Open Cloud eXchange (OCX)

Draft Proposal

GN3plus JRA1 Task 2 - Network Architectures for Cloud Services

Yuri Demchenko
SNE Group, University of Amsterdam

3-6 June 2013, TNC2013, Maastricht

Outline

- GN3+ JRA1: Network Architectures for Horizon 2020
  - Standardisation contribution
- General use cases and scenarios for Cloud services delivery to NRENs and universities
  - Cloud and Intercloud Infrastructure and Services
- Open Cloud eXchange (OCX)
  - Requirements to OCX
  - OCX design principles and suggestions
- Additional information
  - Intercloud Architecture Framework (ICAF) and Intercloud Federation Framework (ICFF)

Cloud services for Universities

- E-mail service, e.g. Gmail
- Storage services
  - Shared storage, e.g. Dropbox, Box, SkyDrive
  - Backup storage
- Scientific data access
  - Genome data
  - LHC experiment data
- Computational power
  - HPC access (to limited extent)
  - VM and Cloud IaaS services
  - Cloud SaaS and CloudApps (e.g. Google Aps)
- *Related (?):* VoIP, CDN and other QoS critical services
- Any other - *To be added*

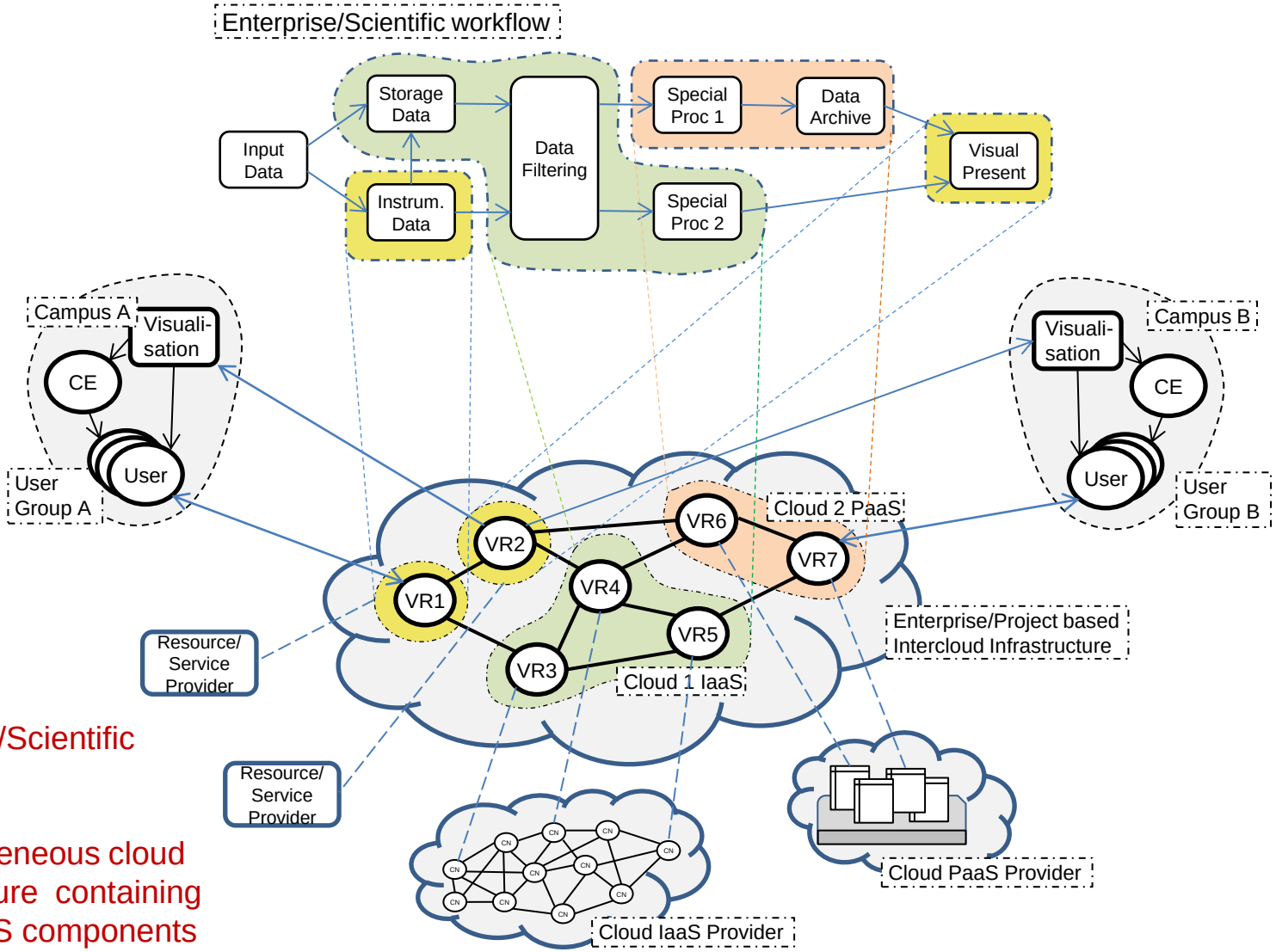
Use Cases for delivering Cloud services to campus based users

- Distributed (Big) Scientific Data processing with MPP tools on distributed facilities
  - Data distributed between few location next to local datacenters
- Streaming high-speed high volume experimental data to labs in campus location
  - Direct links through campus network
- CSP and campus L0-L2(L3) network peering
  - Dark fiber with termination as campus network or as CSP network
- VoIP – SURFnet approach with mobile data access
  - Support mobile access network (LTE) and tunnel access to campus network

Intercloud Access and Delivery Infrastructure

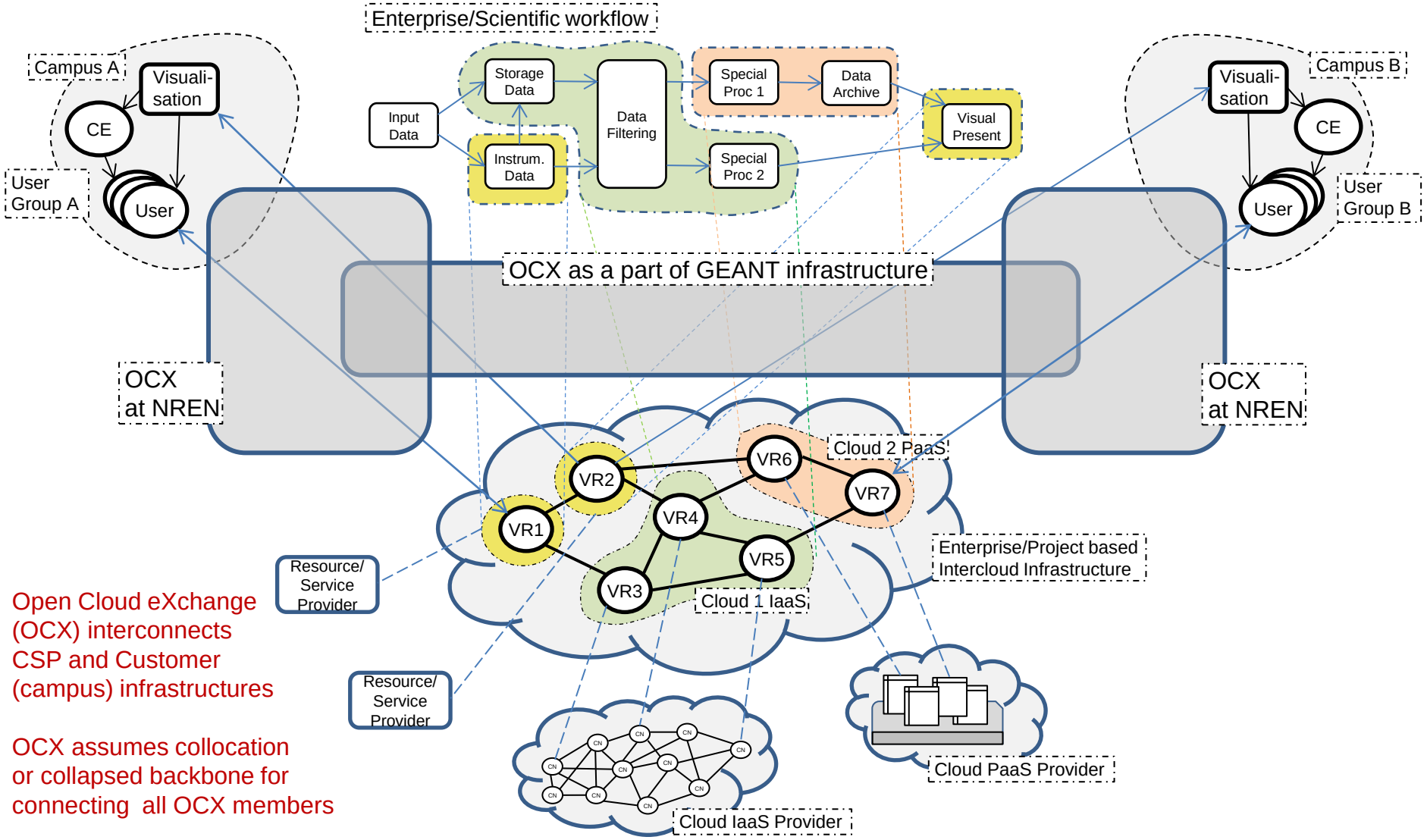
- Intercloud/Cloud Access and Delivery Infrastructure (ICADI) is a functional layer between Cloud Services layer and Customer services
  - Interconnects CSP location/datacenter and customer or user location
    - Also for multiple CSPs (inter-cloud) and multiple customer locations
  - Provides infrastructure for federated services and access control
    - Including service brokering
  - May include dedicated network infrastructure
- Cloud Carrier service layer
  - Place for NREN services
  - “Last mile” for cloud services delivery
- Need for Open Cloud eXchange (OCX)
  - As a core for “collapsed” ICADI layer functions

