ITU Workshop on “Future Trust and Knowledge Infrastructure”, Phase 2
Geneva, Switzerland
1 July 2016

Trusted Inter-Cloud Challenges

Dr Emil Kowalczyk
Orange Polska, Emil.Kowalczyk@orange.com

Motivation

Inter-cloud from Customer perspective:

- avoid vendor lock-in
- distribution across geographies
- utilizing service resources from multiple providers

Inter-cloud from Service Provider perspective:

- scalability and wide resource availability
- cloud data management
- cost efficiency and energy savings

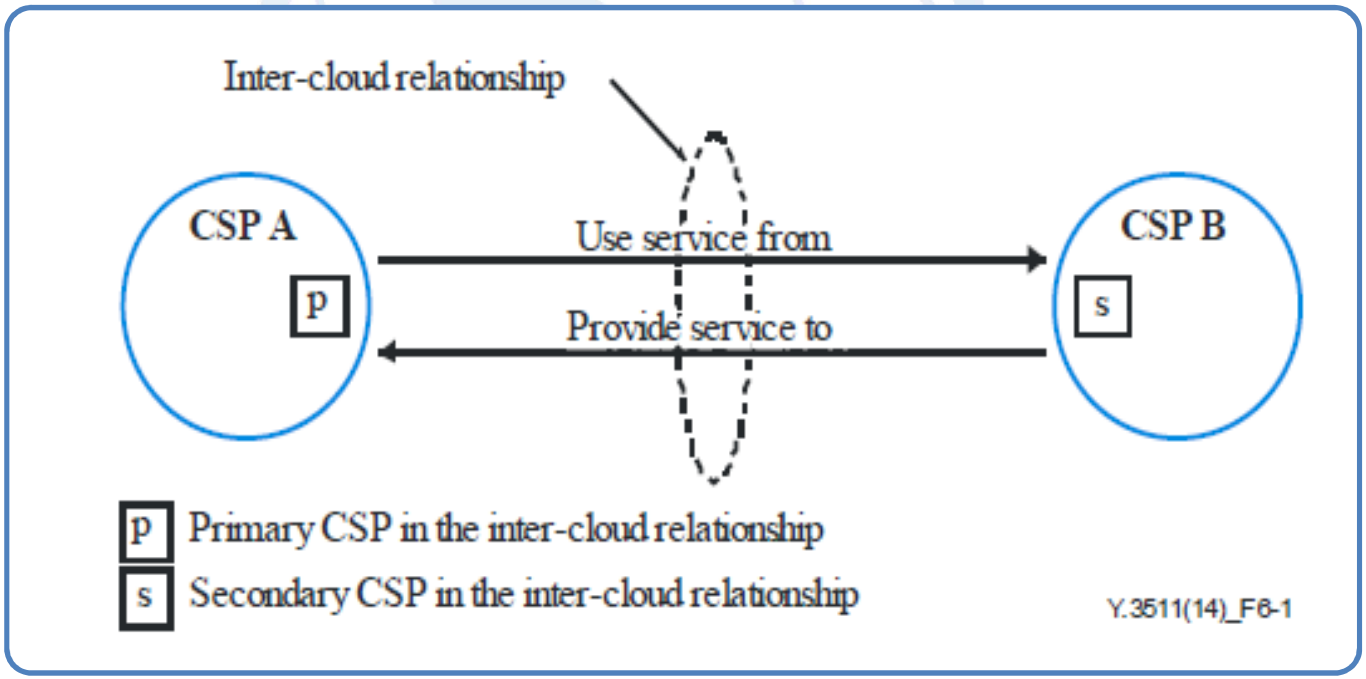
Technical aspects of inter-cloud

1) **Y.3500/ISO 17789: Cloud computing - Overview and Vocabulary***
2) Y.3501: Cloud computing framework and high-level requirements
3) **Y.3502/ISO 17788: Cloud computing - Reference architecture***
4) Y.3510: Cloud Computing Infrastructure Requirements
5) Y.3511: Framework of inter-cloud computing
6) Y.3520: Cloud Computing framework for end-to-end resource management
7) Y.3521: Overview of end-to-end cloud computing management
8) X.1601: Security framework for cloud computing

