security and resiliency aspects of inter-cloud.

7 General requirements for trusted inter-cloud

This clause identifies general requirements applicable to trusted inter-cloud.

7.1 Data separation

It is required that the CSP provides data separation between workloads to ensure security and confidentiality.

7.2 Data annotation

It is recommended that the CSP supports annotation (tagging) of trusted inter-cloud data (workloads) to enable compliance with regulatory obligations.

7.3 Confidentiality of data

It is required that the CSP respects the confidentiality of the CSC's or CSP's data used in trusted inter-cloud system.

7.4 Operational statistics

It is recommended that the CSP supports operational statistics for trusted inter-cloud services according to appropriate methods of measurement.

7.5 Interoperability and dependability

It is recommended that the CSP supports interoperability and dependability of trusted inter-cloud services.

7.6 Master service agreement

It is recommended that the CSP respects master service agreements to reach objectives of trust satisfying governance, security and resiliency aspects of inter-cloud.

8 Requirements for governance of trusted inter-cloud

This clause provides requirements for governance of trusted inter-cloud derived from the use cases described in Appendix I.

8.1 Geographical policies

It is required that the CSP respects all applicable geographical policies in order to realise requests from the CSC or other CSP.

It is recommended that the CSP integrates and validates cloud services from peer CSPs with respect to geographical policies.

It is recommended that the CSP validates and supports resiliency cloud services from peer CSPs with respect to geographical policies.

NOTE – A geographical policy can be conditional, for example "data shall not leave country X *unless* this movement is necessary to continue service during a major outage".

8.2 Governance policies

It is required that the CSP respects governance policies to reach objectives of trusted inter-cloud.

8.3 Governance roles

It is required that the CSP respects governance roles to reach objectives of trusted inter-cloud.

8.4 Regulatory policies

It is required that the CSP complies with applicable data regulation policies (e.g., medical, financial, defence, etc.) and business regulatory policies related to inter-cloud.

NOTE – Regulation policies concern regulations applied to particular types of businesses.

8.5 Laws and regulations

It is required that the CSP complies with applicable laws and regulations as well as local policies.

9 Requirements for management of trusted inter-cloud

This clause provides requirements for management of trusted inter-cloud derived from the use cases described in Appendix I.

9.1 Management policies

It is required that the CSP respects management policies applied to trusted inter-cloud.

9.2 Management roles

It is required that the CSP respects management roles applied to trusted inter-cloud.

9.3 Distributed data

It is recommended that the CSP supports management of distributed data in trusted inter-cloud.

9.4 Identity management

It is recommended that the CSP provides identity management to enable compliance with CSC policy in trusted inter-cloud.

9.5 Access management

It is recommended that the CSP provides access management to enable compliance with CSC policy in trusted inter-cloud.

9.6 Policy language

It is recommended that the CSP supports policy language (related to data annotation) to increase confidentiality of trusted inter-cloud.

10 Requirements for resiliency of trusted inter-cloud

This clause provides requirements for resiliency of trusted inter-cloud derived from the use cases described in Appendix I.

10.1 Service monitoring

It is recommended that the CSP monitors quality of trusted inter-cloud service in real time.

10.2 Service continuity

It is recommended that the CSP supports the resiliency of trusted inter-cloud services in order to respect service continuity in accordance with the SLA established between CSC and CSP or between CSPs.

10.3 Resiliency policies

It is recommended that the CSP integrates and validates cloud services from peer CSPs with respect to resiliency policies.

10.4 Resiliency validation

It is recommended that the CSP validates resiliency of cloud service from peer CSPs.

11 Requirements for security and confidentiality of trusted inter-cloud

This clause provides requirements for security and confidentiality of trusted inter-cloud derived from the use cases described in Appendix I.

11.1 Security and confidentiality policies

It is recommended that the CSP supports unified (commonly adopted) security and confidentiality policies and metadata.

11.2 Level of robustness

It is recommended that the CSP supports appropriate levels of robustness.

11.3 Security policy negotiation

It is recommended that the CSP supports security policy negotiation.

11.4 Security and confidentiality policy

It is required that the CSP respects the security and confidentiality policies established between CSC and CSP or between CSPs.

11.5 Data security

It is recommended that the CSP supports on-demand data security services.

11.6 Security policy monitoring

It is recommended that the CSP supports deployment and monitoring of security policies related to inter-cloud.