General use case for infrastructure provisioning: Workflow => Logical (Cloud) Infrastructure

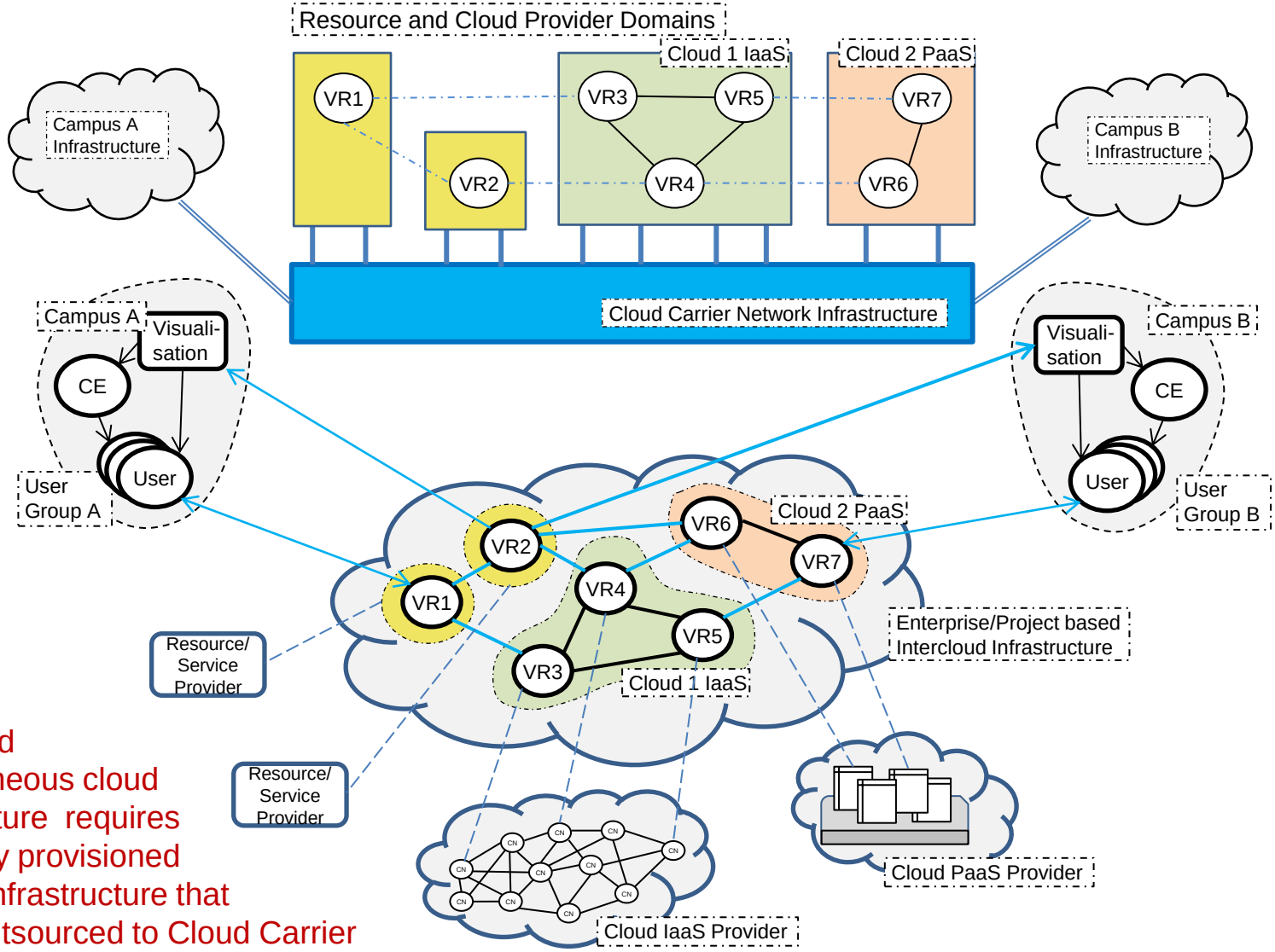


Enterprise/Scientific workflow
Is mapped
to heterogeneous cloud infrastructure containing IaaS, PaaS components

Multi/inter- cloud infrastructure provisioning: => ICADI and OCX functions

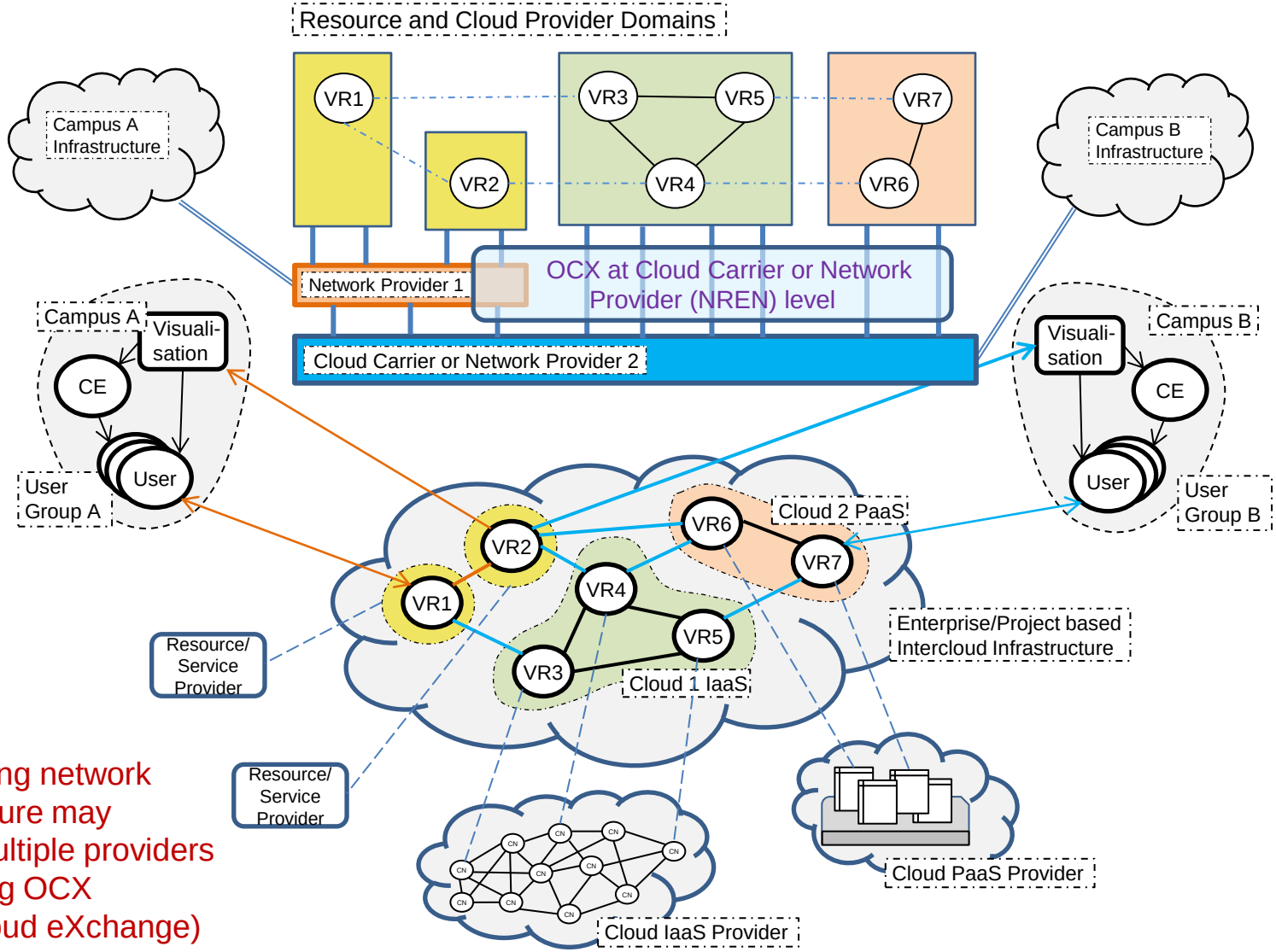


General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (1)