*** Common text with ISO/IEC JTC1 SC38/WG3**

Inter-cloud computing

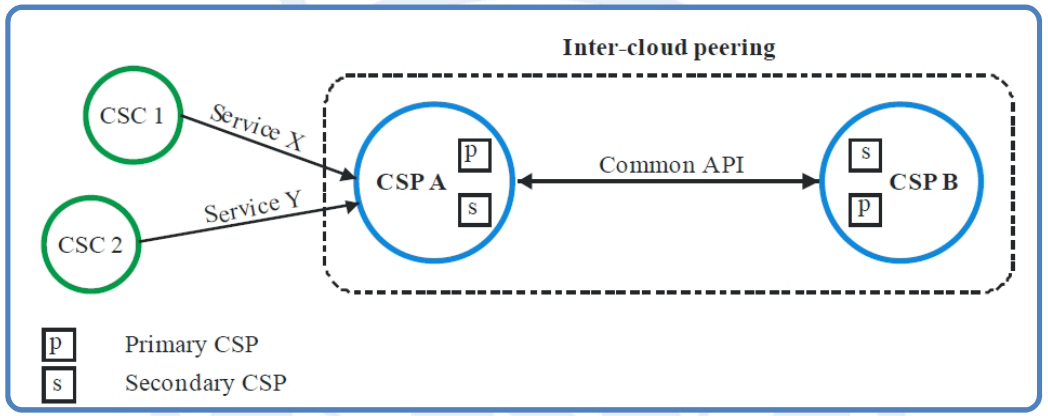
- **ITU-T Y.3511 „Framework of inter-cloud computing” :**
  - **3.2.1 inter-cloud computing**: The paradigm for enabling the interworking between two or more cloud service providers

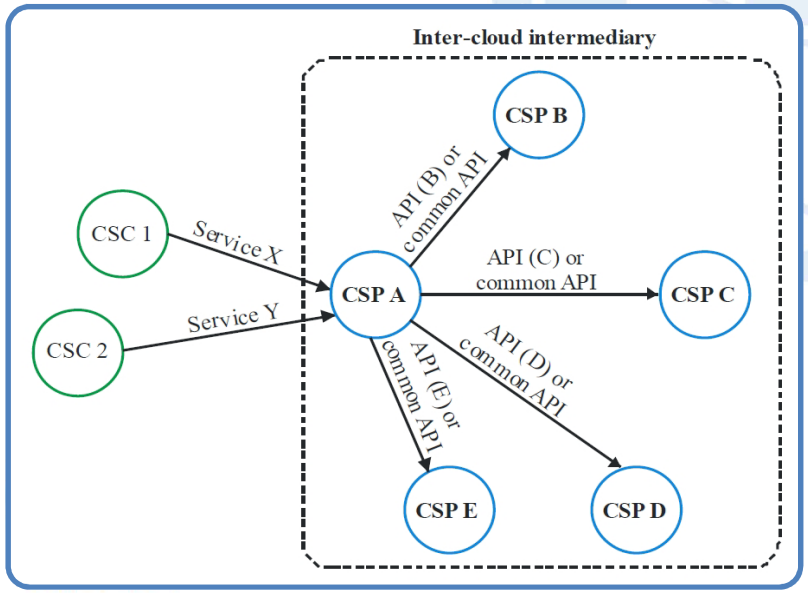


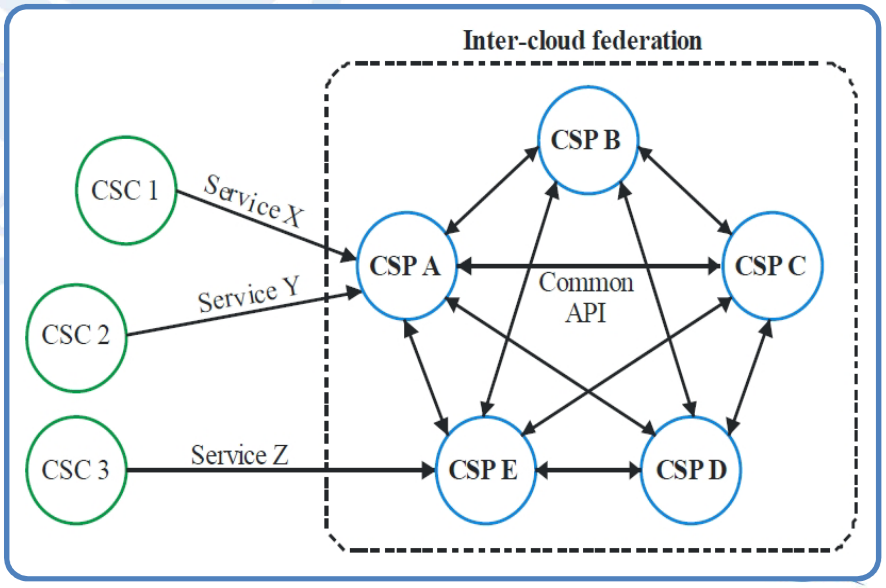
Source: ITU-T Y.3511 „Framework of inter-cloud computing”

