The NAVIGATORS group

A bird's eye view of current Int'l projects

TRONE

Information and Communication Technologies Institute
Carnegie Mellon | PORTUGAL
AN INTERNATIONAL PARTNERSHIP

TRONE CMU|Portugal partnership Project
Trustworthy and Resilient Operations in a Network Environment

- Develop innovative solutions for Network Operation, Administration and Management
  - *Proactive* hazard reduction: **architectural robustness**
  - *Reactive* hazard reduction: **detection and recovery**
- Achieve trustworthy network operation
  - Solutions for dynamic dependability & security enforcement
  - Deal with increasing levels of accidental and malicious faults
    - Diagnosis, detection
    - Prevention/tolerance
    - Automatic reconfiguration
  - Provide architectural solutions and resilient components

FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

FCTUC

Carnegie Mellon University

PT

MASSIF - European IP Project

MAnagement of Security information and events in Service Infrastructures

- IP project **FP7**
- **Project dur:**

Oct 2010 – Sep 2013

- **Overall budget:**

~ 6 Mio. €

- **Project Coordinator:**
  Atos Origin

KARYON European IP Project
Kernel-Based ARchitecture for safetY-critical cONtrol

Academia & Research Institutes
SMEs and Industry

Proof-of-concept prototypes
Simulations

FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

gmv

EMBRAER

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

SP

CHALMERS

4S Group
Technology for Sustainability

Avionics

UAS/Aircraft flight mission

Automotive

Adaptive cruise control
Coordinated lane change
Coordinated intersection crossing

- Provide system solutions for predictable and safe coordination of smart vehicles that autonomously cooperate and interact in an open and uncertain environment
- Expected results:
  - A system architecture for safety/performance management
  - Improvements in the reliable and trustworthy environment perception
  - Middleware for integration of remote sensors & cooperation of simulated and real sensors
  - Tools for evaluation of safety assurance according to ISO 26262 safety standard
  - Proof of concept prototypes and a simulation-based demonstration

SecFuNet - *FP7-ICT-2011-EU-Brazil*
Security for Future Networks

2011.10.1 EU-Brazil Future Internet - security
Research and Development cooperation: Future Internet - security

Name of the coordinating person: Michel Betirac
e-mail: Michel.Betirac@ethertrust.com

Participant no.	Participant organisation name	Part. short name	Country
1 (Coordinator)	EtherTrust	ET	France
2	Twinteq	TWI	Poland
3	Université Pierre et Marie Curie -LIP6	UPMC	France
4	Telecom ParisTech	TPT	France
5	Ecole Normale Supérieure	ENS	France
6	Implementa	IMP	Germany
7	Technische Universität München	TUM	Germany
8	Infineon	INF	Germany
9	Fundação da Faculdade de Ciências da Universidade de Lisboa	FFCUL	Portugal
10 (Coordinator)	Universidade Federal de Pernambuco	UFPE	Brazil
11	Universidade Federal do Rio de Janeiro	UFRJ	Brazil
12	Universidade Estadual do Ceará	UECE	Brazil
13	Universidade Federal do Amazonas	UFAM	Brazil
14	Universidade Federal de Santa Catarina	UFSC	Brazil
15	Universidade Federal do Rio Grande do Sul	UFRGS	Brazil
16	DWA	DWA	Brazil

TClouds European IP Project

Privacy and Resilience for Internet-Scale Critical Infrastructures

http://www.tclouds-project.eu/

- 7,5 Meuro
- Started Autumn 2010
- 3 years duration

Can security- and privacy-critical applications be housed in the clouds? TCLOUDS says yes!

