International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3517

(12/2018)

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

Cloud Computing

Cloud computing – Overview of inter-cloud trust management

Recommendation ITU-T Y.3517

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.3517

Cloud computing – Overview of inter-cloud trust management

Summary

Recommendation ITU-T Y.3517 provides an overview of inter-cloud trust management by specifying isolation and security management mechanisms, inter-cloud trust management model, reputation-based trust management in an inter-cloud environment, cloud service evaluation framework and the relationship with cloud computing reference architecture. It also provides requirements for inter-cloud trust management derived from the corresponding use cases.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3517	2018-12-14	13	11.1002/1000/13814

Keywords

Inter-cloud, inter-cloud trust management model, isolation and security mechanism, management, reputation-based trust management, trust, trust management.

[*] 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.3517

Cloud computing – Overview of inter-cloud trust management

1 Scope

This Recommendation describes inter-cloud trust management aspects including:

- isolation and security management mechanism;
- trust management model;
- reputation-based trust management;
- cloud service evaluation framework;
- relationship with cloud computing reference architecture;
- requirements for inter-cloud trust management and relative use cases.

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.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, *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.3516]	Recommendation ITU-T Y.3516 (2017), *Cloud computing – Functional architecture of inter-cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

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

3.1.3 cloud service agreement [b-ISO/IEC 19086-1]: Documented agreement between the cloud service provider and cloud service customer that governs the covered service(s).

NOTE – A cloud service agreement can consist of one or more parts recorded in one or more documents.

3.1.4 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.

3.1.5 cloud service level objective [b-ISO/IEC 19086-1]: Commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale.

NOTE – An SLO commitment may be expressed as a range.

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

3.1.7 cloud service qualitative objective [b-ISO/IEC 19086-1]: Commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal scale or ordinal scale.

NOTE 1 – A cloud service qualitative objective may be expressed as an enumerated list.

NOTE 2 – Qualitative characteristics typically require human interpretation.

NOTE 3 – The ordinal scale allows for existence/non-existence.

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

3.1.9 service level agreement (SLA) [b-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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS	Business Support System
CSA	Cloud Service Agreement
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DoS	Denial-of-Service
E2E	End-to-End
IaaS	Infrastructure as a Service
NaaS	Network as a Service
OSS	Operations Support System
SaaS	Software as a Service
SDN	Software Defined Network
SLA	Service Level Agreement

SLO	cloud Service Level Objective
SQO	cloud Service Qualitative Objective
SSO	Single Sign-On
TLS	Transport Layer Security
VM	Virtual Machine

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 document is to be claimed.

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

6 Overview of inter-cloud trust management

The inter-cloud computing concept is based on the relationship (pattern) among multiple cloud service providers (CSPs). This pattern (peering, federation or intermediary) allows a 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 CSPs, or between a cloud service customer (CSC) and a CSP, as one of them has to delegate physical control over applications, services, resources and data to the others. Therefore, trust management is a key point between CSPs, or between a CSC and a CSP in inter-cloud.

The trust management of inter-cloud uses a two-dimensional (vertical and horizontal) model, where the vertical axis is based on the layers of the cloud computing reference architecture [ITU-T Y.3502], and the horizontal ones is based on the interconnection of CSPs based on the inter-cloud framework [ITU-T Y.3511].

The inter-cloud trust management framework relies on components for managing isolation and security mechanisms, which handle cross-layer trust and establish chain of trust, respectively [ITU-T Y.3514]. According to particular needs, inter-cloud trust management may either be CSC-related or CSP-related.

From a CSC-related perspective, major threats concern data security and privacy. Even assuming a trusted cloud service provider, a malicious administrator has sufficient permissions to affect unauthorised use and to modify customer information. Thus, CSP control over the infrastructure should be limited to avoid inspection or analysis of user data and virtual machine (VM) instances without explicit CSC consent. Moreover, security should be self-service, so that a CSC can exercise fine-grained control over protection of their cloud resources according to a given security service level agreement (SLA). This means the CSC should be able to actively monitor its allocated resources, while enabling a high level of customizability of the architecture and its services.

From a CSP-related perspective, major threats are malicious customers issuing attacks against the virtualization layer, to break isolation or perform denial-of-service (DoS). An attacker is a non-privileged malicious cloud tenant. Mitigation of such threats implies first isolation: tenants should not be authorized to monitor or modify VM state or data from other tenants. It also means a small trusted computing base: the number of vulnerabilities and failures in the platform is directly linked with the code size run at the highest privilege level and the set of primitives exported.