Inter-cloud computing patterns

❑ ITU-T Y.3511 „Framework of inter-cloud computing”:

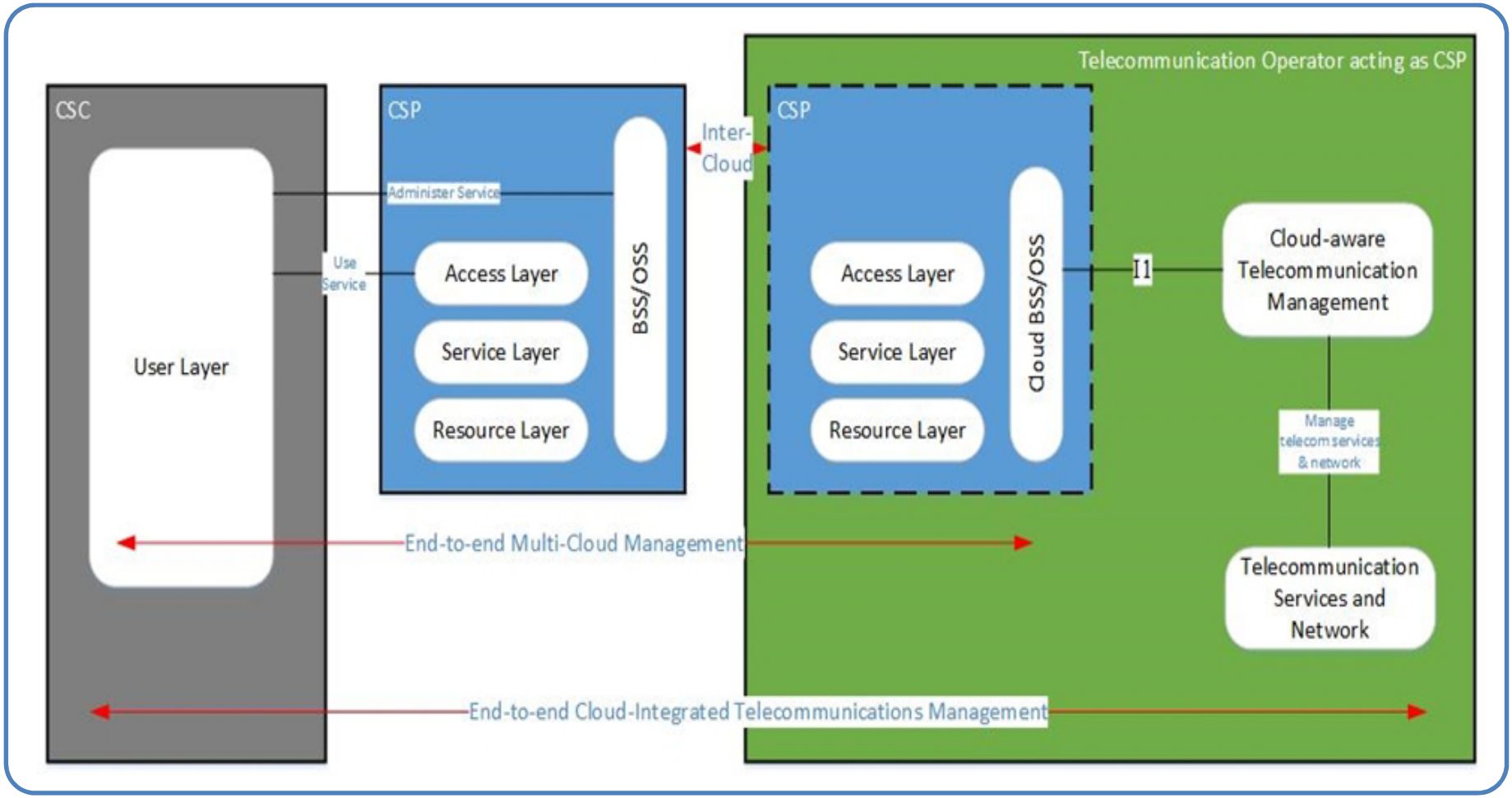






Source: ITU-T Y.3511 „Framework of inter-cloud computing”

