International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3518

(12/2018)

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

Cloud Computing

Cloud computing – Functional requirements of inter-cloud data management

Recommendation ITU-T Y.3518

ITU-T

International Telecommunication Union

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.3518

Cloud computing – Functional requirements of inter-cloud data management

Summary

Recommendation ITU-T Y.3518 provides the overview of inter-cloud data management and its functional requirements. It describes typical use cases and specifies functional requirements for three aspects, namely inter-cloud data policy, inter-cloud data isolation and protection, as well as inter-cloud data management, which are derived from the corresponding use cases.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3518	2018-12-14	13	11.1002/1000/13815

Keywords

Inter-cloud; data management; inter-cloud data policy; inter-cloud data isolation and protection.

[*] 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

Page

Recommendation ITU-T Y.3518

Cloud computing – Functional requirements of inter-cloud data management

1 Scope

This Recommendation provides the overview and functional requirements of inter-cloud data management. This Recommendation consists of:

– the overview of inter-cloud data management;

– functional requirements for inter-cloud data policy;

– functional requirements for inter-cloud data isolation and protection;

– functional requirements for inter-cloud data management.

This Recommendation also provides an appendix describing use cases aimed at deriving the corresponding functional requirements.

2 References

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

[ITU-T X.1601]	Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*
[ITU-T Y.3502]	Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*
[ITU-T Y.3511]	Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing.*
[ITU-T Y.3600]	Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*
[ITU-T Y.3601]	Recommendation ITU-T Y.3601 (2018), *Big data – Framework and requirements for data exchange.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 cloud service category [b-ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.

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

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

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

3.1.5 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.

3.1.6 Network as a Service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.7 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.1.8 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 inter-cloud data policy decision point (IDPDP): An inter-cloud environment entity that makes authorization decision and negotiation of inter-cloud data processes and usage.

3.2.2 inter-cloud data policy enforcement point (IDPEP): An inter-cloud environment entity that implements data policy decision of an inter-cloud data policy decision point (IDPDP) (see clause 3.2.1).

3.2.3 inter-cloud data policy information point (IDPIP): An inter-cloud environment entity that stores the data policy.

3.2.4 inter-cloud data policy administration point (IDPAP): An inter-cloud environment entity that administrates data policies.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Program Interface
BSS	Business Support System
CPPL	Compact Privacy Policy Language
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DPL	Data Policy Language
IDPAP	Inter-cloud Data Policy Administration Point
IDPDP	Inter-cloud Data Policy Decision Point
IDPEP	Inter-cloud Data Policy Enforcement Point
IDPIP	Inter-cloud Data Policy Information Point
KPI	Key Performance Indicator
NaaS	Network as a Service
NFV	Network Function Virtualization
OSS	Operational Support System
PaaS	Platform as a Service

SaaS	Software as a Service
SDN	Software-Defined Networking
SW	Software
vHGW	virtual Home Gateway
XML	extensible Markup Language

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 data management

Nowadays, one of the main challenges for cloud service providers (CSPs) is to ensure credibility of data storage and transport in multi-cloud environments. Inter-cloud data management functions need to consider and reflect security and governance aspects of data handling uniformity and interoperability across different CSPs.

Inter-cloud data categorization in aspects of identification qualifiers and dependency, as well as inter-cloud data annotation, processing and usage, is necessary to attain the data treatment required among multiple CSPs. The appropriate security and access control mechanisms determine access control to inter-cloud data under particular conditions (e.g., temporarily, a certain number of times or related to a particular community and context).

With the development and wide usage of big data-related technologies, more and more data and datasets are stored in geographically distributed and heterogeneous computing environments, also known as inter-cloud environments (e.g., in a high-performance computing scenario). Migrating an application from a centralized or static place to the distributed computing environments may bring the following challenges:

1) transmission of intensive data among different CSPs may cause low data access efficiency;

2) heterogeneous dataset access and sharing may bring extra computation consumption;

3) the necessary and unavoidable maintenance of extensive tracking of metadata, data locations, access control policies, etc.

NOTE – Intensive data transmission and heterogeneous dataset access and sharing-related technologies lie outside the scope of this Recommendation.

[ITU-T Y.3601] specifies the big data exchange framework and requirements based on the big data ecosystem and capabilities specified in [ITU-T Y.3600]. In [ITU-T Y.3601], data exchange is described as a process of receiving source data under a source schema from data source, transforming it into target data under a target schema without altering the representation of source data, and delivering the target data to the data target. This Recommendation focuses on the inter-cloud data management aspects and does not aim to specify any concrete data exchange details. For more information about big data exchange, please refer to [ITU-T Y.3601].

6.1 Inter-cloud data categorization

[b-ISO/IEC 19944] identifies the categories of data that flow across cloud service customer (CSC) devices and cloud services, and can be captured, processed, used and shared. It extends the definitions of CSC data, cloud service-derived data, CSP data and account data. This Recommendation follows the taxonomy of data in [b-ISO/IEC 19944] and focuses on the inter-cloud data aspect. Similarly to [b-ISO/IEC 19944], this Recommendation is not intended to be exhaustive, but is intended to be extensible. It is recommended that the hierarchical relationship based on the four topmost categories defined in [b-ISO/IEC 19944] be maintained.