12 Security considerations

Security aspects for consideration within the cloud computing environment, including inter-cloud computing, are described in [ITU-T X.1601], which analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use case of trusted inter-cloud computing

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

I.1 Use case template

The use cases developed in Appendix I should adopt the following unified format for better readability and convenient material organization.

Title	Note: The title of the use case
Description	Note: Scenario description of the use case
Roles	Note: Roles involved in the use case
Figure (optional)	Note: Figure to explain the use case, but not mandatory
Pre-conditions (optional)	Note: The necessary pre-conditions that should be achieved before starting the use case
Post-conditions (optional)	Note: The post-condition that will be carried out after the termination of current use case
Derived requirements	Note: Requirements derived from the use cases, whose detailed description is presented in the dedicated chapter

I.2 Trusted inter-cloud related use cases

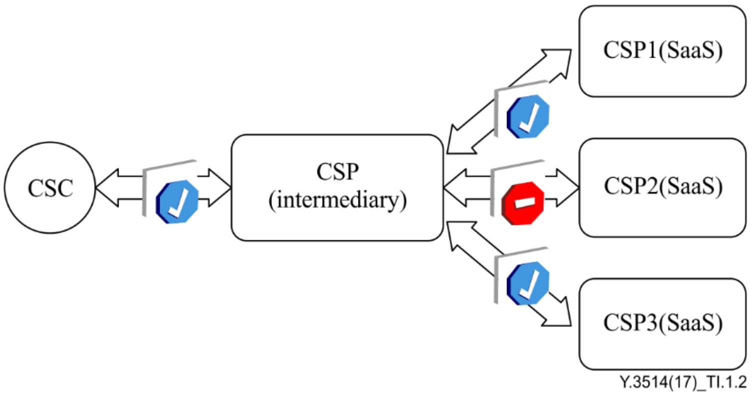
I.2.1 Use case of access security in trusted inter-cloud

This use case illustrates the security aspects of trusted inter-cloud between the primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.1 – Access security in trusted inter-cloud

Title	Access security in trusted inter-cloud
Description	– The CSC requests secure and malware free software as a service (SaaS). – The primary CSP in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validates services from multiple SaaS CSPs (secondary CSPs). – For the CSP(Intermediary), in order to guarantee secure and malware free SaaS software for CSC, it is necessary to validate SaaS from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative SaaS validation the CSP offer of this SaaS is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1(SaaS), the service is automate established between CSP(Intermediary) and CSP3(SaaS).
Roles	CSC, CSP, CSP(SaaS)

Title	Access security in trusted inter-cloud

Figure (optional)	 CSC
	CSP (intermediary)
	CSP1(SaaS)
	CSP2(SaaS)
	CSP3(SaaS)
	Y.3514(17)_TI.1.2

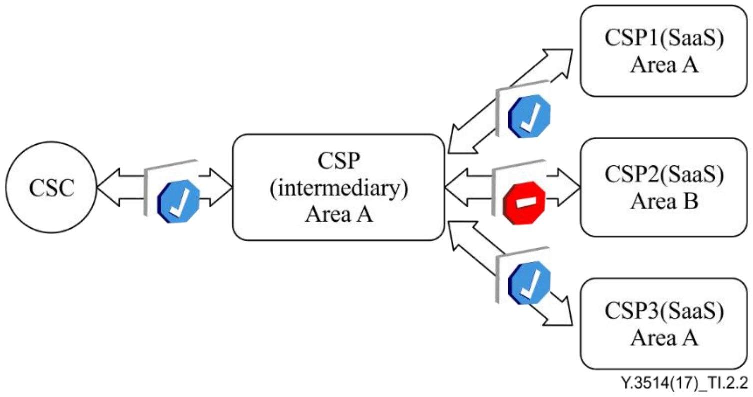
Pre-conditions (optional)	– The CSP1(SaaS) and CSP3(SaaS) deliver malware free software. – The CSP2(SaaS) delivers malware infected software.
Post-conditions (optional)	– The CSP(Intermediary) guarantees secure SaaS. – The CSP(Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP(Intermediary) establishes service between CSC and CSP3(SaaS) in case of failed CSP1(SaaS).
Derived requirements	– access security between the CSC and CSP – integrate and validate services from multiple CSPs – resiliency service from multiple CSPs

I.2.2 Use case of geographical policy in trusted inter-cloud

This use case illustrates the governance aspect of trusted inter-cloud between the primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.2 – Geographical policy in trusted inter-cloud