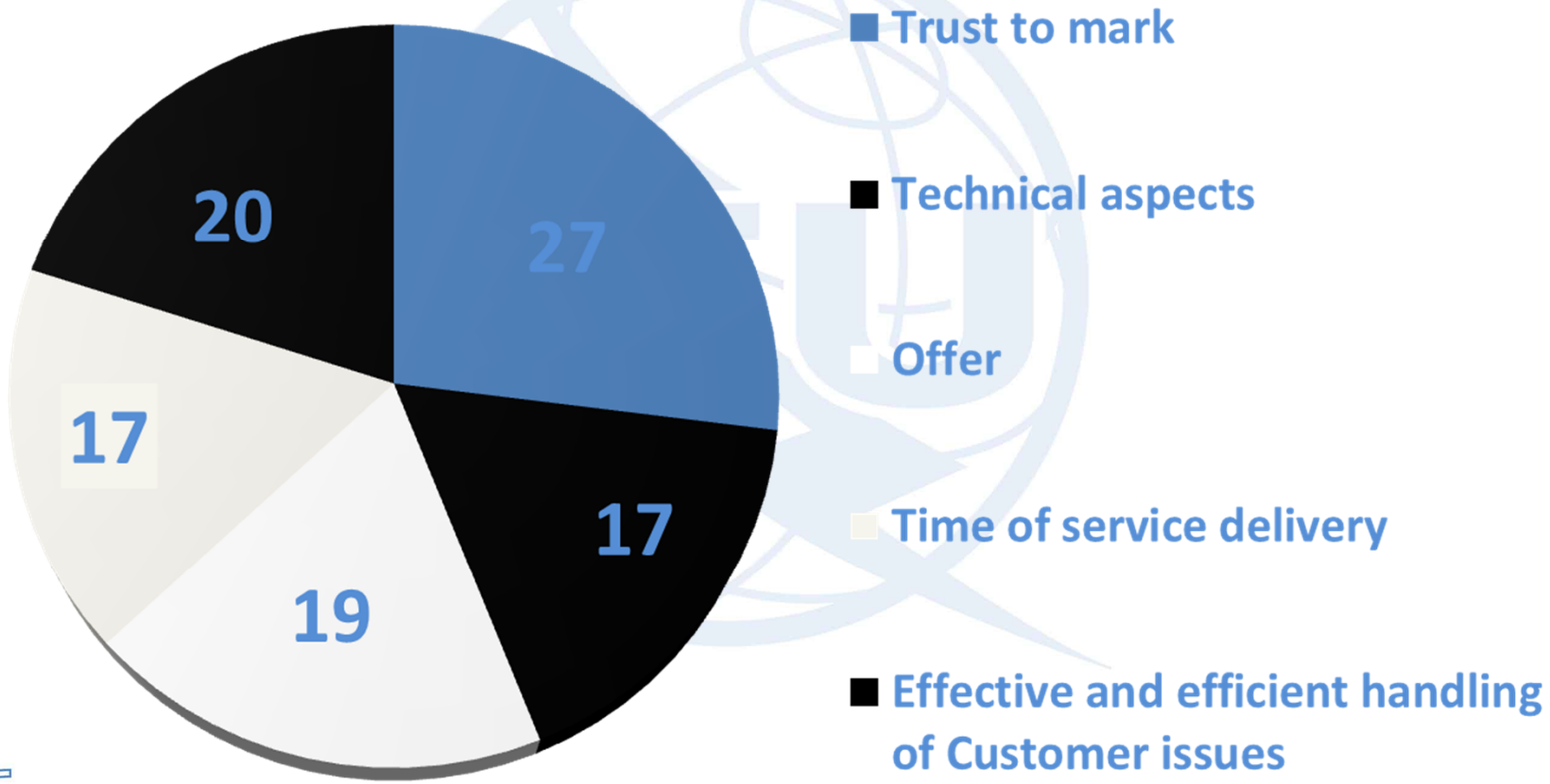
Inter-cloud in telecommunications



Source: ITU-T Y.3521 „Overview of end to end cloud computing management"