6.2 Data policy language

The data policy language (DPL) allows CSPs to annotate, manage, process and use CSC or CSP data in an inter-cloud environment (who can do what and when) according to data policies in force. The main challenges for DPL are related to small storage footprint, human readability, detection of conflicts at time of specification, performance and adaptation to new policy statements that come up with emerging inter-cloud services. The DPL expresses inter-cloud data policies for different cloud service categories [e.g., NaaS, SaaS, platform as a service (PaaS)] provided by the CSPs in an inter-cloud environment.

6.3 Inter-cloud data policy-based management

Inter-cloud data policy-based management enables peer CSPs to control and evaluate who can access which inter-cloud data, how to manage inter-cloud data, how to process and use inter-cloud data.

The main elements of data policy-based management in inter-cloud are as follows.

– An IDPDP collects information about available resources and corresponding properties of the peer CSPs to decide which of these CSP can process and use the inter-cloud data from peer CSPs. The functionalities of IDPDP depend on role-based, rule-based and context-based data policies applied in inter-cloud computing.

– An IDPEP is responsible for enforcing the terms of a CSC or CSP access. This enforcement is run-time based on the capabilities of the IDPEP.

– An IDPIP is a repository of information to support the access decision.

– An IDPAP provides inter-cloud administration, management and monitoring of entitlement policies, as well as delegation and integration with inter-cloud information repositories.

Figure 6-1 illustrates how an IDPAP and IDPIP are related with each other to operate data management policies for a data supplier, and shows that an IDPEP, IDPDP and IDPIP cooperate for a data customer to access data based on policies set by the data supplier.

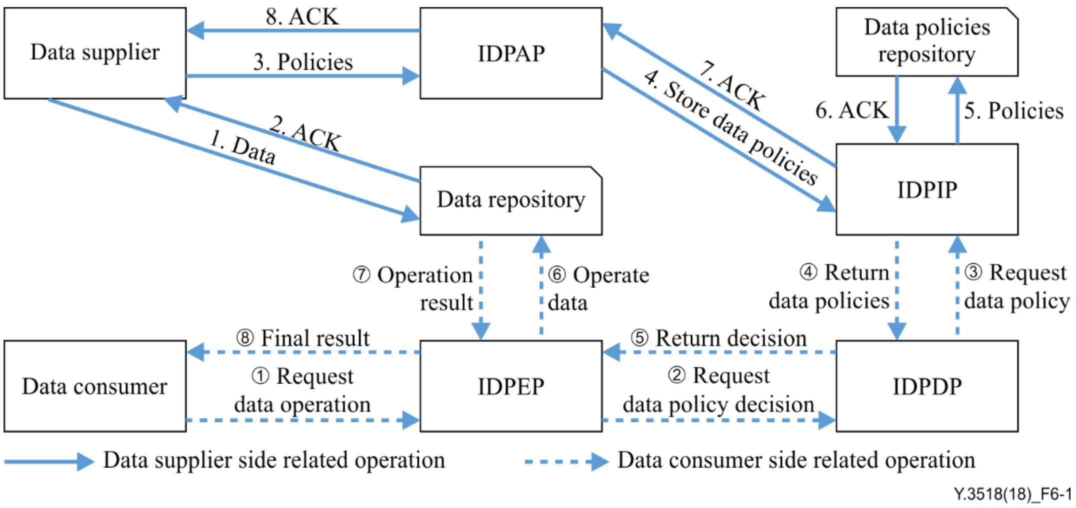


Figure 6-1 – Relationship of main elements in inter-cloud data policy-based management

In Figure 6-1, the data supplier generates and provides data, and also sets the data policies. The data customer uses the data that is provided by the data supplier and processed by policy-based management.

The data supplier side-related operations can be described as the following procedure.

1) The data supplier provides the data to the data repository.

2) The data repository sends an acknowledgement to the data supplier.

3) The data supplier sets the corresponding data policies, which are managed by the IDPAP.

4) The IDPAP requests the IDPIP to store the data policies.

5) The IDPIP stores the data policies in the data policies repository.

6) The data policies repository sends an acknowledgement to the IDPIP.

7) The IDPIP sends an acknowledgement to the IDPAP.

8) The IDPIP sends an acknowledgement to the data supplier.

The data consumer side-related operations can be described as the following procedure.

1) The data consumer requests a data operation from the IDPEP.

2) The IDPEP requests a data policy decision from the IDPDP.

3) The IDPDP requests the specific data policy from the IDPIP.

4) The IDPIP returns the requested data policy to the IDPDP.

5) The IDPDP returns the decision result to the IDPEP based on the collected available resources.

6) The IDPEP performs the data operation based on the data policies.

7) The processed data result is returned to the IDPEP.

8) The IDPEP provides the final results of the data operation to the data consumer.