Distributed heterogeneous cloud infrastructure requires separately provisioned network infrastructure that can be outsourced to Cloud Carrier

General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (2)

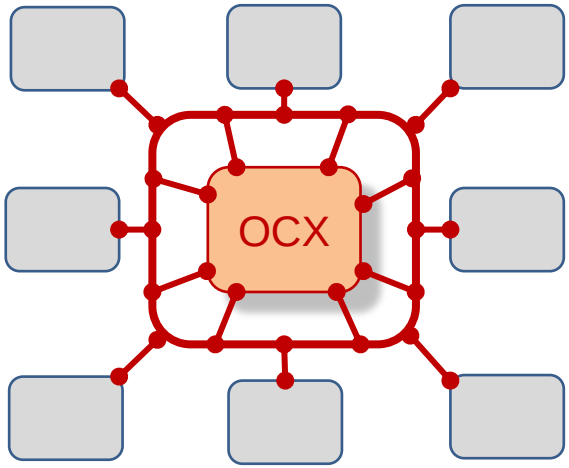


Provisioning network infrastructure may involve multiple providers
Introducing OCX (Open Cloud eXchange)

OCX Definition and Operational Principles

- ***Direct service/inter-member peering***
  - Re-use and leverage Internet eXchange
  - Open collocation services
- ***No third party (intermediary/broker) services***
  - Transparency for cloud based services
  - No involvement into peering or mutual business relations
- ***Trusted Third Party (TTP)***
  - To support dynamic service agreements and/or federation establishment
  - Trusted Introducer for dynamic trust establishment
- May include other special services to support smooth services delivery and integration between CSP and Customer
  - E.g., Local policies, service registry and discovery

OCX Topological model and Connectivity



OCX L0-L2/L3 topology

- Any-to-any
- Distributed or collapsed backbone
- Hierarchical
- Topology information exchange L0-L2 + L3? between members

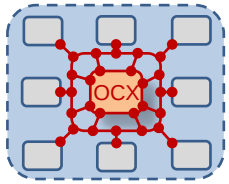
QoS parameters

- Bandwidth
- Speed, latency
- Jitter, impairment

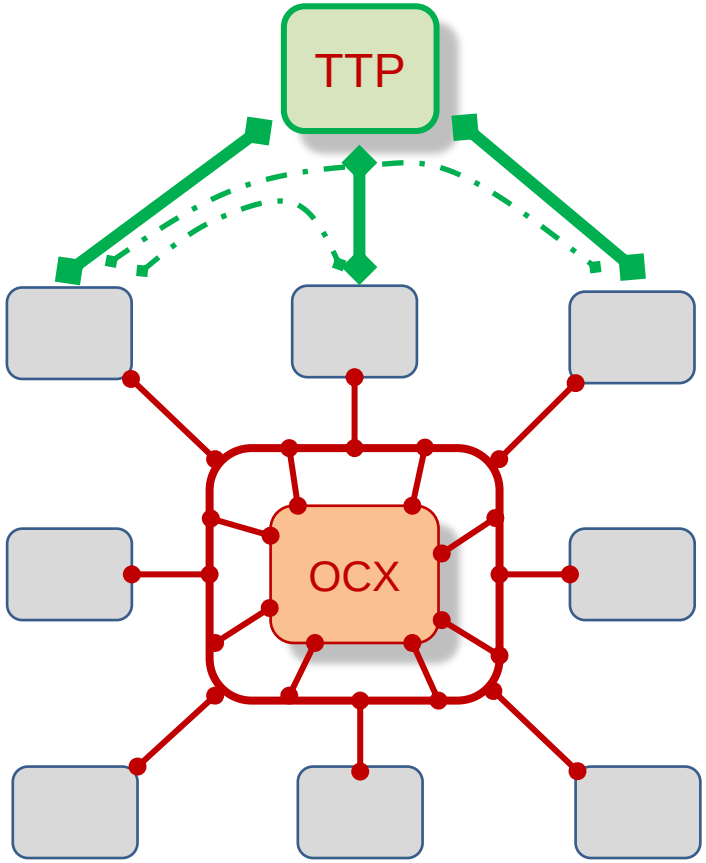
Nodes: Providers and customers

OCX Facilities

OCX backbone links/connectivity (Lo-L2)



OCX Trusted Third Party services



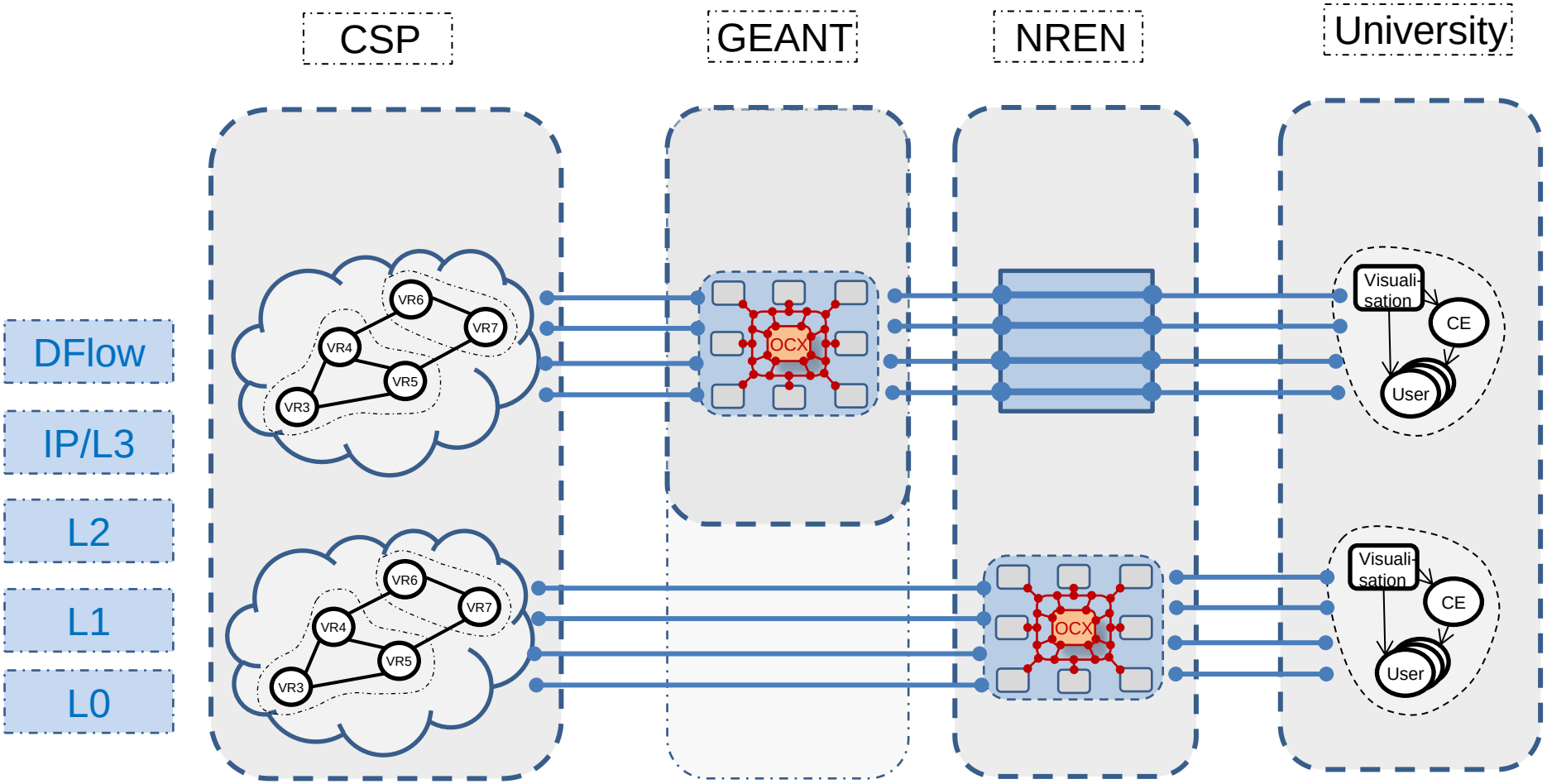
Pre-established trust relation with OCX as TTP