Technical aspects of inter-cloud

Key factors of Customer satisfaction



Source: Orange Poland 2015

Trusted inter-cloud computing

- rely on confidence between Cloud Service Customer (CSC) and CSP or between CSPs. One of them have to shift the physical control over application, service, resource and data to the others.
- appropriate secure mechanisms should be supported during CSPs interactions
- could be express by cross-cutting aspects of reference architecture of cloud (security, governance, management, resiliency)

Security of trusted inter-cloud

- **Security**
  - security and privacy are based on **distributed cloud management**
  - **specialized protocol** design with smart interaction with the underlying cloud network fabric
  - **two dimensional (vertical and horizontal) model**

Resiliency of trusted inter-cloud

- **Resiliency**
  - **set of technical procedures** to monitor, to analyze, to predict faults, to mitigate or to restore inter-cloud service
    - **reliability** (laws and regulations, local policies, service contracts, appropriate standards, etc.)
    - **availability** (technical systems functionality)

Management of trusted inter-cloud

- **Management**
  - **access control** mechanisms and **trust management** system
  - **management objectives** of trusted inter-cloud:
    - **expressivity -** ability to express access control policies
    - **granularity** - ability to decompose access control mechanism
    - **context-awareness** - ability to take context information
  - **inter-cloud data management**:
    - **define a terminology (language)** to annotate workloads
    - **strong security protection** and **traffic isolation**
    - **practically placed, executed and store** workloads

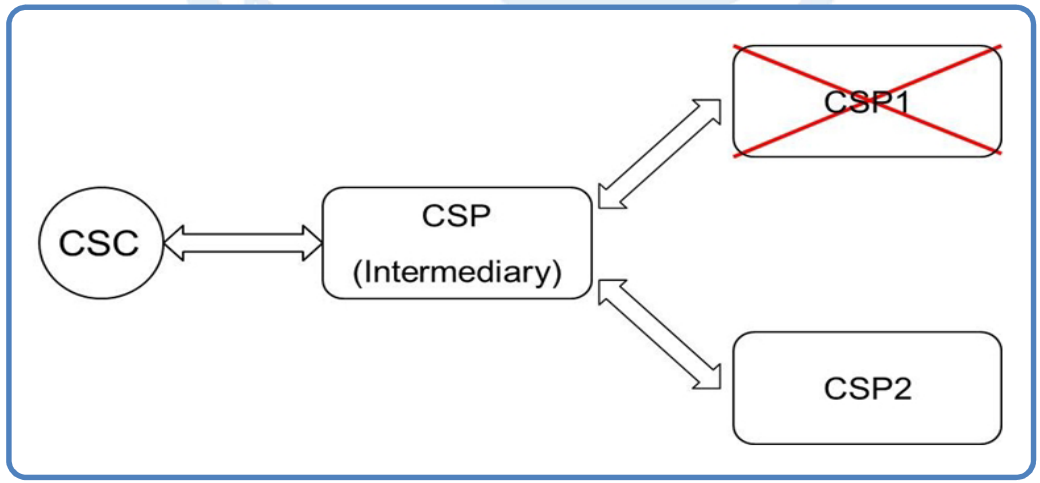
Reputation in trusted inter-cloud

- **process continues monitored** instead of stable state
- **behavior** in past, situations of risk and uncertainty
- **categorization** (reputation score) of involved actors
  - based on **prediction of cloud actors behaviours**
  - based on **SLA**
- **measurable and qualified** reputation scores

Practical use cases (1/4)