Paulo Esteves Veríssimo

Faculdade de Ciências da Univ. de Lisboa (FCUL), LaSIGE, Portugal,

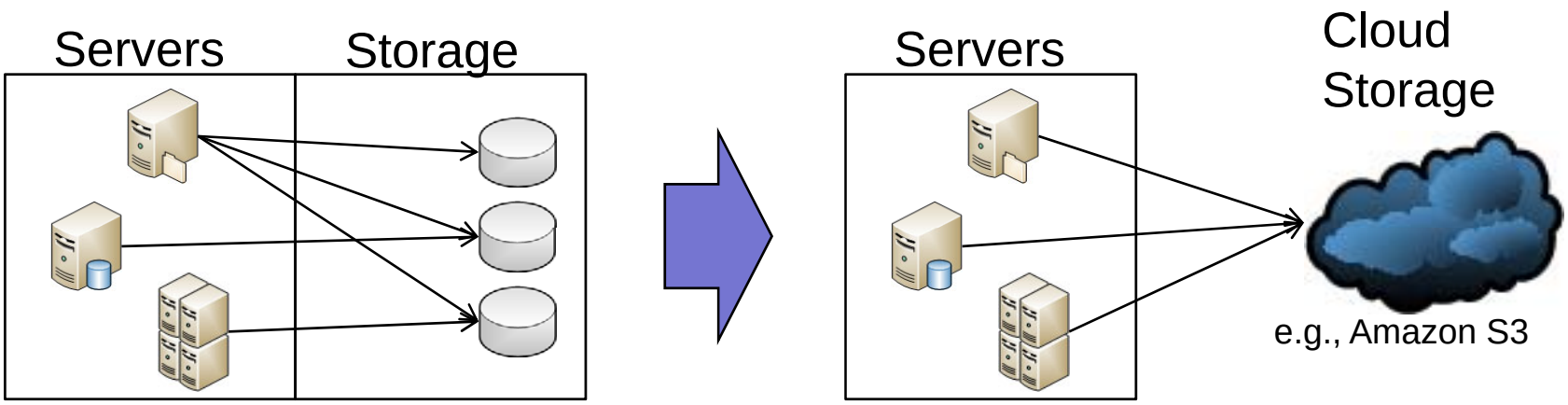
pjv@di.fc.ul.pt http://www.di.fc.ul.pt/~pjv

61st IFIP WG 10.4 Meeting, Sainte-Luce – France

January 26-30, 2012

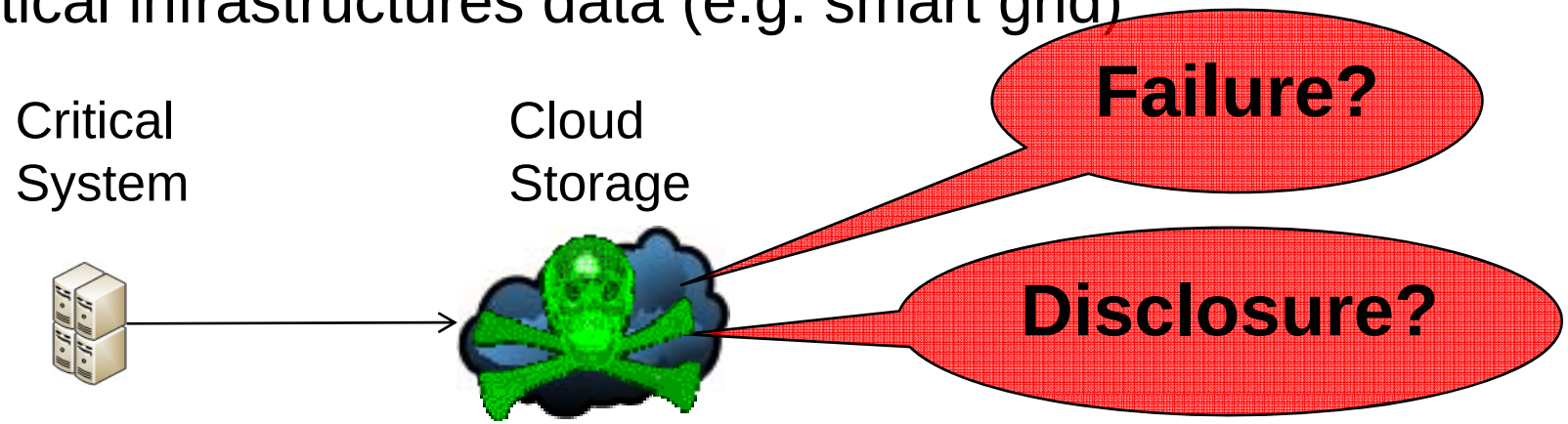
Moving to Clouds

- Data are moving to the cloud
- Main reason: costs (pay-per-use model)
- Still hesitation for critical applications (e.g., smart energy grids), but it's a matter of time…



Critical applications on the cloud?