6.4 Relationship with cloud computing reference architecture

[ITU-T Y.3502] specifies two functional components to support inter-cloud computing, also known as peer service integration (see clause 9.2.5.1.4 of [ITU-T Y.3502]) and peer service management (see clause 9.2.5.3.9 of [ITU-T Y.3502]). [ITU-T Y.3516] identifies an inter-cloud specific extension to the functional components of [ITU-T Y.3502] that are part of integration, security systems, operational support system (OSS) and business support system (BSS) (see clause 8 of [ITU-T Y.3516]). This Recommendation is based on the functions defined in [ITU-T Y.3502] and [ITU-T Y.3516] on inter-cloud computing and does not define or extend any new functions. This Recommendation focuses on data management in the inter-cloud environment based on the establishment of a relationship (pattern) among multiple peer CSPs, including peering, federation and intermediary, which are defined in [ITU-T Y.3511].

7 Functional requirements for inter-cloud data policy

This clause provides the functional requirements for inter-cloud data policy derived from the use cases described in Appendix I.

7.1 Data policy language

It is recommended that the CSP support inter-cloud data policy to satisfy data processing and usage.

It is recommended that the CSP support the DPL to annotate (tagging) cloud workloads.

It is recommended that the CSP support inter-cloud data annotation (tagging) in order to realize the CSC request.

7.2 Inter-cloud data policy administration point

It is recommended that the CSP support the IDPAP to administer data policies in inter-cloud.

7.3 Inter-cloud data policy information point

It is recommended that the CSP support the IDPIP to store the data policy provided by the CSC in inter-cloud.

7.4 Inter-cloud data policy decision point

It is recommended that the CSP support the IDPDP to enforce the data policy on the basis of information collected by the IDPEP about data processing and usage among peer CSPs in inter-cloud.

7.5 Inter-cloud data policy enforcement point

It is recommended that the CSP support the IDPEP to implement the data policy decision of the IDPDP in the inter-cloud environment.

It is recommended that the CSP support the IDPEP to collect information about data processing and usage among peer CSPs in inter-cloud and deliver this information to the IDPDP.

7.6 Inter-cloud data policy monitoring

It is recommended that the CSP support real-time data policy monitoring in inter-cloud to fulfil the data policy provided by the CSC.

7.7 Inter-cloud dynamic data policy management

It is recommended that the CSP support dynamic data policy management in inter-cloud to fulfil the data policy provided by the CSC.

7.8 Inter-cloud autonomic data policy management

It is recommended that the CSP support autonomic data policy management in inter-cloud to fulfil the data policy provided by the CSC.

7.9 Inter-cloud cognitive data policy management

It is recommended that the CSP support cognitive data policy management in inter-cloud to fulfil the data policy provided by the CSC.

8 Functional requirements for inter-cloud data isolation and protection

This clause provides the functional requirements for inter-cloud data isolation and protection derived from the use cases described in Appendix I.

8.1 Datasets placement policies among different CSPs

It is recommended that CSPs support dataset placement policies for data-intensive applications in geographically distributed data centres.

NOTE 1 – The conditions of placement policy include, but are not limited to, the time cost of data transmission, storage space, network performance and dataset dependencies.

NOTE 2 –Dataset placement policies themselves lie outside the scope of this Recommendation. For example, in some specific scenario, because the same set of raw data needs to be accessed by many CSCs, duplication/splitting can be selected as part of the dataset placement policies.

8.2 Data movement regulation across geographical borders

It is recommended that the CSP identify the different data movement regulations once the data needs to flow across geographical borders and provides the solution, if necessary and possible.

It is recommended that the CSP support the mechanisms to monitor the validity of the data movement regulations at geographical borders and provides the negotiation, if necessary and possible.

9 Functional requirements for inter-cloud data management

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

9.1 Inter-cloud data use policies

It is required that the CSP support data use policy in order to realize a CSC request.

It is recommended that the CSP integrate and validate services from multiple CSPs as an aspect of inter-cloud data use policy.

It is recommended that the CSP support inter-cloud data classification in order to realize a CSC request.

9.2 Secure data management of the SaaS replication model in inter-cloud

It is required that the CSP provide functionalities of data integrity management to check whether the data is identical to that of other CSPs.

It is recommended that the CSP provide to CSCs secure application program interfaces (APIs) to access SaaS securely.

9.3 Secure data management of the SaaS partition model in inter-cloud

It is required that the CSP provide functionalities for data identity management for software logic to find appropriate data and avoid data duplication among SaaSs.

It is recommended that the CSP provide cloud storage support data encryption functionalities to protect data.

9.4 Secure data management of the SaaS data partition model in inter-cloud

It is required that the CSP provide merging functionalities to incorporate new data into an already existing dataset.

It is recommended that the CSP provide functionalities for integrated key management among CSPs so that encryption/decryption SaaS data can merge.

10 Security considerations

Security aspects for consideration within the cloud-computing environment, including inter-cloud computing, are addressed by security challenges for CSPs as 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 inter-cloud data management

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

This appendix includes inter-cloud data management-related use cases from which the corresponding functional requirements are derived.

I.1 Use case template

The use cases developed in this appendix adopt the format in Table I.1 for better readability and convenient material organization.