Many different classes of mechanisms and architectures have been proposed to address this issue, where trust management and isolation are intimately linked. Representative isolation architectures include modular hypervisors partly controlled by the CSC or secure enclaves based on hardware security mechanisms. Side-channel attacks also introduce major isolation issues for inter-cloud systems. Although many cryptographic solutions protect user confidentiality in the cloud, it is not possible to perform efficient and fast enough arbitrary computations on the data while they are encrypted.

In an inter-cloud environment, reputation is a key factor for selecting the CSP to transact with. There are different approaches to implement reputation-based trust management in inter-cloud environments, all of them are based on a uniform cloud SLA framework which could make CSP and CSC avoid confusion and have a common understanding about the cloud service quality commitment.

6.1 Isolation and security management mechanism

The isolation and security of trusted inter-cloud is based on distributed cloud management. It enables the CSP who provides cloud services to a CSC to have end-to-end (E2E) and unified control for trust of cloud services across multiple CSPs.

For implementation of managing isolation and security, mechanisms could be used as follows:

– **Annotation of workloads and data**: to increase security 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., software defined network (SDN)) for strong security protection and traffic isolation 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 might be based on standards for data categorization (see clause 6.4 of [ITU-T Y.3514]).

– **Modular hypervisors partly controlled by the CSC**: hypervisors usually have a large and complex administrative domain with privileges to inspect a client's VM state. Attacks against or misuse of the administrative domain can compromise client security and privacy. Moreover, these hypervisors provide clients inflexible control over their own VMs. Modular hypervisors simultaneously address problems with security/privacy and inflexible control. It introduces a novel privilege model that reduces the power of the administrative domain and gives the CSC more flexible control over their own VMs. It splits administrative privileges between a system-wide domain and per-client administrative domains. Each CSC can manage and perform privileged system tasks on its own VMs, thereby providing flexibility. The system-wide administrative domain cannot inspect the code, data or computation of client VMs, thereby ensuring security and privacy.

– **Secure enclave based on hardware security mechanisms**: secure enclave is an isolated process, executed on a platform that provides confidentiality and integrity of code and data as well as sealing and attestation. Isolated execution of a process restricts access to a subset of memory to that particular process or enclave. No other process on the same processor, operating system, hypervisor, or system management module, can access this memory. Sealing is the authenticated encryption of data with an encryption key based on the identity of the enclave and the platform it is running on. Attestation is the ability to prove to third parties that a secure enclave is running with a particular identity securely on the hardware.

- **Single sign-on (SSO)**: in an inter-cloud environment, the CSC should be able to access various resources and services offered by different CSPs once they are successfully authenticated in the inter-cloud. Since each CSP has its own authentication mechanism, a standard method that provides SSO authentication within inter-cloud environments should be deployed. In an inter-cloud environment, SSO can be achieved through the delegation of trust that allows an entity to act on another entity's behalf. This mechanism allows entities of inter-cloud to securely interact by establishing a chain of trust of proxy certificates. SSO can also be achieved through the use of a trusted third party who will certify credentials on behalf of all parties of inter-cloud.

  NOTE – The functionalities for managing isolation and security mechanisms are provided in Appendix II.

6.2 Inter-cloud trust management model

The inter-cloud trust management is realized based on a two-dimensional (vertical and horizontal) model as follows:

- The vertical axis (cross-layer) is based on the layers of the cloud computing reference architecture [ITU-T Y.3502]. The inter-cloud trust management in this dimension is realized over functional components for managing isolation and security mechanisms. The components managing isolation ensure that different tenants and their workloads and data are isolated and inaccessible to one another in each layer. The components managing security, establish a chain of trust in the cross-layer dimension. In higher layers, it focusses on user-centric trust, such as user identity management, authentication and authorization. In lower layers it focusses on resource control and security over the distributed inter-cloud infrastructure, such as virtualization and encryption management.
- The horizontal axis (cross-provider) is based on the interconnection of CSPs and relies on the inter-cloud framework [ITU-T Y.3511]. The inter-cloud trust management in this dimension is realized over functional components for managing security mechanisms. The trust management functionalities located in the multi-layer function ("Authorization and security policy management") establish a chain of trust between CSPs with peering, federation and intermediary patterns.

6.3 Reputation-based trust management in inter-cloud environment

In an inter-cloud environment, information such as a CSP's competence, honesty, availability, quality of service and reputation will influence the selection of the CSP to transact with. Therefore, there is a need to assess and maintain the reputation of CSPs.