Trust relations established as a part of dynamic federation between OCX members

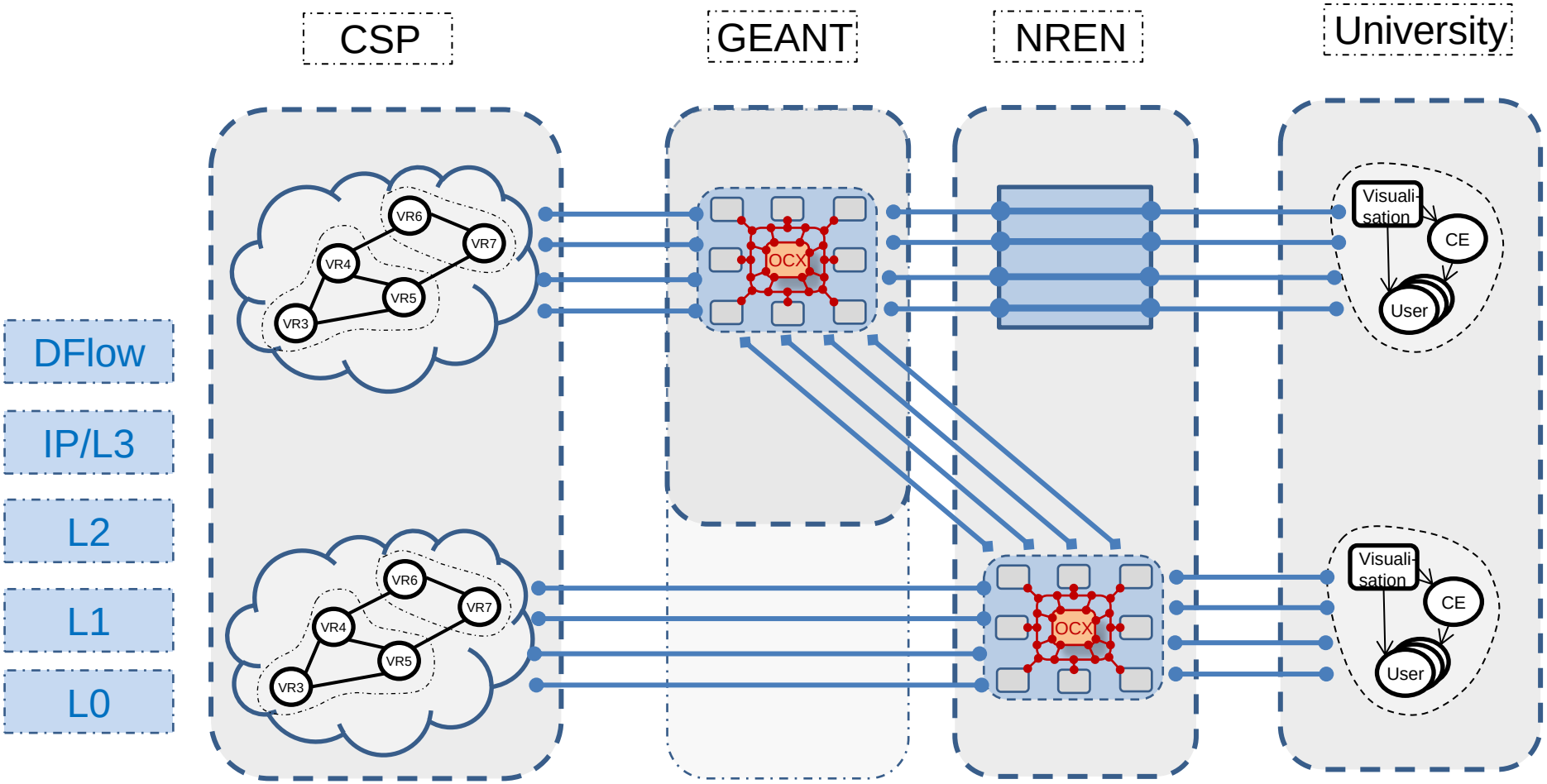
TTP goals and services

- Enable dynamic federations establishing
- Trusted Certificates and CA's Repository
  - Similar to TACAR (TERENA Academic CA Repository)
- Trusted Introducer
- Service Registry and Discovery
- Intercloud policy clearinghouse
  - Repository of CSP policies
  - Common policy template
- SLA repository and clearinghouse

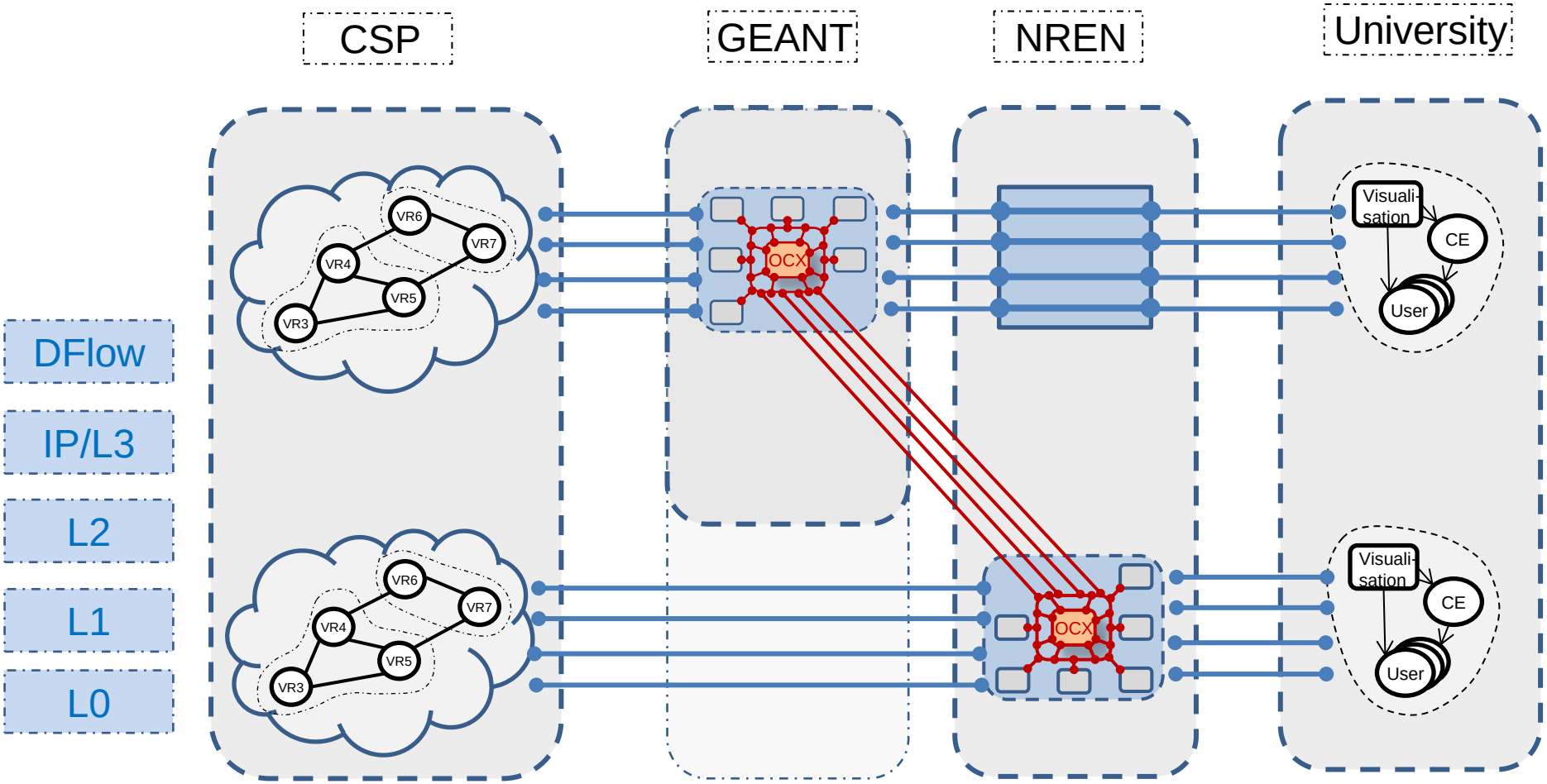
OCX location options: GN3, NREN (+University?)



OCX Hierarchical Topology Model



OCX Extended Backplane Topology Model



OCX Development – Next Steps

- Initial draft issued – 27 May 2013
- GN3plus inter-activities discussion and feedback
  - First round of comments and update – end of June 2013
  - Second round of comments and update – Sept. 2013
  - External comments and community feedback – by Sept 2013
- Design and implementation – TBD
- Standardisation contribution – OGF, IETF, ITU-T, IEEE, NIST