- depending on one cloud *(or provider thereof)* is not enough to build trust
- E.g., privacy- and security-critical data storage
  - Medical records
  - Company financial data
  - Critical infrastructures data (e.g. smart grid)

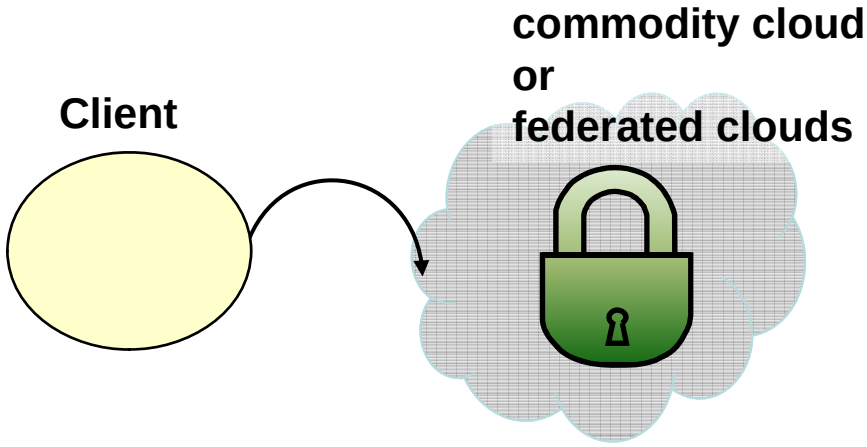


Trusted-Trustworthy Clouds

Option 1:

1) *Rely on improved cloud infrastructure by single or federated cloud providers*

***CON**: dependence on actual provider(s) trustworthiness (single point of failure, lock-in, collusion)*



Trusted-Trustworthy Clouds

Option 1:

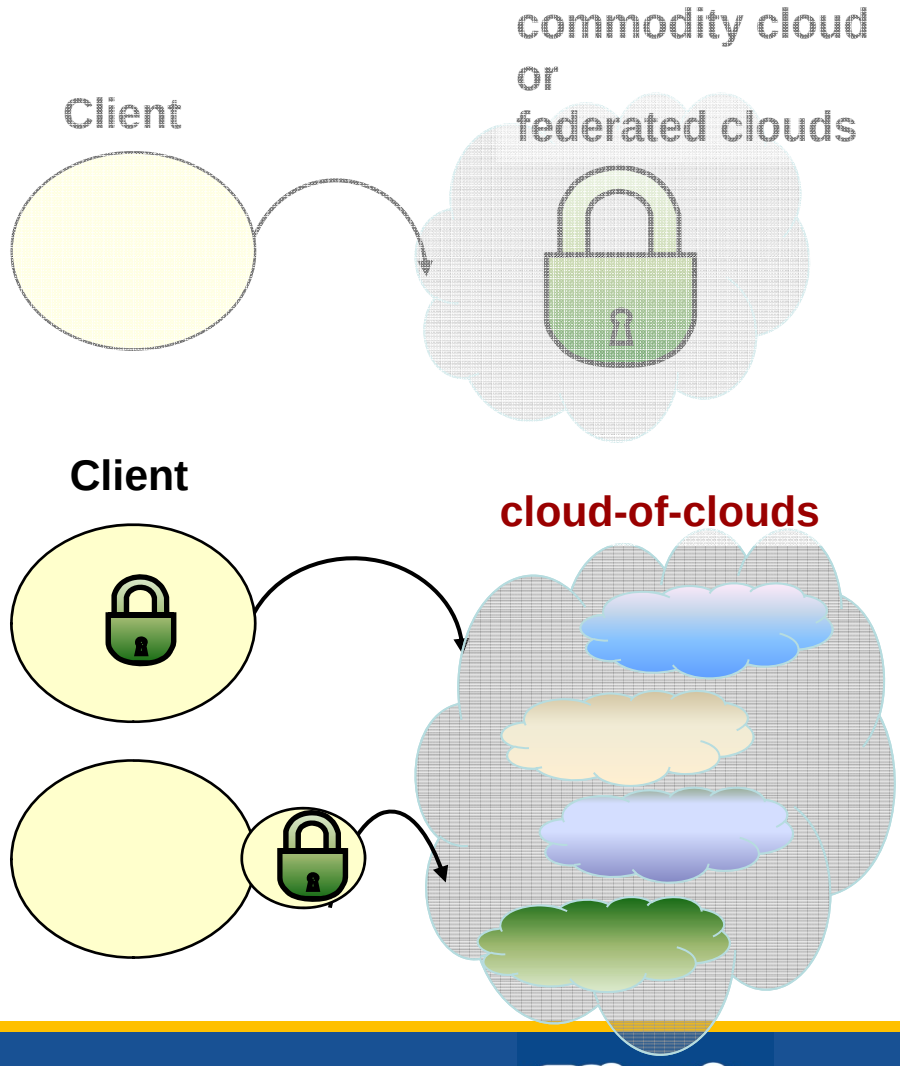
1) *Rely on improved cloud infrastructure by single or federated cloud providers*