Reputation is a measurement which could be derived from direct or indirect knowledge of earlier interactions of peers and is used to assess the level of trust to a peer. As an entity can trust another entity in the inter-cloud based on their reputation, we can use reputation to build trust.

One approach to implementing reputation-based trust management is shown in Figure 6-1. It is a distributed framework that enables interested parties to determine the reputation of inter-cloud entities. In this approach, each CSP has its own trust evaluation system which maintains and computes its trust values locally. Trust value is a reputation scoring for CSPs and could be referenced in selecting a CSP to transact with. It could be calculated in realtime based on direct observation and experience (i.e., first-hand reputation information) and indirect information by sharing observations and experience measures with other entities (i.e., second-hand reputation information).

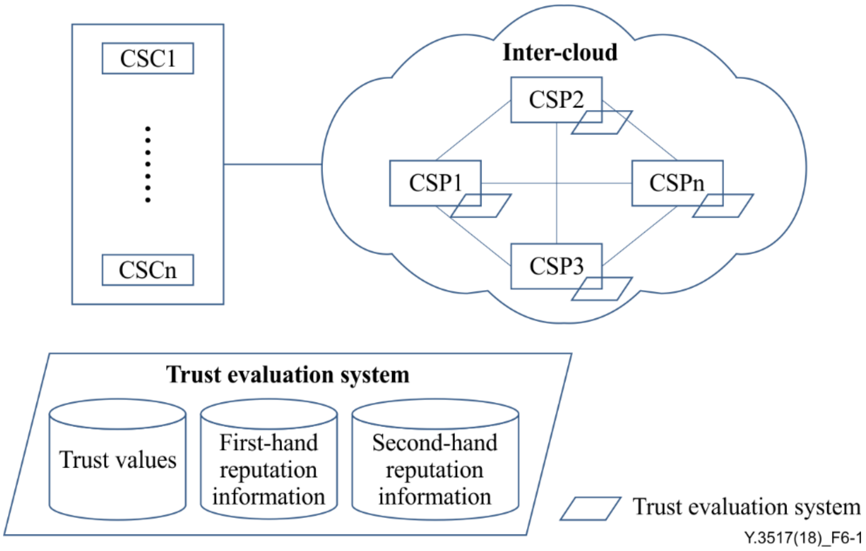


Figure 6-1 – One approach to implement reputation-based trust management

The trust evaluation system is responsible for collecting and maintaining reputation information such as a CSP's competence, honesty, availability, quality of service about every other CSP that it has peering agreements with, and this information could be represented by parameters such as "mean time between failures", "mean time to restore service", "ready for service date" and so on. First-hand reputation information should be updated when a CSP completes a transaction with other CSPs. At the same time, the trust evaluation system should publish its updated first-hand reputation information to a subset of their peers that they have a peering agreement with. Since the integrity of the second-hand reputation information has signally influence on the quality of a trust evaluation system, a mechanism should be implemented to protect against unfair ratings from others.

Another approach to implement reputation-based trust evaluation is shown in Figure 6-2. It is a centralized framework which has one or some independent trust evaluation systems operated by a third-party operator. With this approach, CSPs do not have their own trust evaluation system; they only provide their first-hand reputation information to the centralized trust evaluation system and query the trust values of CSPs from the centralized trust evaluation system when they need it. In this approach, the trust evaluation system calculates the trust value for CSPs only based on second-hand reputation information provided by CSPs in the inter-cloud. Therefore, an efficient mechanism for protecting against unfair ratings is more important in this approach.