Title	Geographical policy in trusted inter-cloud
Description	– The CSC request SaaS service performed exactly within area A (geographical policy). – The primary CSP in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validates SaaS services from multiple CSPs (secondary CSPs). – For the CSP(Intermediary), in order to respect the request of CSC, it is necessary to validate governance polices from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative validation, the secondary CSP offer is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1(SaaS), the SaaS service is automatically established between CSP(Intermediary) and CSP3(SaaS).
Roles	CSC,CSP, CSP(SaaS)

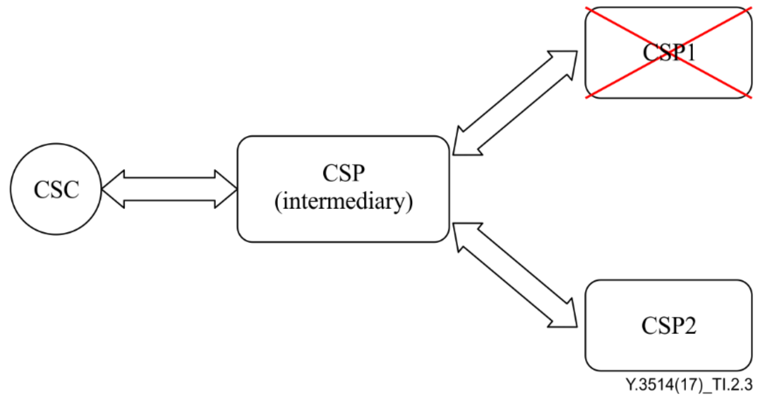
Title	Geographical policy in trusted inter-cloud
Figure (optional)	 CSC CSP (intermediary) Area A CSP1(SaaS) Area A CSP2(SaaS) Area B CSP3(SaaS) Area A Y.3514(17)_TI.2.2
Pre-conditions (optional)	– The primary CSP(Intermediary) and secondary CSPs are in trusted inter-cloud relationship. – The CSP1(SaaS) and CSP3(SaaS) effects geographical polices. – The CSP2 performs SaaS service out of the requested area.
Post-conditions (optional)	– The CSP(Intermediary) guarantees governance policies of SaaS. – The CSP (Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP (Intermediary) establishes service between CSC and CSP3(SaaS) in case of failed CSP1(SaaS).
Derived requirements	– geographical policies – integrate and validate services from multiple CSPs – resiliency service from multiple CSPs

I.2.3 Use case of video gaming in trusted inter-cloud

This use case illustrates the resiliency aspect of trusted inter-cloud between the primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.3 – Video gaming in trusted inter-cloud

Title	Video gaming service in trusted inter-cloud
Description	– The CSC requests video gaming service with quality of service (QoS) (Premium service under SLA). – The primary CSP in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validates video gaming services from multiple CSPs (secondary CSPs). – The CSP(Intermediary) monitors quality of service from secondary CSP1 and CSP2. In case service quality drops below premium service level, due to internal or external problems of CSP1 (e.g., overloaded resources, human error, distributed denial of service(DDoS)), the service is automatically established between CSP(Intermediary) and CSP2 without interruption.
Roles	CSC, CSP

Title	Video gaming service in trusted inter-cloud
Figure (optional)	 CSC CSP (intermediary) ~~CSP1~~ CSP2 Y.3514(17)_TI.2.3
Pre-conditions (optional)	– The primary CSP(Intermediary) and secondary CSPs are in trusted inter-cloud relationship. – The CSP1 and CSP2 offer video gaming service (Premium service). – The CSP (Intermediary) integrates and validates gaming services with QoS. – The CSP (Intermediary) establishes service between CSC and CSP1.
Post-conditions (optional)	– The CSP1 is under internal or external perturbation and quality of video gaming service drops below premium service level. – The service is automatically established between CSP(Intermediary) and CSP2 without service interruption.
Derived requirements	– real-time monitoring quality of trusted service – integrate and validate services from multiple CSPs – resiliency service from multiple CSPs