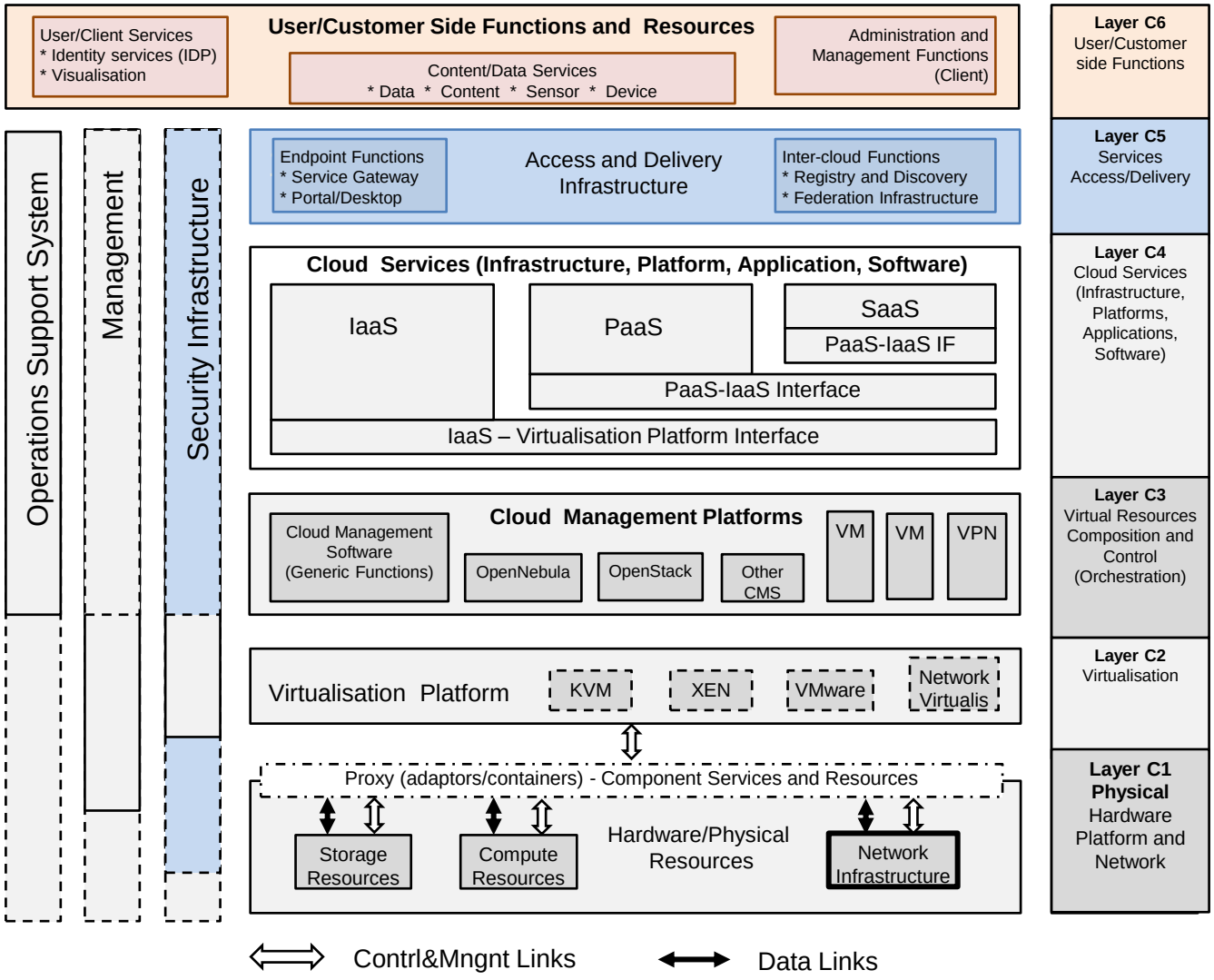
Discussion and Questions

Additional Information

InterCloud Architecture Framework (ICAF)

- Multi-layer Cloud Services Model (CSM)
  - Combines IaaS, PaaS, SaaS into multi-layer model with inter-layer interfaces
  - Including interfaces definition between cloud service layers and virtualisation platform
- InterCloud Control and Management Plane (ICCMP)
  - Allows signaling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds
  - Including management interface from applications to network infrastructure and virtualisation platform
- InterCloud Federation Framework (ICFF)
  - Defines set of protocols and mechanisms to ensure heterogeneous clouds integration at service and business level
  - Addresses Identity Federation, federated network access, etc.
- InterCloud Operations Framework (ICOF)
  - RORA model: Resource, Ownership, Role, Action
    - RORA model provides basis for business processes definition, SLA and access control
  - Broker and federation operation
- Intercloud Security Framework (ICSF)
  - Dynamic Security Infrastructure provisioning and protocols

Multilayer Cloud Services Model (CSM)



CSM layers

(C6) User/Customer side Functions

(C5) Intercloud Access and Delivery Infrastructure

(C4) Cloud Services (Infrastructure, Platform, Applications)