***CON**: dependence on actual provider(s) trustworthiness (single point of failure, lock-in)*

Option 2:

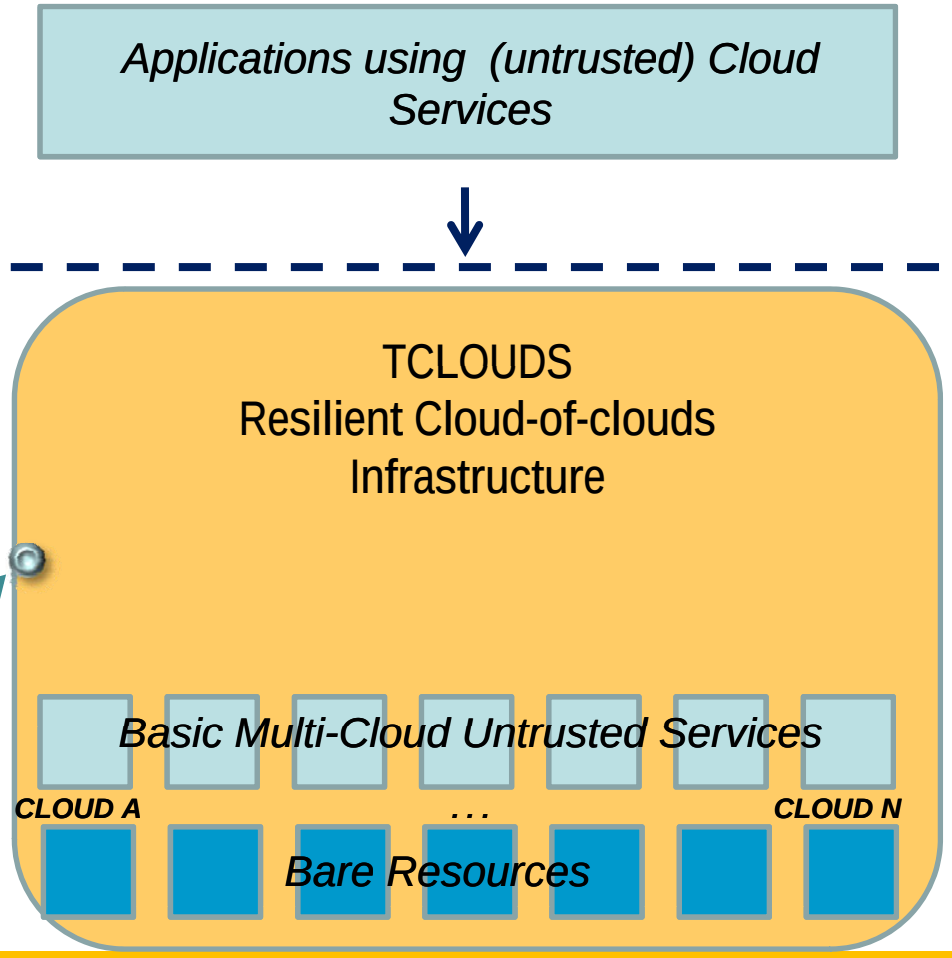
2) ***cloud-of-clouds** – use multi-cloud environments independently*