Resiliency: Video gaming

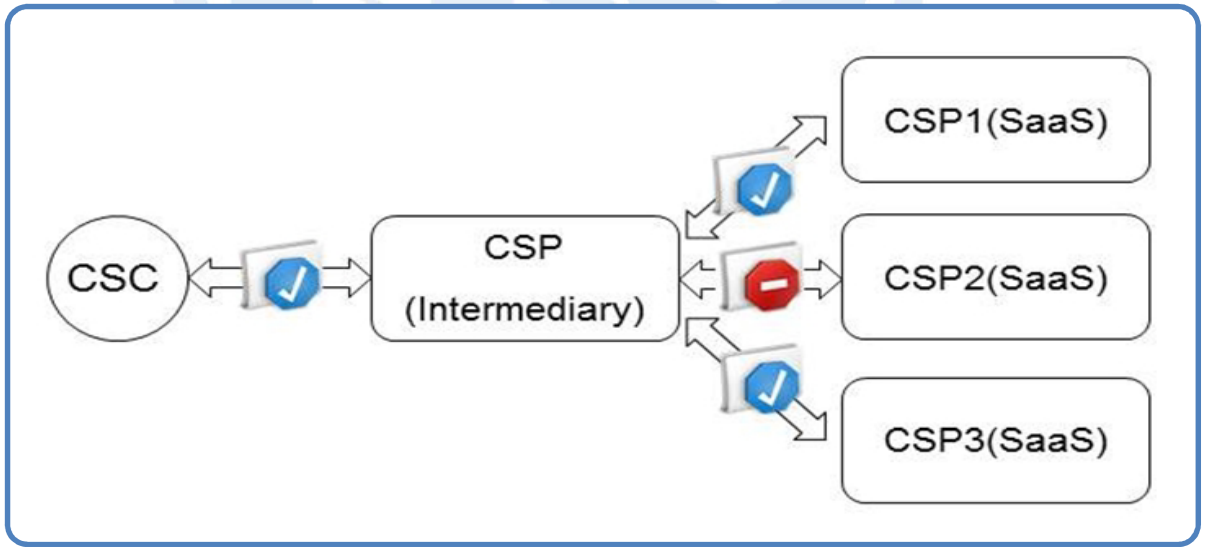
- CSC requests Premium video gaming service with QoS
- CSP(Intermediary) integrates and validates services from s-CSPs
- CSP(Intermediary) monitors QoS from secondary CSP1 and CSP2
- CSP(Intermediary) automate reallocate and re-establish service in case of service quality drops below Premium service level



Practical use cases (2/4)

Security: Access security

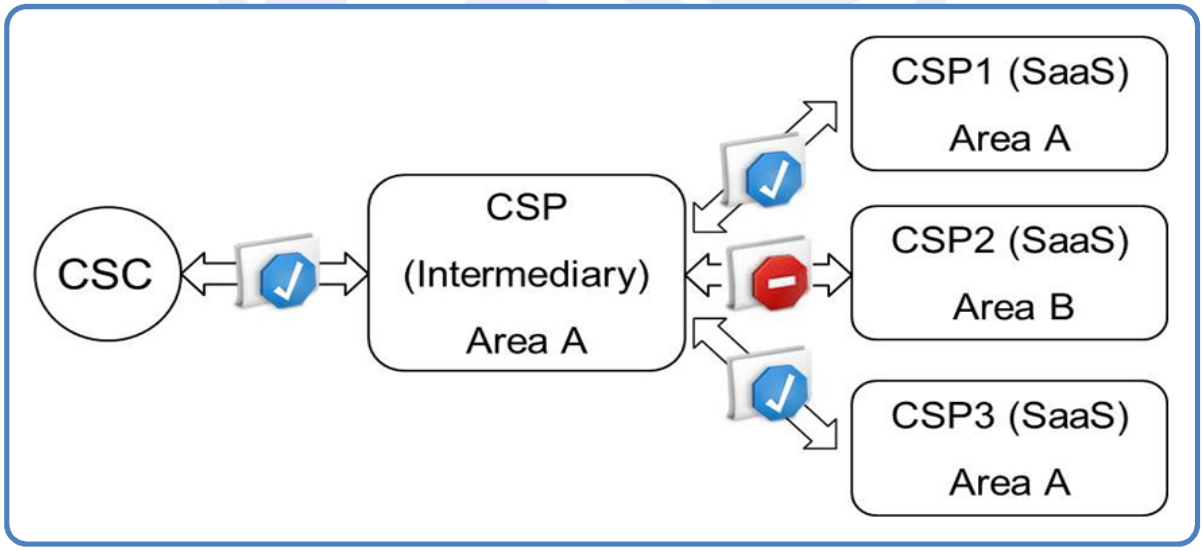
- CSC requests secure and malware free SaaS
- CSP(Intermediary) integrates and validates services from s-CSPs
- CSP(Intermediary) does not present negative validated service to CSC
- Service is automate reallocated and re-established in case of failure