Table I.1 – Use case template table

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, but 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 clause.

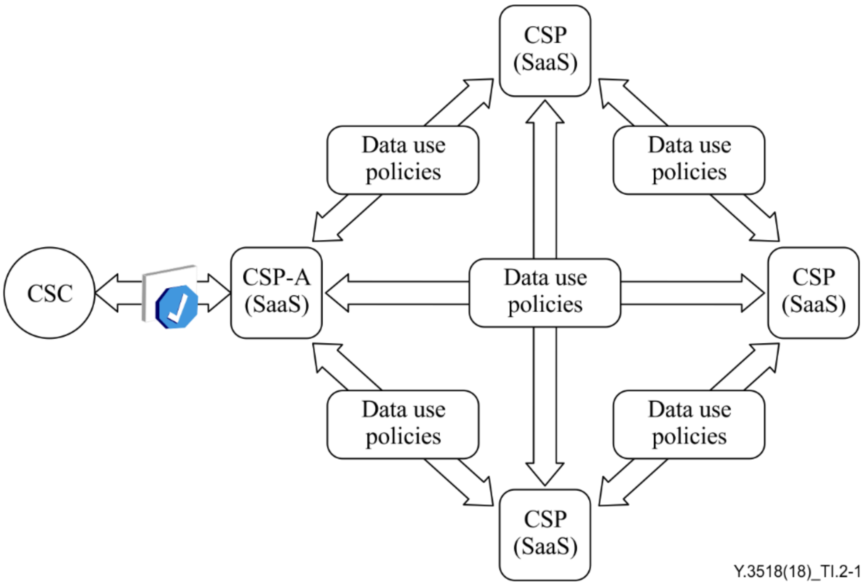
I.2 Use case of data use policies in inter-cloud

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

Table I.2 – Data use policies in inter-cloud

Title	Data use policies in inter-cloud
Description	The CSC requests SaaS, which operates its data in specific countries. The CSP-A (SaaS) acts in an inter-cloud federation pattern among CPSs (SaaS) and becomes the contact point for the CSC. The CSP-A (SaaS) determines and validates appropriate data use policies or principles that allow exchange and operational use of CSC data among the inter-cloud federation. If the CSP (SaaS) operates out of specific countries, CSC data is not exchanged.
Roles	CSC, CSP (SaaS).

Table I.2 – Data use policies in inter-cloud

Figure (optional)	 CSP (SaaS) Data use policies Data use policies CSC CSP-A (SaaS) Data use policies CSP (SaaS) Data use policies Data use policies CSP (SaaS) Y.3518(18)_TI.2-1
Pre-conditions (optional)	The CSPs (SaaS) forms an inter-cloud federation pattern.
Post-conditions (optional)	The CSPs (SaaS) implement data use policy in their management system.
Derived requirements	Inter-cloud data use policies (refer to clause 9.1).

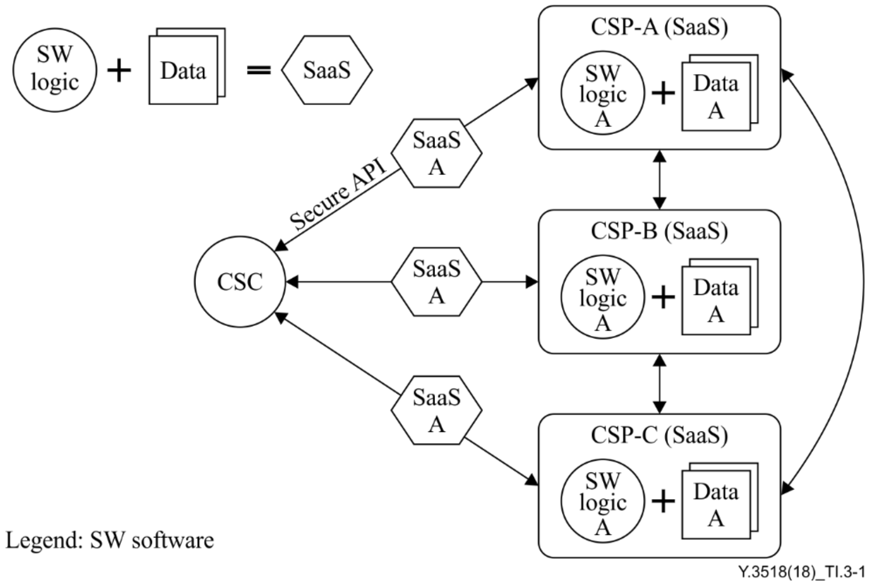
I.3 Use case of secure data management of the SaaS replication model in inter-cloud

This use case illustrates secure data management of the SaaS replication model in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.3 – Secure data management of the SaaS replication model in inter-cloud

Title	Secure data management of the SaaS replication model in inter-cloud
Description	The SaaS replication model, deployed on multiple CSPs, that combines software logic and data into one service enables the user to get evidence of the integrity of the result among multiple CSPs in order to guarantee that an operation performed in a cloud system has not been tampered with by the CSP or attackers.
Roles	CSC, CSP (SaaS)