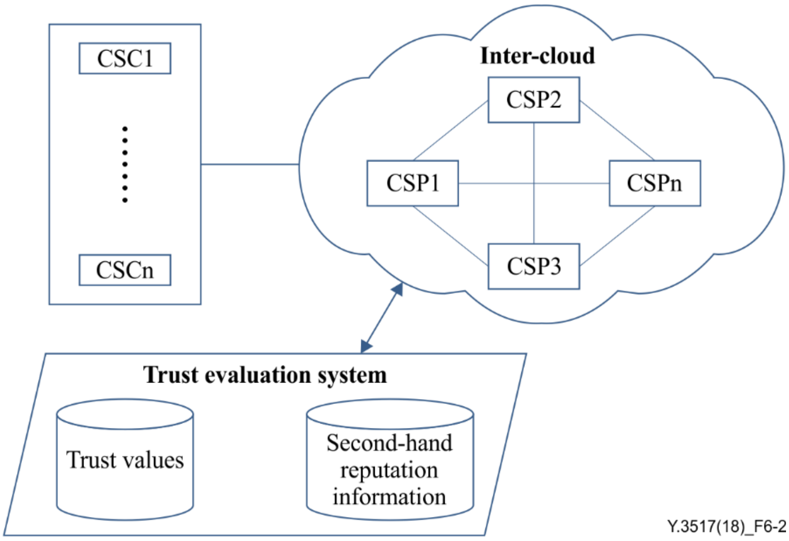


Figure 6-2 – Another approach to implement reputation-based trust management

6.4 Cloud service evaluation framework

The reputation of a CSP is highly correlated with the evaluation of cloud services it provides. A CSC could compare and evaluate cloud services through the cloud SLA provided by the CSP. A cloud SLA is a part of the cloud service agreement (CSA) that includes cloud service level objectives (SLOs) and cloud service qualitative objectives (SQOs) for the covered cloud service. An SLO is a commitment a CSP makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale. An SQO is a commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal scale or ordinal scale. Both SLO and SQO could be measured by metrics. Metric is the standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement.

With a uniform cloud SLA framework, a CSP and a CSC could avoid confusion and have a common understanding about the cloud service quality commitment. Therefore, it could be used as a cloud service evaluation framework by a CSC when comparing cloud services from different cloud service providers.

For more information about CSA, cloud SLA, SLO, SQO and cloud SLA metric models refer to [b-ISO/IEC 19086-1] and [b-ISO/IEC 19086-2].

6.5 Relationship with cloud computing reference architecture

The cloud computing reference architecture [ITU-T Y.3502] provides an architectural framework that is effective for describing the cloud computing roles, sub-roles, cloud computing activities, cross-cutting aspects, as well as the functional architecture and functional components of cloud computing. It also defines functional components for supporting inter-cloud computing, e.g., peer service integration and peer service management.

The inter-cloud computing functional architecture [ITU-T Y.3516] identifies inter-cloud specific extensions to functional components that are part of integration, security systems, operations support systems (OSSs) and business support systems (BSSs). For trusted inter-cloud, it defines a function called trust management. The trust management functionalities (see clause 6.2 of [ITU-T Y.3514]) are supported by the "authorization and security policy management" functional component within the multi-layer functions of the cloud computing reference architecture [ITU-T Y.3502]. Inter-cloud trust management can be realized using above functional components and functionalities. Inter-cloud trust management is also supported by functional components for managing isolation and security mechanisms, these functional components located in the "security systems" of the cloud computing reference architecture, as well.

This Recommendation is based on the functions defined in [ITU-T Y.3502], [ITU-T Y.3516] and [ITU-T Y.3514]. This Recommendation focuses on the trust management model and requirements in an inter-cloud environment based on the establishment of relationships (patterns) among multiple peer CSPs, including peering, federation and intermediary which are defined in [ITU-T Y.3511].

7 Requirements for inter-cloud trust management

This clause identifies requirements applicable to inter-cloud trust management.

7.1 Inter-cloud trust policies and credentials

It is recommended that a CSP provides specification of policies and credentials used for trust management.

It is recommended that a CSP implements a trust management system to evaluate whether the provided credentials satisfy the specified policy.

7.2 Inter-cloud reputation scoring

It is recommended that a CSP uses a trust scheme to evaluate whether other CSPs among inter-cloud relationships fulfil trust management requirements.

It is recommended that a CSP evaluate other CSPs among inter-cloud relationships to create and update reputation scoring of CSPs.

7.3 Inter-cloud reputation-based trust evaluation

It is recommended that a CSP has a trust evaluation system to manage other CSPs' reputations.

It is recommended that a CSP supports query and compares reputation of other CSPs from a third- party trust evaluation system.

7.4 SSO authentication

It is recommended that a CSP supports an SSO mechanism to enable a CSC’s access to various services offered by different CSPs once it is successfully authenticated by inter-cloud.

7.5 Periodical verification

It is recommended that a CSP supports a periodical verification mechanism to check if a CSC still has the privilege of accessing the CSP's service.

7.6 Control privilege for VM and data

It is recommended that a CSP avoids inspection or analysis of a CSC's data and VM instances without explicit CSC consent.

It is recommended that a CSP supports fine-grained CSC control over protection of its cloud resources according to a given security SLA.

It is required that a CSP avoids unauthorised use or modifications of a CSC’s VM state, service data or CSC data by other CSCs.

8 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 these security challenges.