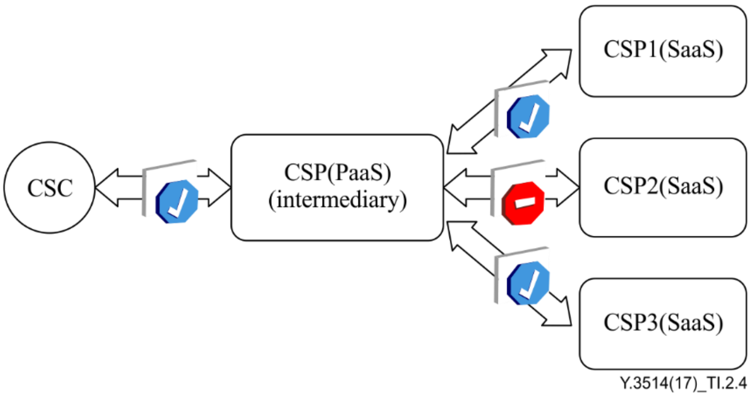
I.2.4 Use case of distributed image processing platform in trusted inter-cloud

This use case illustrates the security and confidentiality aspects of trusted inter-cloud between a primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.4 – Distributed image processing platform in trusted inter-cloud

Title	Distributed image platform in trusted inter-cloud
Description	– The CSC requests the CSP for a platform to build image processing and storage systems. CSC is required to provide its own part of the software into the cloud. – The CSC request that the platform fits regulatory policy to reach safety, security and confidentiality constraints. The CSC requests QoS for data processing. – The CSC requests that the physical location (localization) for its data store as well as CSP can be chosen by CSC in an elastic manner. – The primary CSP(PaaS) in an inter-cloud intermediary pattern CSP(Intermediary) is the contact point for CSC. – The CSP(Intermediary) integrates and validates SaaS services from multiple CSPs (secondary CSPs). – The CSP2(SaaS) offers the same service as CSP1(SaaS) or CSP3(SaaS) but does not meet the required business regulatory policy. – For the CSP(Intermediary), in order to respect the request of a CSC, it is necessary to validate security and confidentiality policies from

Title	Distributed image platform in trusted inter-cloud
	secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative validation, the secondary CSP offer is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1, the SaaS service is automatically established between CSP(Intermediary) and CSP3. In particular, an example of such service could be sharing information of patients' healthcare between hospitals. The hospitals can exchange all medical data of patients, while other agencies such as insurance or government have access limited to statistical information only without personally identifiable information (PII).
Roles	CSC, CSP(PaaS), CSP(SaaS)

Figure (optional)	 CSC
	CSP(PaaS) (intermediary)
	CSP1(SaaS)
	CSP2(SaaS)
	CSP3(SaaS)
	Y.3514(17)_TI.2.4

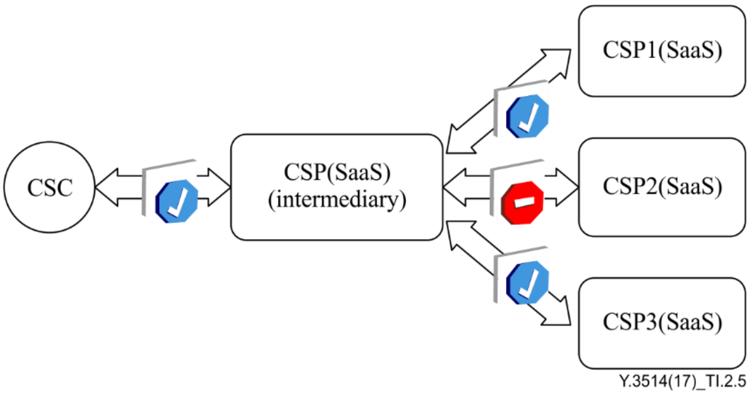
Pre-conditions (optional)	– The primary CSP(PaaS) and secondary CSPs are in trusted inter-cloud relationship. – The CSP1(SaaS) and CSP3(SaaS) effects security, safety and confidentiality polices. – The CSP2(SaaS) performs service out of business regulatory policy.
Post-conditions (optional)	– The CSP(Intermediary) guarantees security and confidentiality policy of SaaS. – The CSP(Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP(Intermediary) establishes service between CSC and CSP3 (SaaS) in case CSP1(SaaS) fails.
Derived requirements	– security and confidentiality policies – unified (commonly adopted) security policies and metadata – interoperability and dependability – support appropriate level of robustness – security policy negotiation terminology – management of distributed data – resiliency service from multiple CSPs

I.2.5 Use case of distributed information exchange system in trusted inter-cloud

This use case illustrates the security and confidentiality aspect of trusted inter-cloud between a primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.5 – Distributed information exchange system in trusted inter-cloud