Practical use cases (3/4)

Management: Geographical policy

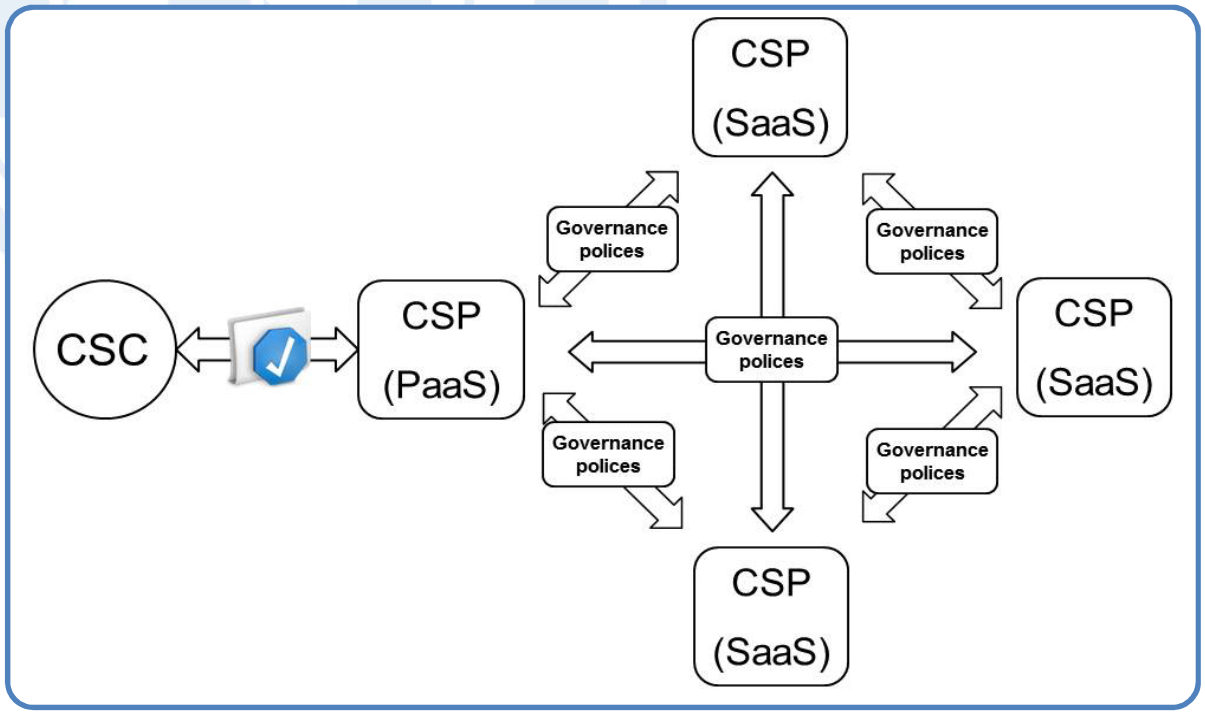
- CSC requests SaaS service performed exactly within area A
- CSP(Intermediary) integrates and validates services from s-CSPs
- CSP(Intermediary) does not present negative validated service to CSC
- Service is automate reallocated and re-established in case of failure



Practical use cases (4/4)

Government: Distributed exchange system

- CSC requests distributed cloud-based system to exchange documents
- CSP(PaaS) forms federation pattern among CPSs(SaaS)
- CSP(PaaS) determine appropriate policies to use system in trustworthy manner



Business aspects of trusted inter-cloud

- Resources are limited (even in inter-clouds)
- Real-time monitoring and charging
- Real-time risk mitigation
- Every (inter-)cloud service elements counts
- Time-based pricing (*pay-as-you-go*)
- Demand-based pricing (*uberization*)
- Flexible model: *broker, (real-time) bidding*

Summary

- **Challenges for short term (1-2 years):**
  - Distributed network management
  - SLA / SLO / QoS
- **Challenges for medium term:**
  - End-to-end service management
- **Challenges for long term:**
  - Interoperability and portability
  - Performance of heterogonous cloud
  - Business models


ITU


1956
2016
CCITT / ITU-T