Appendix I

Use case of inter-cloud trust management

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

I.1 Use case template

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

Table I.1 – Use case template

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

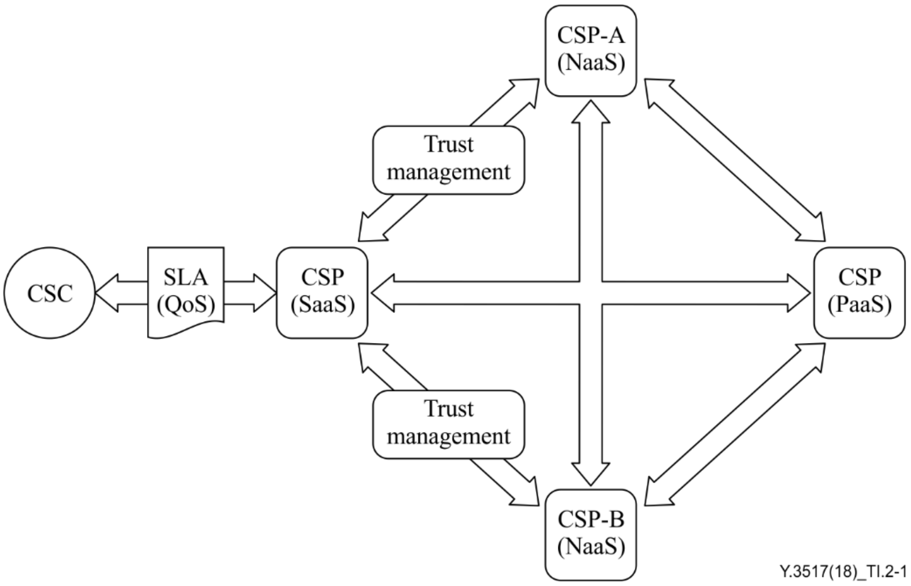
I.2 Use case of trusted network function virtualization

This use case illustrates trust management aspect in inter-cloud. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2 – Trusted network function virtualization

Title	Trusted network function virtualization
Description	A CSC requests "premium aoftware" as a service (software as a service (SaaS)), respecting network quality of service (QoS). The CSP (SaaS) forms inter-cloud federation pattern among CSP(PaaS) and CSPs (network as a service (NaaS)). The CSP(SaaS) becomes contact point for CSC. The CSP-A(NaaS) and CSP-B(NaaS) uses network function virtualization (NFV) and SDN technologies to serve NaaS service. The CSP(SaaS) uses a trust management system to keep track of CSP(NaaS) service. In case CSP-A(NaaS) performed out of schemes used to compute trust, the SaaS service is automatically established between the CSP(SaaS) and CSP-B(NaaS). Additionally, the CSP(SaaS) updates information on reputation of CSPs(NaaS).
Roles	CSC, CSP(SaaS), CSP(PaaS), CSP(NaaS).

Table I.2 – Trusted network function virtualization

Figure (optional)	 CSP-A (NaaS) Trust management CSC SLA (QoS) CSP (SaaS) CSP (PaaS) Trust management CSP-B (NaaS) Y.3517(18)_TI.2-1
Pre-conditions (optional)	– The CSPs(SaaS) form federation pattern of inter-cloud.
Post-conditions (optional)	– The CSPs(SaaS) implement trust management system. – The CSP(SaaS) uses reputation scores of CSPs.
Derived requirements	– Inter-cloud trust policies and credentials (refer to clause 7.1). – Inter-cloud reputation scoring (refer to clause 7.2).

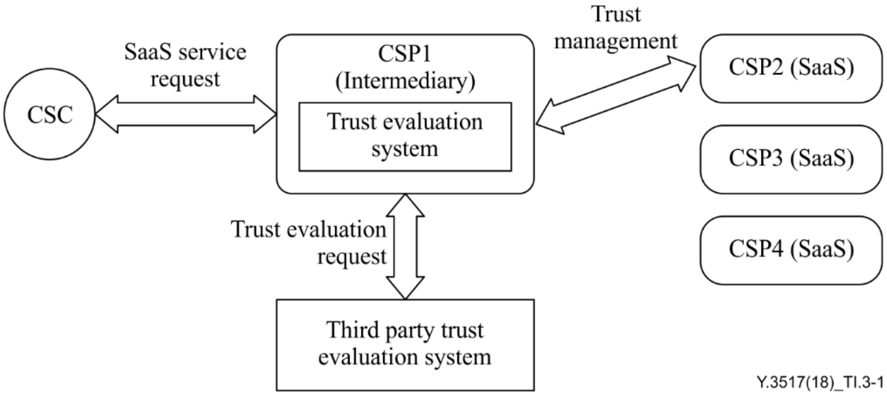
I.3 Use case of selecting CSP by reputation-based trust evaluation