Table I.3 – Secure data management of the SaaS replication model in inter-cloud

Figure (optional)	 SW logic + Data = SaaS CSP-A (SaaS) SW logic A Data A SaaS A Secure API CSP-B (SaaS) CSC SaaS A SW logic A Data A SaaS A CSP-C (SaaS) SW logic A Data A Legend: SW software Y.3518(18)_TI.3-1
Pre-conditions (optional)	The CSPs form an inter-cloud federation pattern.
Post-conditions (optional)	
Derived requirements	Data integrity among CSPs (see clause 9.2) Secure APIs (see clause 9.2)

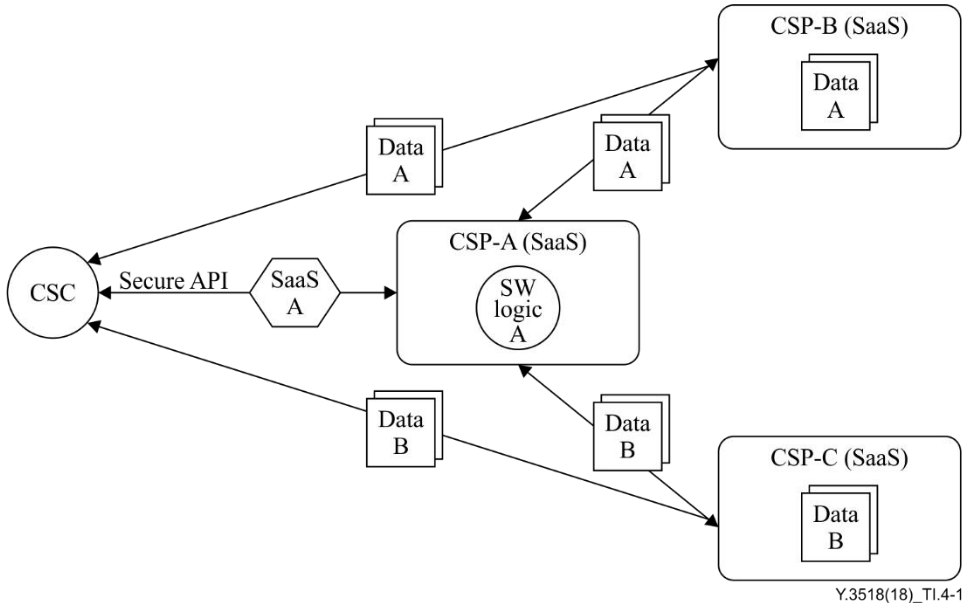
I.4 Use case of secure data management of the SaaS partition model in inter-cloud

This use case illustrates secure data management of the SaaS partition model in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.4 – Secure data management of the SaaS partition model in inter-cloud

Title	Secure data management of the SaaS partition model in inter-cloud
Description	This case separates software logic and data, and deploys them on each CSP to consider any inadvertent data breach during execution of cloud services in third party CSPs. This case considers data protection from malicious CSP threats. For example, the software logic is deployed on CSP-A and data A, B are stored on reliable cloud storage providers, CSP-B and CSP-C, respectively; the CSP-A provides the SaaS securely using data A and B stored on CSP-B and CSP-C.
Roles	CSC, CSP (SaaS)

Table I.4 – Secure data management of the SaaS partition model in inter-cloud

Figure (optional)	 CSP-B (SaaS) Data A Data A Data A CSP-A (SaaS) SW logic A CSC Secure API SaaS A Data B Data B CSP-C (SaaS) Data B Y.3518(18)_TI.4-1
Pre-conditions (optional)	The CSPs (SaaS) form an inter-cloud federation pattern.
Post-conditions (optional)	
Derived requirements	Unique data identity management (see clause 9.3) Data encryption in cloud storage (se clause 9.3)

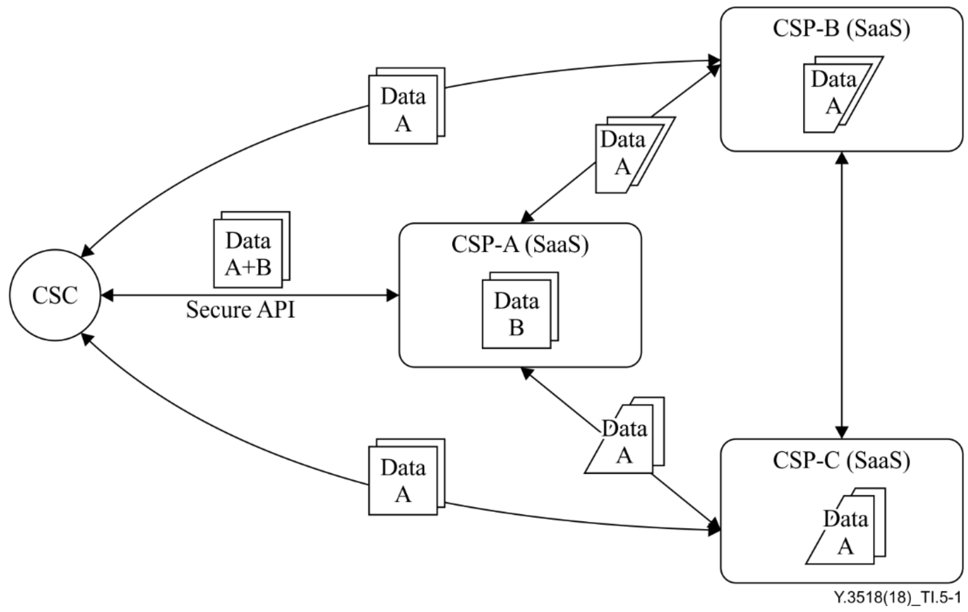
I.5 Use case of secure data management of the SaaS data partition model in inter-cloud