Title	Distributed information exchange system in trusted inter-cloud
Description	– The CSC from regulation business domain (e.g., healthcare, finance, defence), requests the CSP for a service to build an information exchange system. CSC requires that information will be distributed respecting business regulatory policies and data regulation policy. – The CSC requests that distributed information exchange system fits regulatory policy to reach safety, security and confidentiality constraints. – The CSC requests that physical location (localization) for their data store as well as CSP can be chosen by CSC in an elastic manner. – The primary CSP(SaaS) in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validate SaaS services from multiple CSPs (secondary CSPs). – The CSP2(SaaS) offers the same service as CSP1(SaaS) or CSP3(SaaS) but does not meet the required business regulatory policy. – For the CSP(Intermediary), in order to respect the request of CSC, it is necessary to validate security and confidentiality policies from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative validation, the secondary CSP offer is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1, the SaaS service is automatically established between CSP(Intermediary) and CSP3. In particular, an example of such service could be PaaS-based processing of satellite image data for farm crop analysis.
Roles	CSC,CSP(SaaS)

Figure (optional)	 CSC
	CSP(SaaS) (intermediary)
	CSP1(SaaS)
	CSP2(SaaS)
	CSP3(SaaS)
	Y.3514(17)_TI.2.5

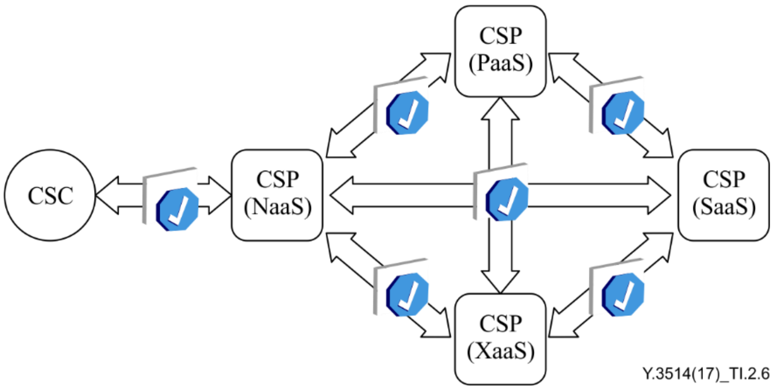
Pre-conditions (optional)	– The primary CSP(SaaS) and secondary CSPs are in a trusted inter-cloud relationship. – The CSP1(SaaS) and CSP3(SaaS) effects security, safety and confidentiality policies. – The CSP2(SaaS) performs service out of business regulatory policy.
Post-conditions (optional)	– The CSP(Intermediary) guarantees the security and confidentiality policy of SaaS. – The CSP(Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP(Intermediary) establishes service between CSC and CSP3(SaaS) in case of failed CSP1(SaaS).

Title	Distributed information exchange system in trusted inter-cloud
Derived requirements	– security and confidentiality policies – master service agreements – on-demand data security services – deployment and monitoring of security policies around CSPs – respect data regulation policy (e.g., medical, financial, defence, etc.) NOTE – Regulation policy concern regulation applied to particular business. – respect business regulatory policies – resiliency service – respect laws and regulations, – respect local policies.

I.2.6 Use case of virtual home gateway in trusted inter-cloud

This use case illustrates management aspect of trusted inter-cloud between CSC and CSP or between CSPs. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.6 – Virtual home gateway in trusted inter-cloud