This use case illustrates reputation-based trust evaluation in inter-cloud. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.3 – Selecting CSP by reputation-based trust evaluation

Title	Selecting CSP by reputation-based trust evaluation
Description	– The CSC requests a SaaS service from CSP1; – CSP1 cannot provide the service by itself, it plans to fulfil the service with inter-cloud intermediary pattern in which CSP1 acts as the intermediary; – All of CSP2(SaaS), CSP3(SaaS) and CSP4(SaaS) can provide the services CSP1 needs; – CSP1 will select a CSP as the secondary CSP base on the reputation of them. In this step: 1) If CSP1 has an internal trust evaluation system, it will query and compare the reputation of CSP2, CSP3 and CSP4 in this system and choose the best one to establish a trust relationship with; 2) If CSP1 does not have an internal trust evaluation system or there are no records about CSP2, CSP3 and CSP4 in the internal system, CSP1 should find a third-party trust evaluation system to query and compare the reputation data about these CSPs; – CSP2(SaaS) is the best choice and CSP1 establishes a trust relationship with it.

Table I.3 – Selecting CSP by reputation-based trust evaluation

Roles	CSC, CSP, CSP(SaaS).
Figure (optional)	 CSC SaaS service request CSP1 (Intermediary) Trust evaluation system Trust management CSP2 (SaaS) CSP3 (SaaS) CSP4 (SaaS) Trust evaluation request Third party trust evaluation system Y.3517(18)_TI.3-1
Pre-conditions (optional)	– All of CSP2(SaaS), CSP3(SaaS) and CSP4(SaaS) can provide the services CSP1 needs. – CSP1 has an internal trust evaluation system. – There is a third-party trust evaluation system.
Post-conditions (optional)	– CSP1 establishes a trust relationship with CSP2(SaaS) and provides service to the CSC with an inter-cloud intermediary pattern.
Derived requirements	– Inter-cloud reputation-based trust evaluation (refer to clause 7.3).

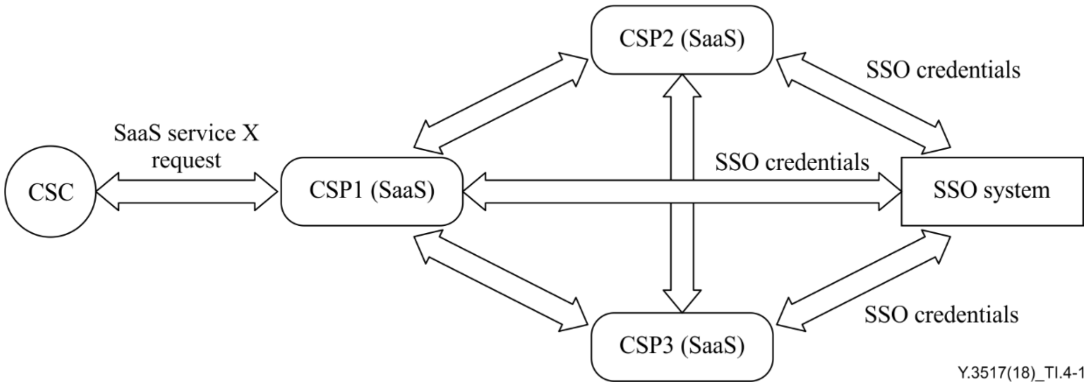
I.4 Use case of SSO authentication within inter-cloud environment

This use case illustrates SSO authentication in inter-cloud. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.4 – SSO authentication within inter-cloud environment

Title	SSO authentication within inter-cloud environment
Description	– The CSC requests SaaS service X from CSP1(SaaS); – The CSPs(SaaS) form inter-cloud federation pattern among them. The service X is integrated from services provided by CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS); – Each CSP has its own identity management system, and the CSC is not willing to be authenticated more than one time when accessing SaaS service X; – There is a trusted third-party SSO system which provides a certification service to certify credentials on behalf of all parties in the federation. With this SSO mechanism, the CSC is able to access various SaaS services offered by different CSPs once it is successfully authenticated by any member of the federation; – Each CSP supports a periodical verification mechanism to check if the CSC still has the privilege to access the CSP's service.
Roles	CSC, CSPs(SaaS).