This use case illustrates secure data management of the SaaS data replication model in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.5 – Secure data management of the SaaS data partition model in inter-cloud

Title	Secure data management of the SaaS data partition model in inter-cloud
Description	This case partitions data and distributes fine-grained fragments of data to distinct clouds. None of the CSPs involved gains access to all the data, which safeguards data confidentiality. Data is partitioned by two methods according to data type. In unstructured data (e.g., picture, document), data can be partitioned using cryptographic data splitting. In database or structured data [e.g., extensible markup language (XML) data, log], data can be partitioned by distributing different parts of the data to different cloud service providers (CSP-A, CSP-B and CSP-C).
Roles	CSC, CSP (SaaS)

Table I.5 – Secure data management of the SaaS data partition model in inter-cloud

Figure (optional)	 CSP-B (SaaS) Data A Data A Data A Data A+B CSC Secure API CSP-A (SaaS) Data B Data A Data A CSP-C (SaaS) Data A Y.3518(18)_TI.5-1
Pre-conditions (optional)	The CSPs (SaaS) form an inter-cloud federation pattern.
Post-conditions (optional)	
Derived requirements	Merging technologies for encrypted data (see clause 9.4) Integrated key management (see clause 9.4)

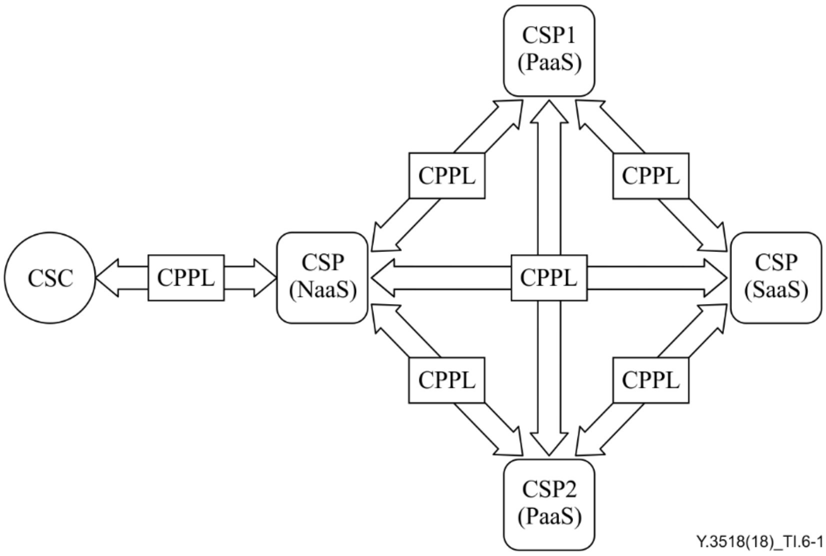
I.6 Use case of data policy language

This use case illustrates inter-cloud data annotation, processing and usage aspects between CSC and CSP or between CSPs. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.6 – Data policy language

Title	Data policy language
Description	A CSP (NaaS) offers access to Internet (service) over virtual home gateway (vHGW) facilities using network functions virtualization (NFV) and software-defined networking (SDN) technologies. The CSP (NaaS) forms an inter-cloud federation pattern with a group of peer CSPs [here CSPs (PaaS) and CSP (SaaS)] to optimize its own resources and leverage area of service availability. The CSP (NaaS) uses a data policy language to annotate, process and use vHGW data in the inter-cloud environment. The CSP (NaaS) monitors service (here access to Internet) to ensure that particular key performance indicators (KPIs) are respected (e.g., energy efficiency, resource optimization, performance). In the case of a given KPI cross threshold, the service (here access to Internet) is automatically reallocated among members of the federation that respect data policy determined by the CSP (NaaS).
Roles	CSC, CSP (NaaS), CSP (PaaS), CSP (SaaS)

Table I.6 – Data policy language

Figure (optional)	 CSP1 (PaaS) CPPL CPPL CSC CPPL CSP (NaaS) CPPL CSP (SaaS) CPPL CPPL CSP2 (PaaS) Y.3518(18)_TI.6-1 CPPL: compact privacy policy language
Pre-conditions (optional)	The CSP (NaaS), CSPs (PaaS) and CSP (SaaS) form an inter-cloud relationship to optimize their own resources and leverage area of service availability.
Post-conditions (optional)	The CSP (NaaS) establishes service chaining (here vHGW) between the CSC (PaaS) and CSP (SaaS). The CSP (NaaS) uses data policy language. The CSP (NaaS) reallocates service (here access to Internet) between CSPs in the federation if KPIs drop below threshold (e.g., energy efficiency, resource optimization).
Derived requirements	Data policy language (see clause 7.1)