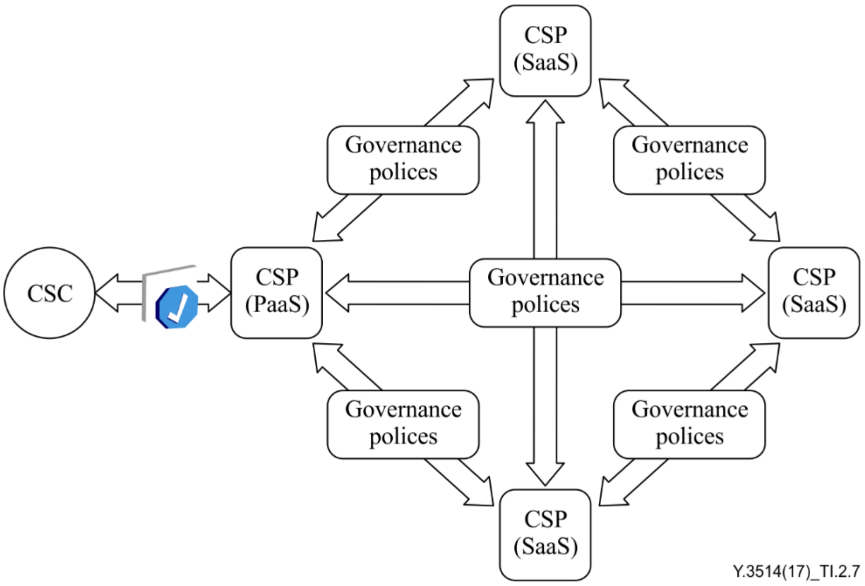
Title	Virtual home gateway in trusted inter-cloud
Description	– A large group of CSCs requests from CSP(NaaS) secured access to Internet with parental control service. A CSP(NaaS) serves such service over virtual home gateway (vHGW) facilities using network functions virtualization (NFV) and SDN technologies. – The CSP(NaaS) forms an inter-cloud federation pattern within a group of peer CSPs due to lack of own resources for request realization. According to the management of sensitive CSC's data, the CSP(NaaS) establish a trusted relationship between CSPs(PaaS) and CSPs(SaaS) involved in federation. – The CSP(NaaS) forms service chaining on parental control service from a set of network virtual functions (e.g., virtual firewall (vFW), virtual network address translation (vNAT), virtual load balancer (vLB)) hosted by CSP(PaaS) and CSP(SaaS). – The CSP(NaaS) monitors quality of service chaining and in case of quality drops below threshold or in case of the realization of particular key performance indicators (KPIs) (e.g., low power consumption, service balancing), the service is automatically reallocated within the federation, respecting policy and governance roles applied.
Roles	CSC, CSP(NaaS), CSP(PaaS), CSP(SaaS), CSP(XaaS)
Figure (optional)	 CSC CSP (NaaS) CSP (PaaS) CSP (SaaS) CSP (XaaS) Y.3514(17)_TI.2.6

Title	Virtual home gateway in trusted inter-cloud
Pre-conditions (optional)	– The CSP(NaaS) and CSP(PaaS) and CSP(SaaS) are in a trusted inter-cloud relationship.
Post-conditions (optional)	– The CSP(NaaS) guarantees governance policy of SaaS. – The CSP(NaaS) establishes service chaining between CSP(PaaS) and CSP(SaaS). – The CSP(NaaS) reallocate service between CSPs among federation in case service quality drops below threshold or in case of the realization of particular KPIs (e.g., low power consumption, service balancing).
Derived requirements	– policies and governance roles – confidentiality of CSC's data – service statistics – annotation (tagging) of cloud workloads

I.2.7 Use case of distributed document exchange system in trusted inter-cloud

This use case illustrates governance aspect of trusted inter-cloud between CSC and CSP or between CSPs. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.7 – Distributed document exchange system in trusted inter-cloud

Title	Distributed document exchange system in trusted inter-cloud
Description	– The CSC requests from CSP(PaaS) cloud-based system which allows exchanging documents between their partners. – The CSC requests that these documents could be reviewed, updated and audited by the CSC or cloud service partner (CSN). – The CSC requests that distributed document exchange system fits regulatory policy to reach safety, security and confidentiality constraints. – The CSP(PaaS) forms federation pattern among CPSs(SaaS) and becomes contact point for CSC. – The CSP(PaaS) determine appropriate policies or principles which allows using of distributed document system in trustworthy manner.
Roles	CSC, CSP(PaaS), CSP(SaaS)
Figure (optional)	 CSP (SaaS) Governance polices Governance polices CSC CSP (PaaS) Governance polices CSP (SaaS) Governance polices Governance polices CSP (SaaS) Y.3514(17)_TI.2.7

Title	Distributed document exchange system in trusted inter-cloud
Pre-conditions (optional)	– The CSP(PaaS) and CSPs(SaaS) are in trusted inter-cloud relationship.
Post-conditions (optional)	– The CSPs implements governance policy in theirs management system.
Derived requirements	– governance policies and governance roles – data separation for ensuring security and confidentiality – annotation (tagging) of cloud workloads to comply with regulatory needs – identity and access management to comply with CSC policy

Bibliography

[b-ISO/IEC 19086-1] ISO/IEC 19086-1:2016, *Information technology – Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 38500:2015] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization*.

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer-Service Delivery Framework Cloud Interface V2.2*. <https://www.tmforum.org/?s=TR198>

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, 2019