Table I.4 – SSO authentication within inter-cloud environment

Figure (optional)	 CSP2 (SaaS) SSO credentials SaaS service X request CSC CSP1 (SaaS) SSO credentials SSO system SSO credentials CSP3 (SaaS) Y.3517(18)_TI.4-1
Pre-conditions (optional)	– The CSPs(SaaS) form a federation pattern of inter-cloud. – The CSPs(SaaS) use a third-party SSO system for implementing SSO authentication functionality within their federation.
Post-conditions (optional)	– The CSC is able to access various services offered by different CSPs once it is successfully authenticated by any member of the CSPs(SaaS) federation.
Derived requirements	– SSO authentication (refer to clause 7.4). – Periodical verification (refer to clause 7.5).

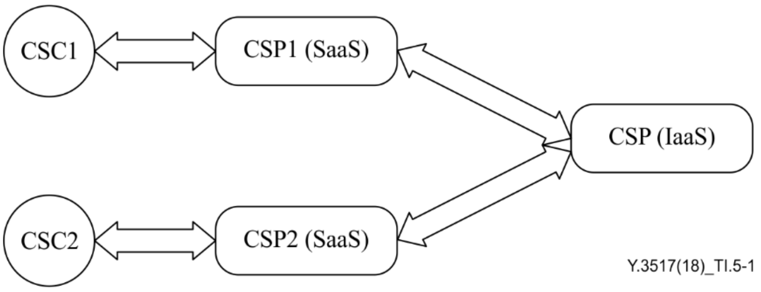
I.5 Use case of control privilege of inter-cloud

This use case illustrates security and control concerns in inter-cloud. The peering pattern of inter-cloud used to illustrate the use case is an example only.

Table I.5 – Control privilege of inter-cloud

Title	Control privilege of inter-cloud
Description	– The CSC requests SaaS service from CSPs(SaaS); – Both CSP1(SaaS) and CSP2(SaaS) use infrastructure including computing and storage resources from CSP (infrastructure as a service (IaaS)) to provide their cloud services. Therefore, they all have service instances and data in CSP(IaaS); – For the sake of CSPs(SaaS) data security and privacy, CSP(IaaS) control over the infrastructure should be limited to avoid inspection or analysis of CSPs(SaaS) data and VM instances without explicit CSPs(SaaS) consent; – CSPs(SaaS) should be able to exercise fine-grained control over protection of their cloud resources according to a given security SLA. This means that CSPs(SaaS) should be able to actively monitor their allocated resources; – CSPs(SaaS) should not be authorized to monitor or modify VM state, service data and CSC data from other CSCs.
Roles	CSCs, CSPs(SaaS), CSP(IaaS).

Table I.5 – Control privilege of inter-cloud

Figure (optional)	 CSC1 CSP1 (SaaS) CSP (IaaS) CSC2 CSP2 (SaaS) Y.3517(18)_TI.5-1
Pre-conditions (optional)	– The CSPs(SaaS) and CSP(IaaS) form peering pattern of inter-cloud.
Post-conditions (optional)	
Derived requirements	– Control privilege for VM and data (refer to clause 7.6).

Appendix II

Functionalities for managing isolation and security mechanism

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

This appendix provides functionalities for managing isolation and security mechanisms.

II.1 Functionalities for managing isolation and security mechanism

The functionalities for managing isolation and security mechanisms are supported by the 'authentication and identity management", "authorization and security policy management", "encryption management" and "platform and virtualization management" functional components within the multi-layer functions of the cloud computing reference architecture [ITU-T Y.3502]. The positioning of these functionalities for managing isolation and security mechanisms across the CSPs, which provide inter-cloud services, is presented in Figure II.1.