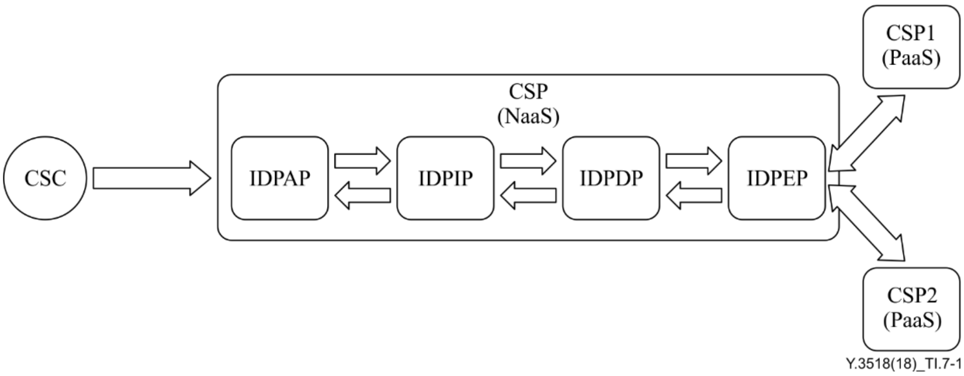
I.7 Use case of CSC data policy implementation in inter-cloud

This use case illustrates inter-cloud data policy processing and usage aspects between CSC and CSP or between CSPs. The inter-cloud intermediary pattern used to illustrate the use case is an example only.

Table I.7 – CSC data policy implementation in inter-cloud

Title	CSC data policy implementation in inter-cloud
Description	The CSP (NaaS) offers access to Internet (service) over virtual home gateway (vHGW) facilities using network functions virtualization (NFV) and software-defined networking (SDN) technologies. The CSP (NaaS) is involved in an inter-cloud intermediary pattern with two peer CSPs (PaaS), i.e., CSP1 (PaaS) and CSP2 (PaaS). The CSP (NaaS) respects data policy related to vHGW data in the inter-cloud environment. The CSP (NaaS) uses inter-cloud data policy management to process and use inter-cloud data. The CSP (NaaS) lets the CSC provide data policy related to CSC workloads passing into the inter-cloud environment. The IDPAP acts as access control for CSC data policies. The data policies are stored at the IDPIP. The IDPDP collects information about available resources and corresponding policies of peer CSPs to be able to decide which CSP can process and use vHGW data. The IDPEP establishes the service (here vHGW) between the CSP (NaaS) and one of CSP1 (PaaS) and CSP2

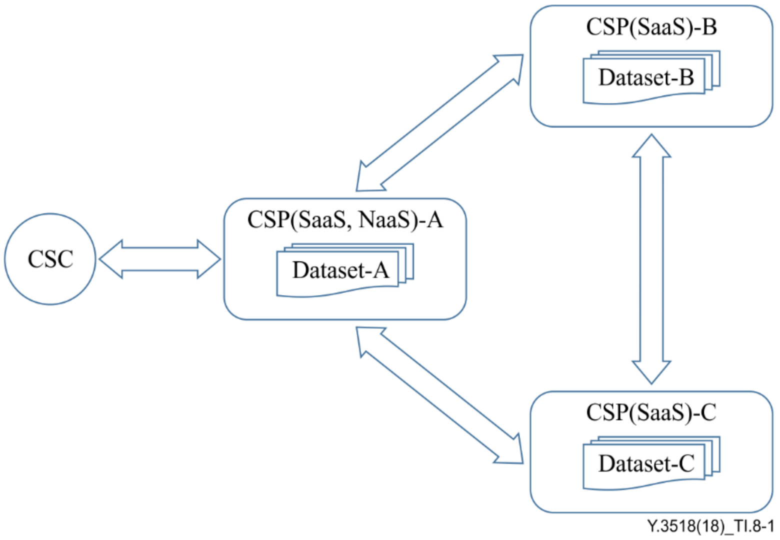
Table I.7 – CSC data policy implementation in inter-cloud