(C3) Virtual Resources Composition and Orchestration

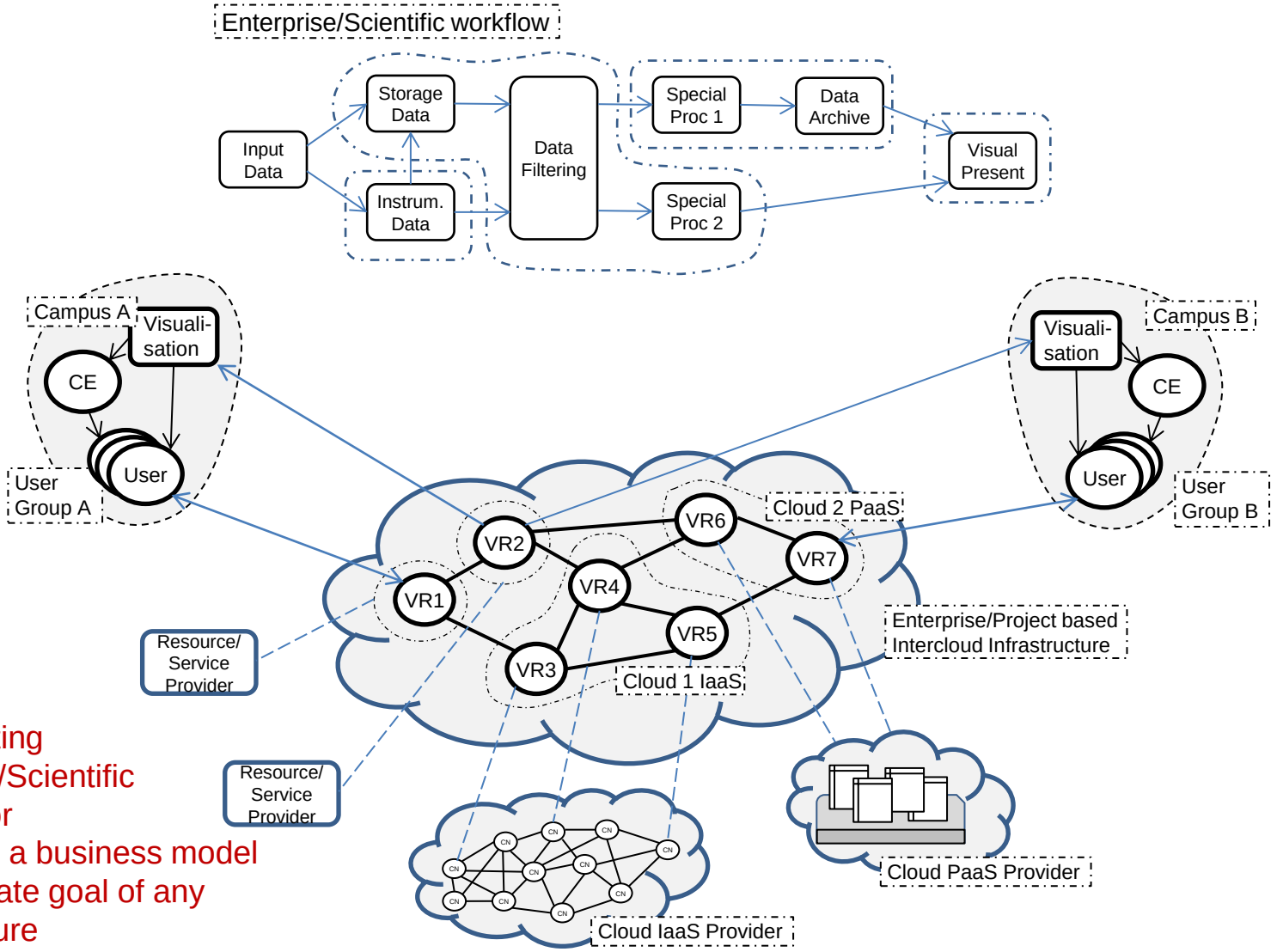
(C2) Virtualisation Layer

(C1) Hardware platform and dedicated network infrastructure

Control/ Mngnt Links

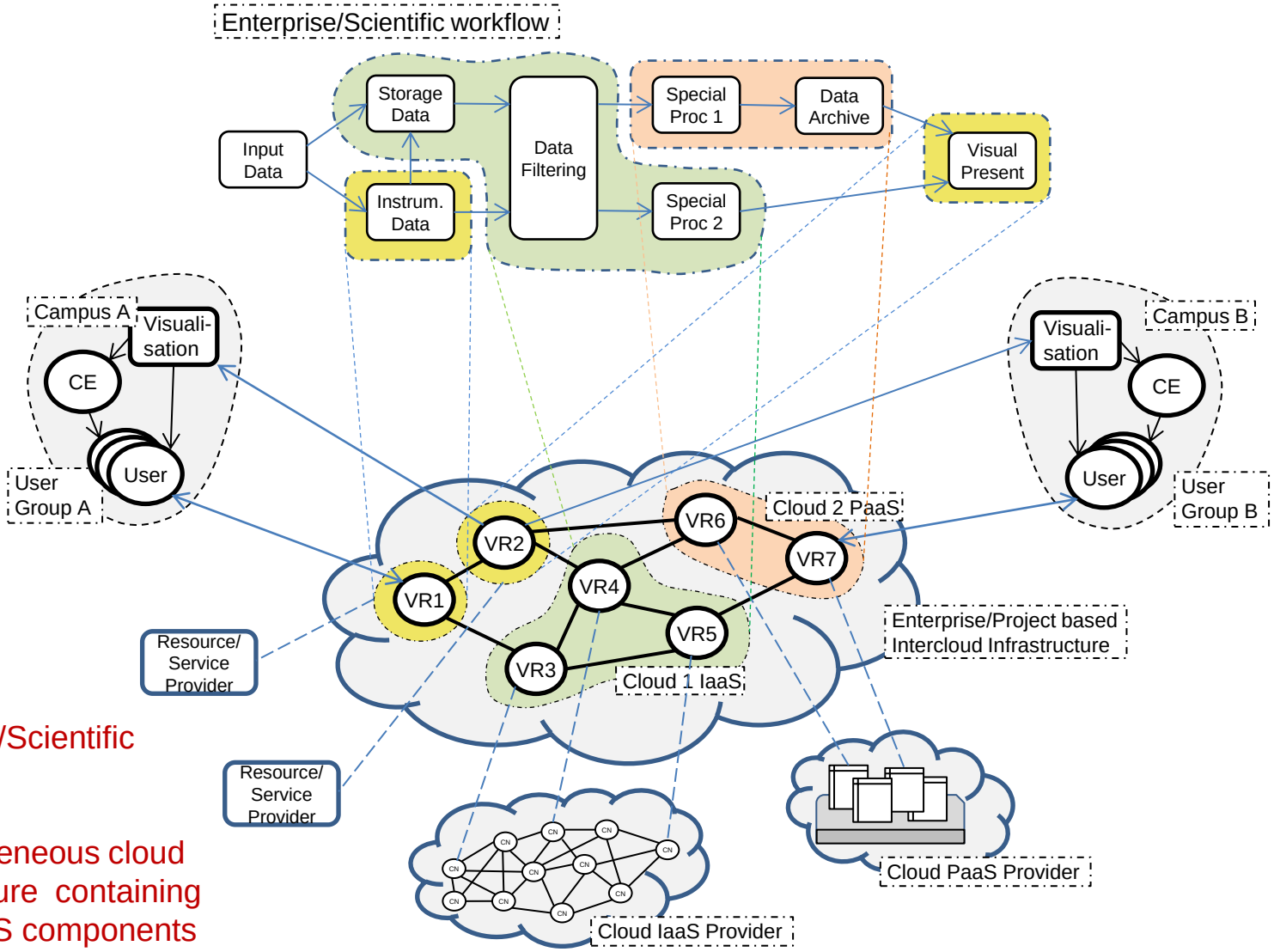
Data Links

General use case for infrastructure provisioning: Workflow => Logical (Cloud) Infrastructure (1)



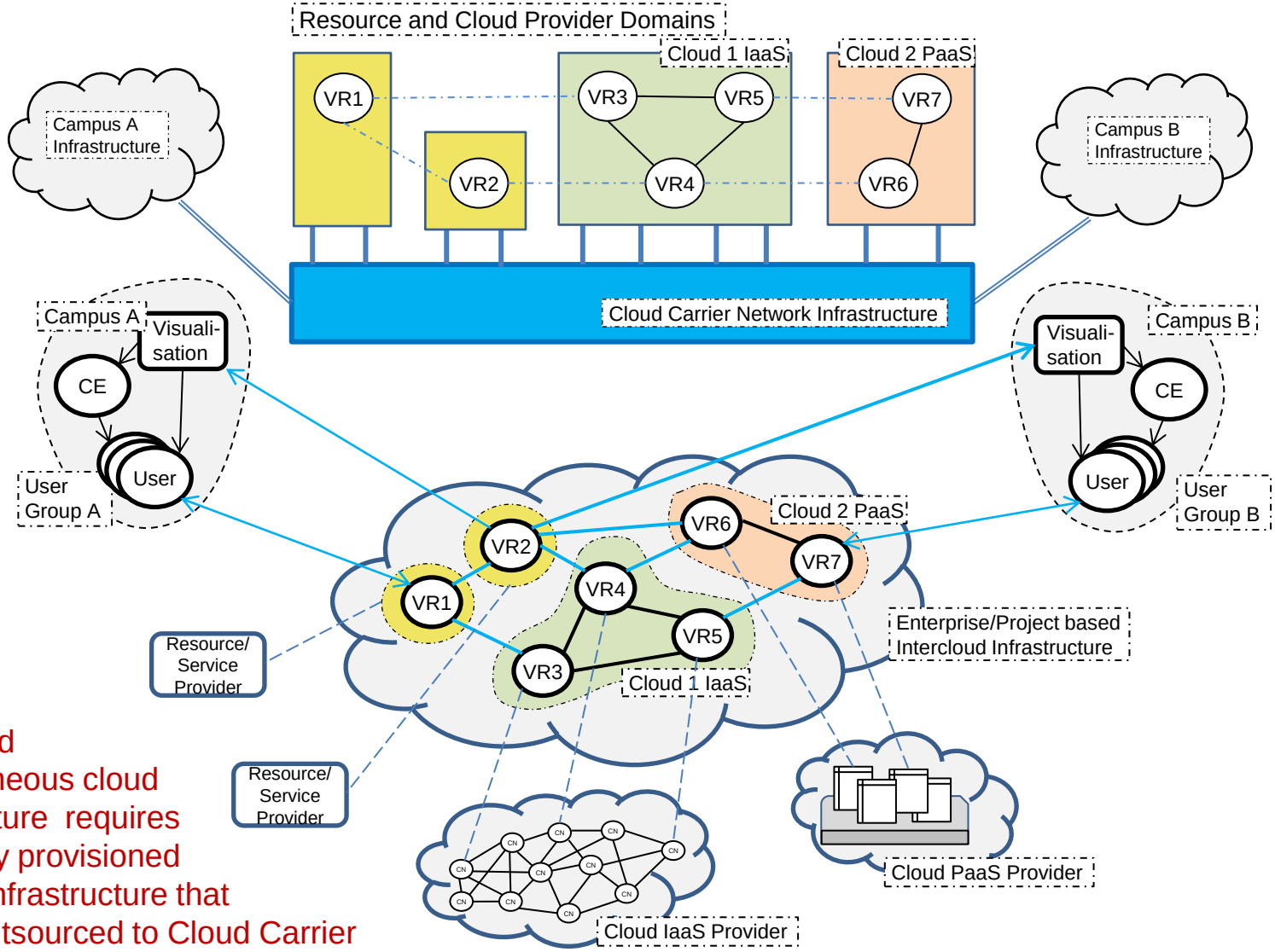
Implementing Enterprise/Scientific workflow or supporting a business model is an ultimate goal of any infrastructure

General use case for infrastructure provisioning: Workflow => Logical (Cloud) Infrastructure