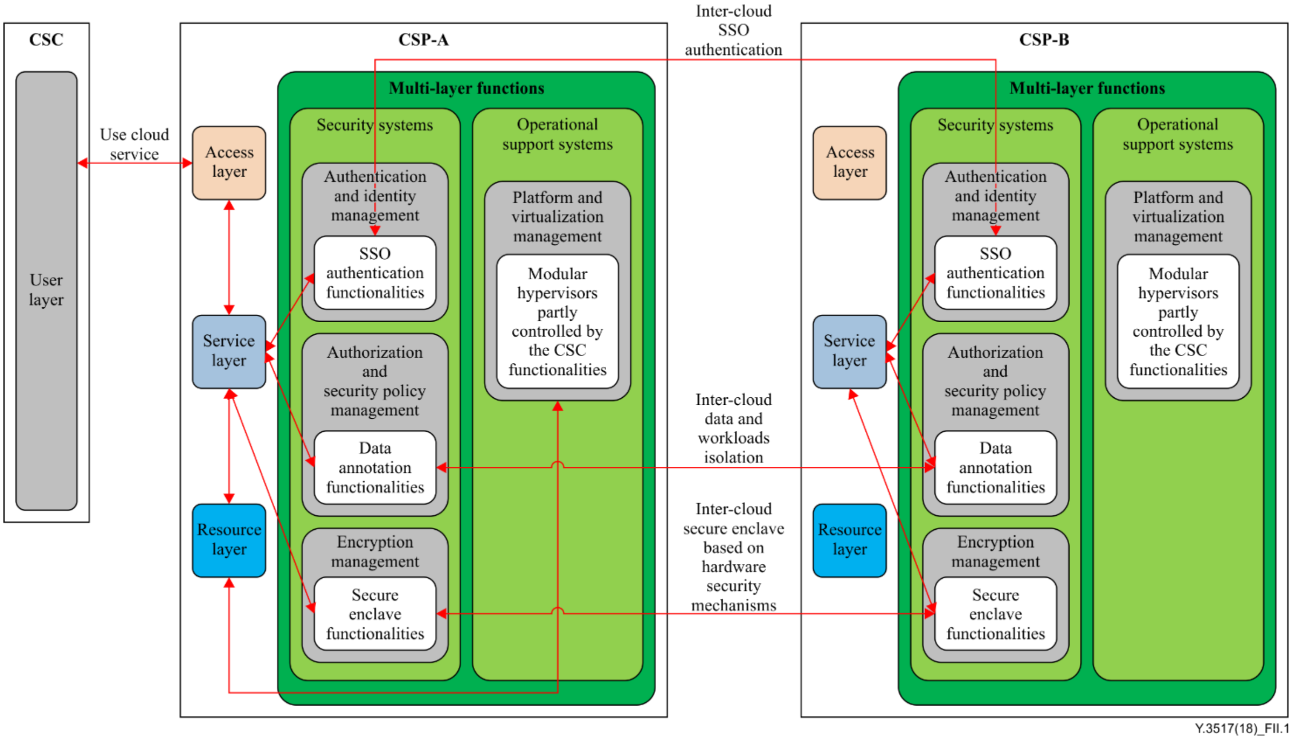

CSC
User layer
Use cloud service
CSP-A
Access layer
Service layer
Resource layer
Multi-layer functions
Security systems
Authentication and identity management
SSO authentication functionalities
Authorization and security policy management
Data annotation functionalities
Encryption management
Secure enclave functionalities
Operational support systems
Platform and virtualization management
Modular hypervisors partly controlled by the CSC functionalities
Inter-cloud SSO authentication
Inter-cloud data and workloads isolation
Inter-cloud secure enclave based on hardware security mechanisms
CSP-B
Access layer
Service layer
Resource layer
Multi-layer functions
Security systems
Authentication and identity management
SSO authentication functionalities
Authorization and security policy management
Data annotation functionalities
Encryption management
Secure enclave functionalities
Operational support systems
Platform and virtualization management
Modular hypervisors partly controlled by the CSC functionalities
Y.3517(18)_FII.1

Figure II.1 – The positioning of functionalities for managing isolation and security mechanisms in inter-cloud

The data annotation functionalities are built upon elements as follows:

- **Data annotation definer:** manages the terminology (language) to annotate (or tag) workloads and data;
- **Data annotation manager:** responsible for annotating the workloads and data according to the isolation and security requirements;
- **Data annotation handler:** responsible for parsing and executing the isolation and security requirements based on the annotations of workloads and data.

The modular hypervisors partly controlled by the CSC functionalities are built upon elements as follows:

- **User domain manager:** responsible for building and managing the per-user administrative domain and user domains for each user;
- **System domain manager**: responsible for building and managing the system-wide administrative domain.

The secure enclave based on hardware security mechanisms functionalities are built upon elements as follows:

- **Secure enclave library:** responsible for implementing encrypted networking using transport layer security (TLS) (e.g., using a standard TLS library), encrypted and sealed storage, attestation, and inter-process communication. These are features that are exposed to the application code. Cloud service developers use these secure primitives to write their secure cloud service.
- **Discrete security chips coupled with processor features:** responsible for providing the necessary underlying capabilities to implement secure enclave.

The SSO authentication functionalities are built upon elements as follows:

- **User request handler:** responsible for accepting the identity information provided by the cloud service user and forwarding this information to the identity management system;
- **Identity management system:** responsible for authenticating CSC requests and sharing the result of this authentication to inter-cloud members. It is also responsible for managing the identity information of its associated inter-cloud members.

Bibliography

[b-ITU-T Y.3500]	Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.
[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 19086-2]	ISO/IEC 19086-2:2018, *Information technology – Cloud computing – Service level agreement (SLA) framework – Part 2: Metric model*.

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