	(PaaS) selected by the DPDP. The IDPEP is responsible for monitoring the inter-cloud environment and fulfilment of CSC data policy. In the case of violation, the IDPEP triggers the IDPDP to establish the service (here vHGW) between the CSP (NaaS) and other CSPs, which fulfils the CSC data policy.
Roles	CSC, CSP (NaaS), CSP1 (PaaS), CSP2 (PaaS)
Figure (optional)	 CSP1 (PaaS) CSP (NaaS) CSC IDPAP IDPIP IDPDP IDPEP CSP2 (PaaS) Y.3518(18)_TI.7-1
Pre-conditions (optional)	The CSP (NaaS) has an inter-cloud relationship with two CSPs (PaaS), i.e., CSP1 (PaaS) and CSP2 (PaaS). The CSP (NaaS) respects data policy.
Post-conditions (optional)	The CSP (NaaS) supports inter-cloud data policy management. The IDPAP acts as access control for the CSC data policy and delivers policies to the IDPIP. The IDPIP stores data policies provided by the CSC. The IDPDP selects the policy on the basis of collected information about data processing and usage among peer CSPs. The IDPDP decides which CSP processes and uses vHGW data. The IDPEP implements decisions of the IDPDP in the inter-cloud environment.
Derived requirements	Inter-cloud data policy administration point (see clause 7.2) Inter-cloud data policy information point (see clause 7.3) Inter-cloud data policy decision point (see clause 7.4) Inter-cloud data policy enforcement point (see clause 7.5) Inter-cloud data policy monitoring (see clause 7.6) Inter-cloud dynamic data policy management (see clause 7.7) Inter-cloud autonomic data policy management (see clause 7.8) Inter-cloud cognitive data policy management (see clause 7.9)

I.8 Use case of data placement policies for data-intensive applications in the inter-cloud environment

This use case illustrates data placement policies for data-intensive applications in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

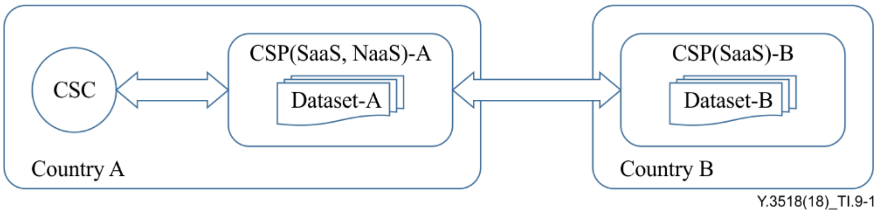
Table I.8 – Data placement policies for data-intensive applications in the inter-cloud environment

Title	Data placement policies for data-intensive applications in the inter-cloud environment
Description	Data-intensive applications are widely used in an increasing number of fields, e.g., high-energy physics, bioinformatics and astronomy. There are several challenges if the datasets required by this kind of application, including already existing data, intermediate data and final data, should be placed in the inter-cloud environment. Therefore, it is essential for federated CSPs to negotiate an appropriate placement policy for the different datasets. The placement policy conditions include, but are not limited to, the time cost of data transmission, storage space, network performance and data dependencies. The following aspects are described as the illustrations. – The transmission of data among different CSPs is inevitable. On one hand, the data scale is huge and the bandwidth limited; on the other, sometimes, there are several datasets limited to location in some specific CSP based on application logic. Consideration of how to reduce the time cost of data movements is required. – There are dependencies among these different datasets placed in different CSPs. Consideration of how to maintain these dependencies is required in order to improve calculation efficiency.
Roles	CSC, CSP (SaaS), CSP (NaaS, SaaS)
Figure (optional)	 CSP(SaaS)-B Dataset-B CSC CSP(SaaS, NaaS)-A Dataset-A CSP(SaaS)-C Dataset-C Y.3518(18)_TI.8-1
Pre-conditions (optional)	The CSPs form an inter-cloud federation pattern. The datasets need placement in different CSPs. There are dependencies among these datasets.
Post-conditions (optional)	
Derived requirements	Dataset placement policies among different CSPs (see clause 8.1)

I.9 Use case of data regulation across different countries in the inter-cloud environment

This use case illustrates data regulation across different countries in the inter-cloud. The inter-cloud peering pattern used to illustrate the use case is an example only.

Table I.9 – Data regulation across different countries in the inter-cloud environment

Title	Data regulation across different countries in the inter-cloud environment
Description	With the development of industrial globalization, data movement across geographical borders in the inter-cloud environment is increasingly frequent. However, data movement regulation varies significantly in different counties in several aspects, e.g., data ownership, privacy protection, law application and jurisdiction, as well as international trade rules. Therefore, the CSP needs to identify the various data movement regulations once data needs to flow across geographical borders and provide the solution, if necessary and possible. For example, when the CSC requests SaaS service requiring datasets located separately in country A and country B, CSP-A acts in an inter-cloud federation pattern among CSPs and becomes the contact point for the CSC. CSP-A needs to monitor the validity of the data movement regulation of country B and negotiate between country A and country B, if necessary and possible.
Roles	CSC, CSP (SaaS), CSP (NaaS, SaaS)
Figure (optional)	 CSC CSP(SaaS, NaaS)-A Dataset-A Country A CSP(SaaS)-B Dataset-B Country B Y.3518(18)_TI.9-1
Pre-conditions (optional)	The CSPs form an inter-cloud federation pattern. The data needs to flow across borders of countries that have different data movement regulations.
Post-conditions (optional)	
Derived requirements	Data movement regulation across geographical borders (see clause 8.2)

Bibliography

[b-ITU-T Y.3500]	Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.
[b-ISO/IEC 19944]	International Standard ISO/IEC 19944:2017, *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*.

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