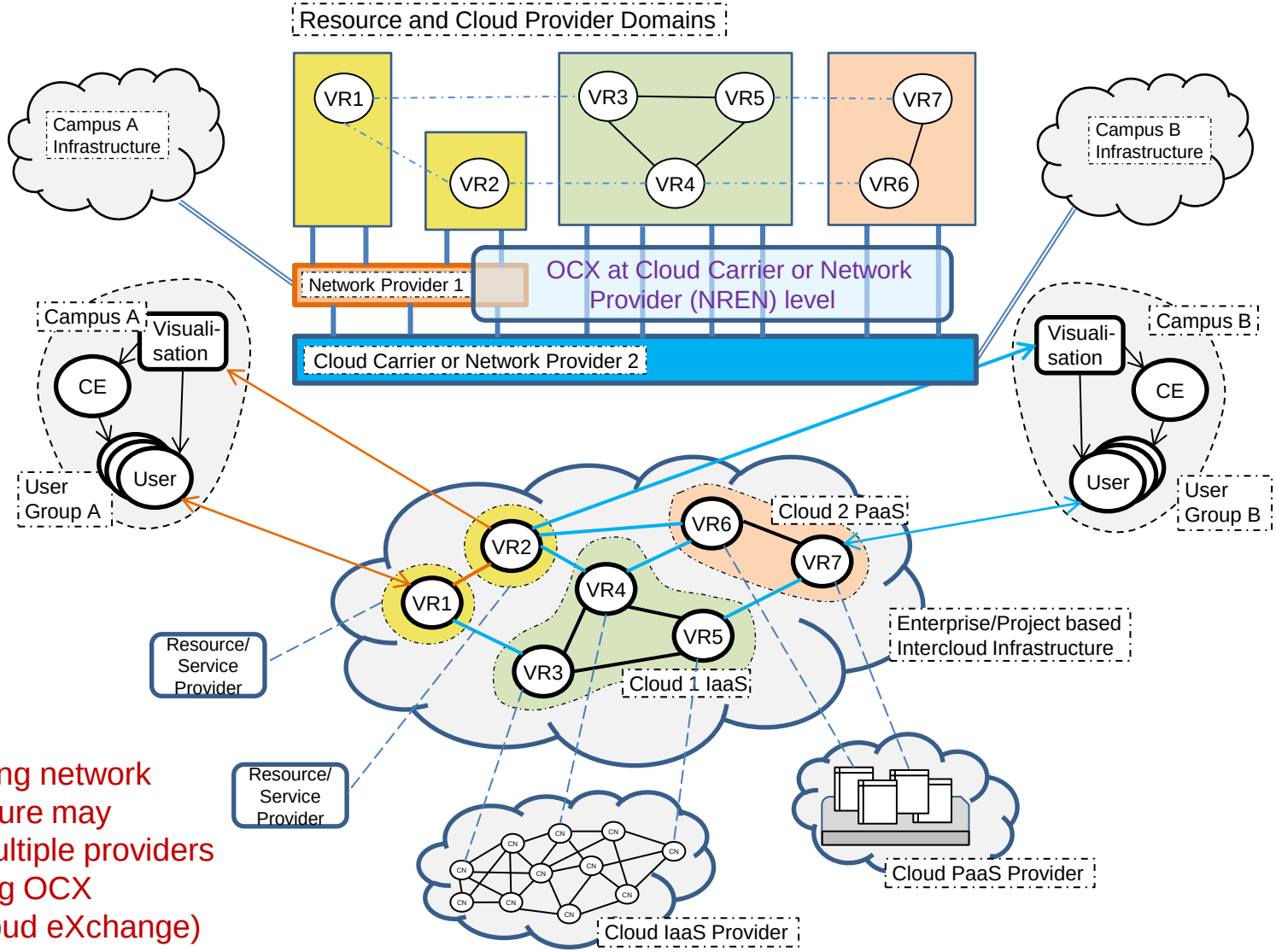
Enterprise/Scientific workflow
Is mapped
to heterogeneous cloud infrastructure containing IaaS, PaaS components

General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (1)



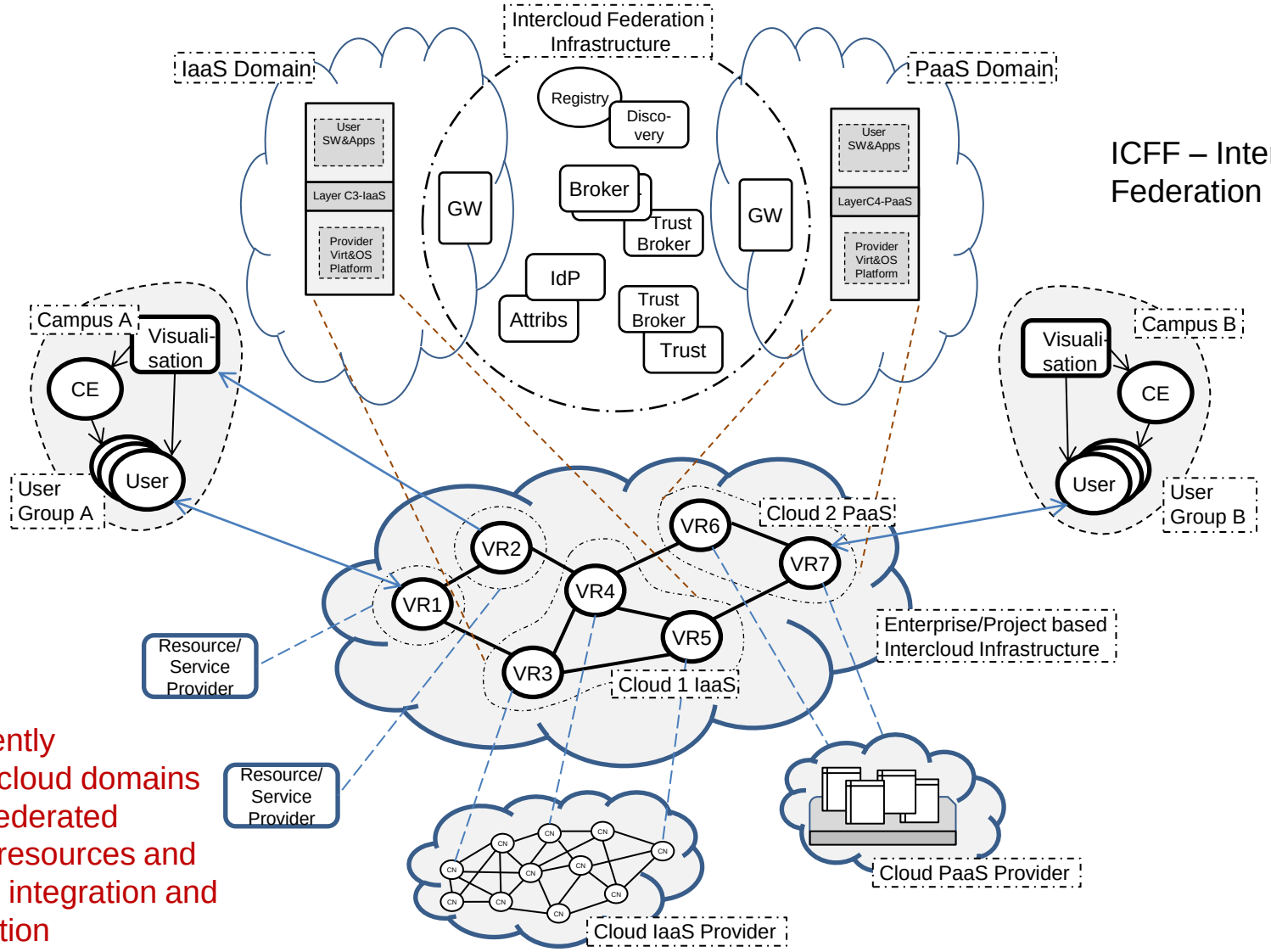
Distributed heterogeneous cloud infrastructure requires separately provisioned network infrastructure that can be outsourced to Cloud Carrier

General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (2)



Provisioning network infrastructure may involve multiple providers
Introducing OCX (Open Cloud eXchange)

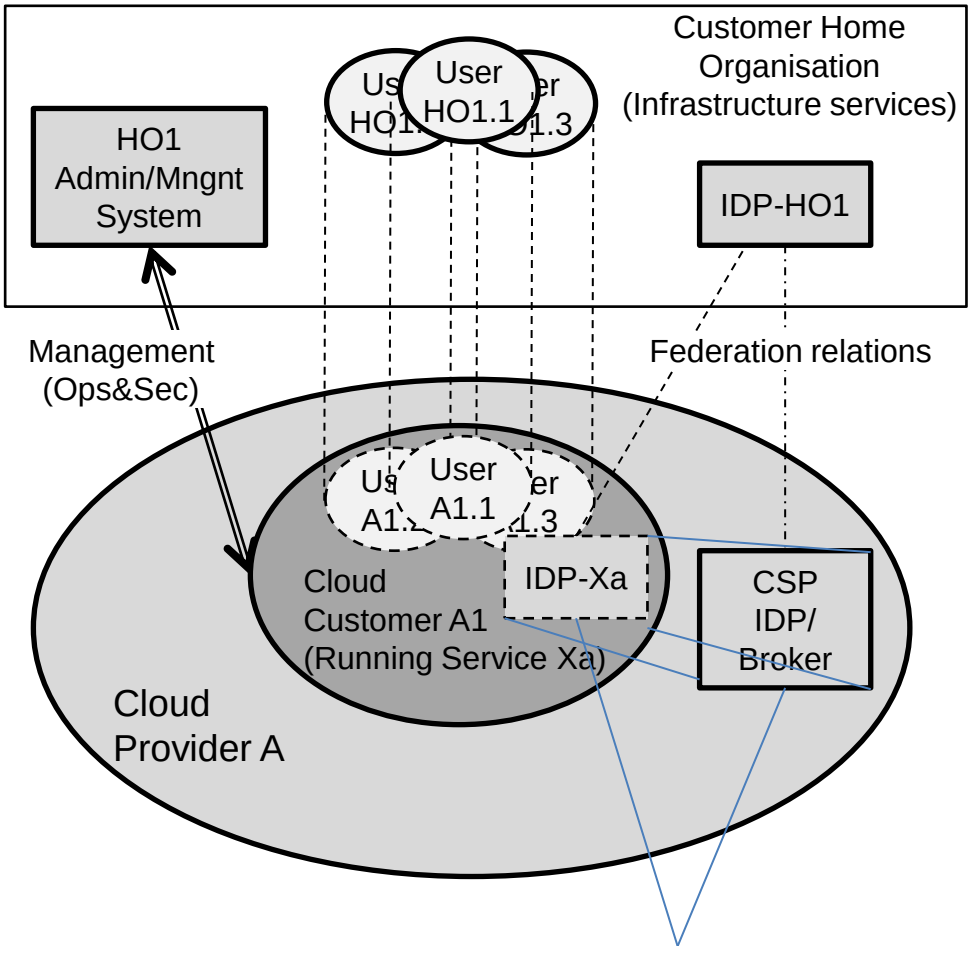
Intercloud Federation Framework (ICFF)



ICFF – InterCloud Federation Framework

Independently managed cloud domains may use federated model for resources and processes integration and interoperation

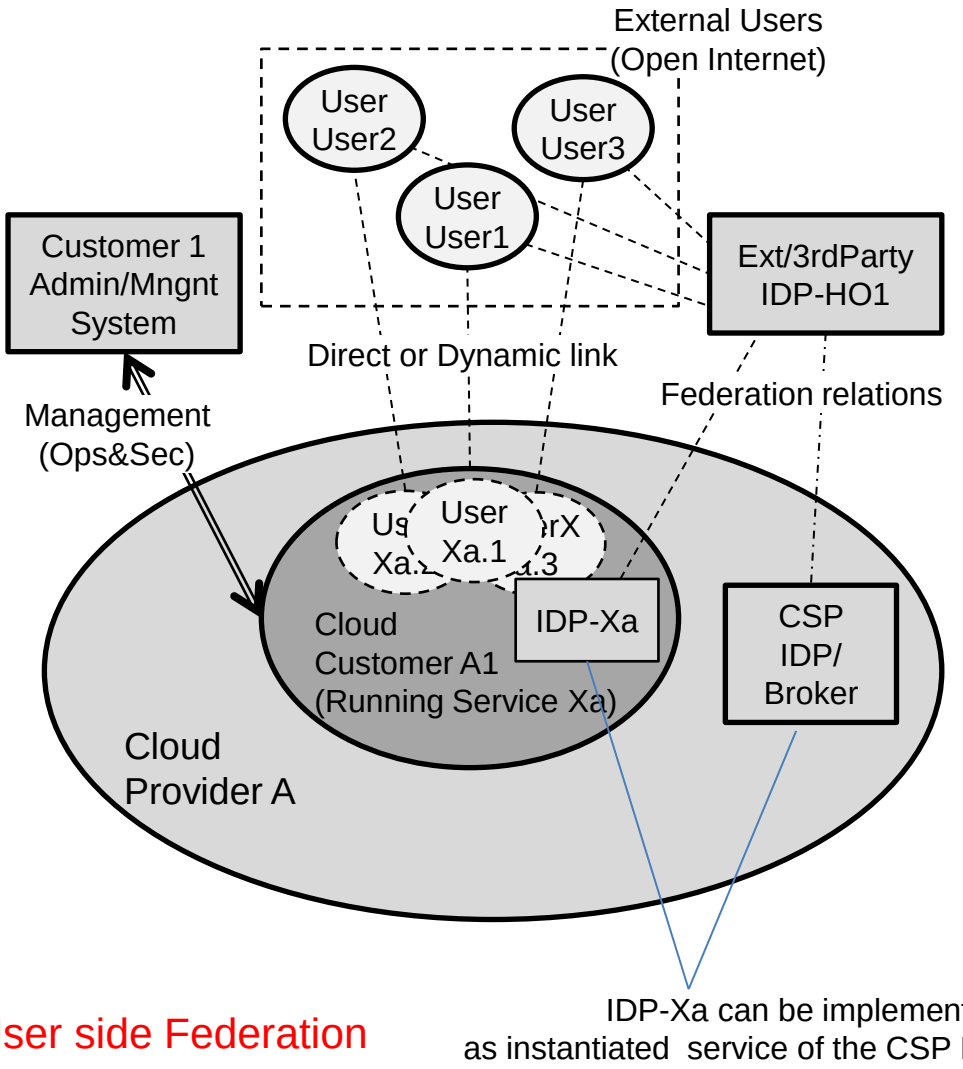
Basic Cloud Federation model (1.2) – Federating HO and CSP domains (IDP-HO1 and IDP-CSP)



User side Federation

- Simple/basic scenario 1: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for users from HO1 and managed by HO1 Admin/Management system
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those created for Service Xa
- TODO: Extend with AuthN/AutnZ service in Virtual Service Environment

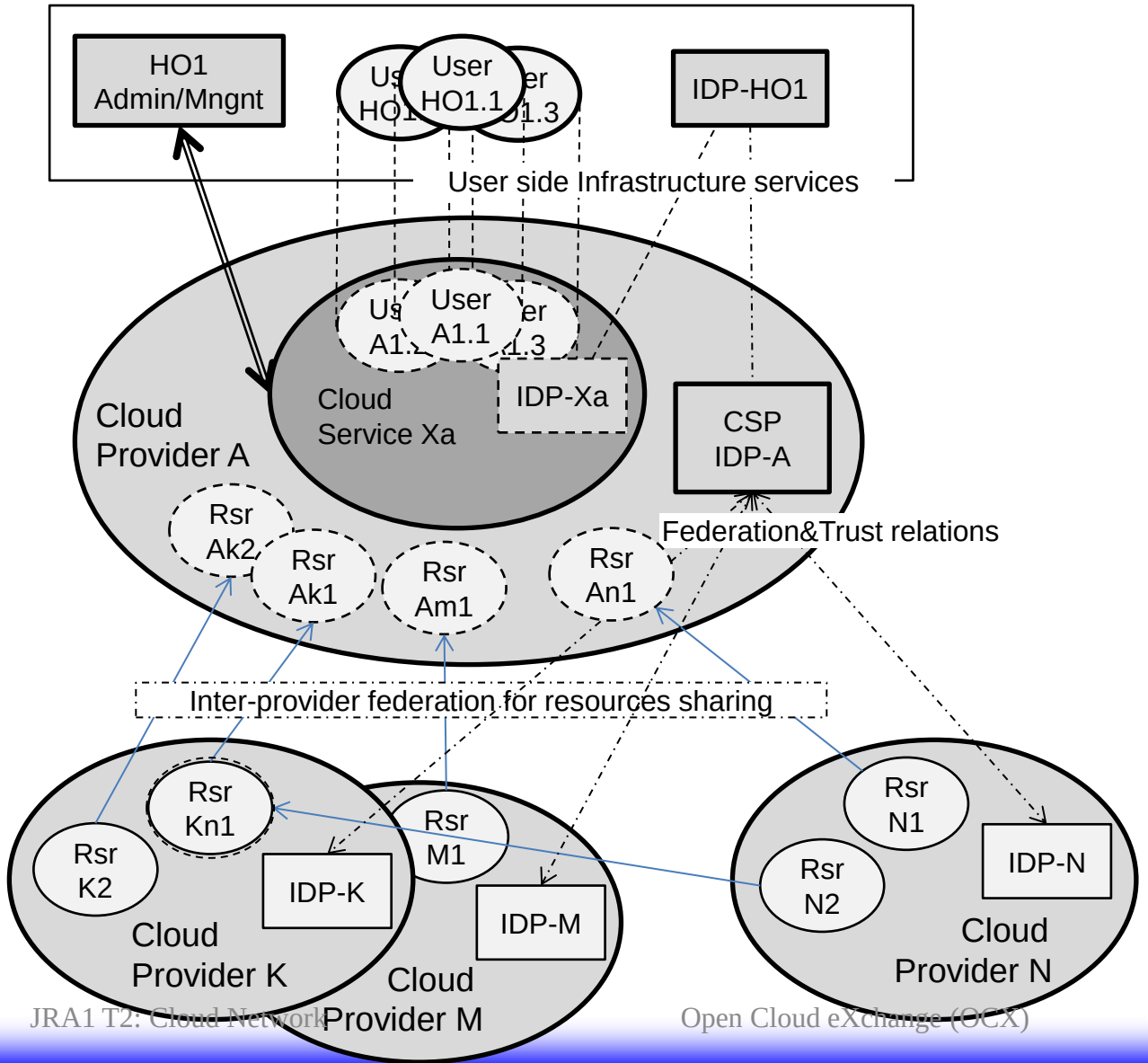
Basic Cloud Federation model (1.3) – Using 3rd party IDP for external users



User side Federation

- Simple/basic scenario 2: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for external users (e.g. website) and managed by Customer 1
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those IDP-Xa created for Service Xa

Basic Cloud Federation model (2.1) – Federating CSP's/multi-provider cloud resources



- Cloud provider side federation for resources sharing
- Federation and Trust relations are established between CSP's via Identity management services, e.g. Identity Providers (IDP)
  - May be bilateral or via 3rd party/broker service
- Includes translation or brokering
  - Trust relations
  - Namespaces
  - Attributes semantics
  - Policies
- Inter-provider federation is transparent to customers/users

Provider side Federation

Intercloud Federation Infrastructure and OCX