***PRO**: be your own master w.r.t. trust*



Status-quo

- Existing Technologies:
  - "cloudified" scenario has **availability + security needs that cannot be met by application layer alone.**
  - proprietary approaches to security **can create exclusion** and make interoperation difficult and expensive
  - **single-cloud** solutions, even if open, will not address high resilience objectives, since they are a **single point of failure**
- A solution - **resilient cloud-of-clouds infrastructure**:
  - automated computing resilience against attacks and accidents in complement or in addition to commodity clouds

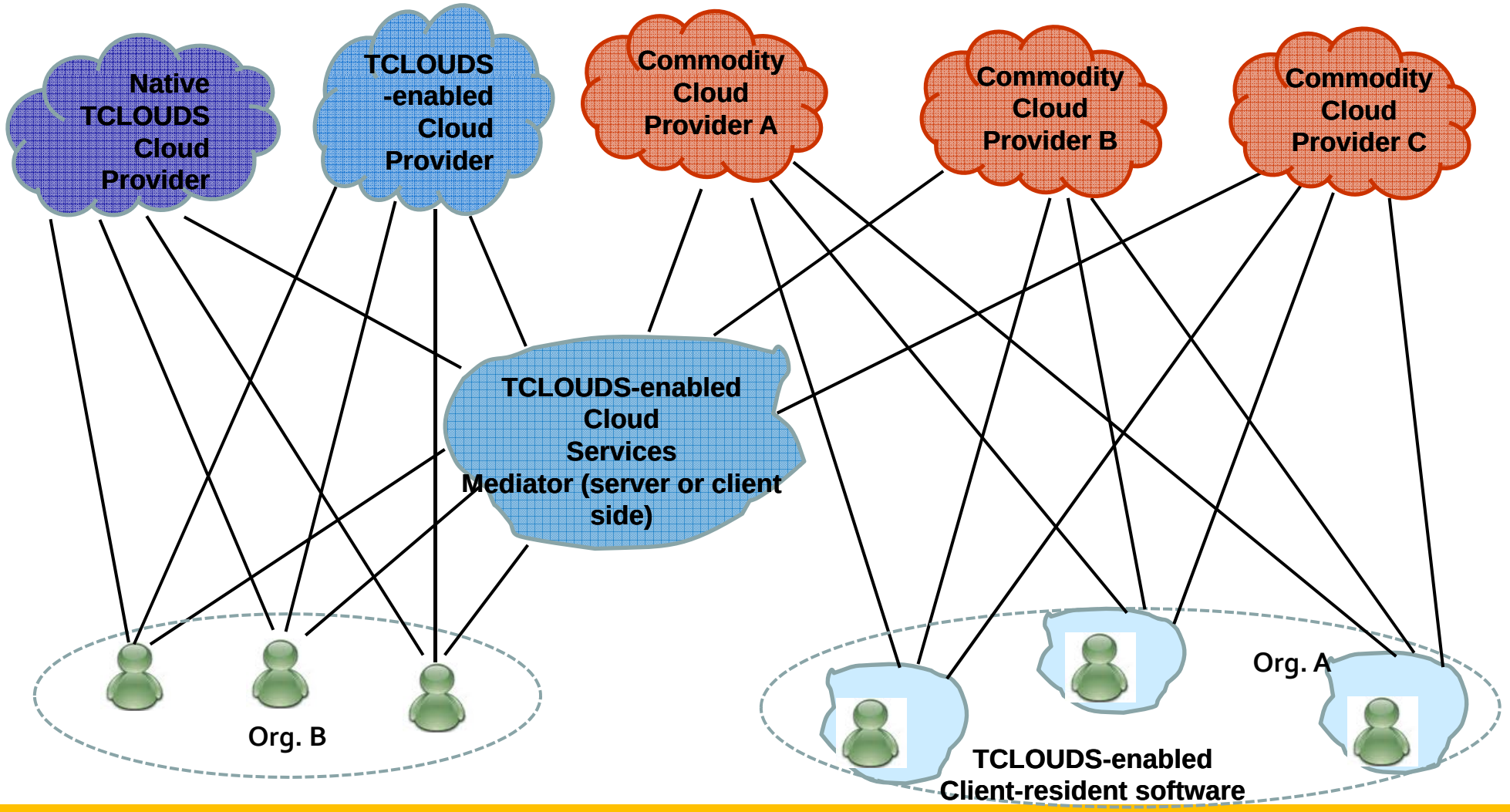


TCLOUDS big challenge

- How to allow a swift migration path from current commodity insecure clouds to future natively resilient (secure and dependable) clouds?
- How to promote, along and at the end of this road, a diverse and open ecosystem?

- How about a coherent architecture, with modular and reusable artefacts?

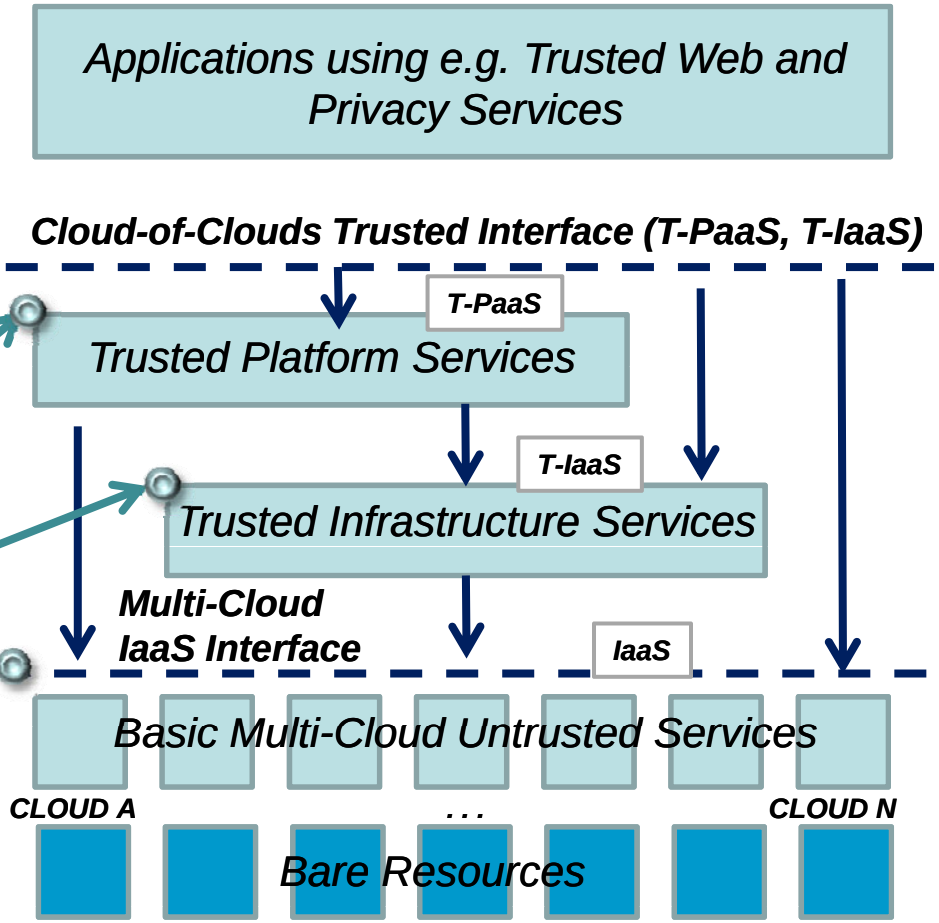
TCLOUDS Diverse ecosystem - big picture



Overview of the TCLOUDS CoC architecture

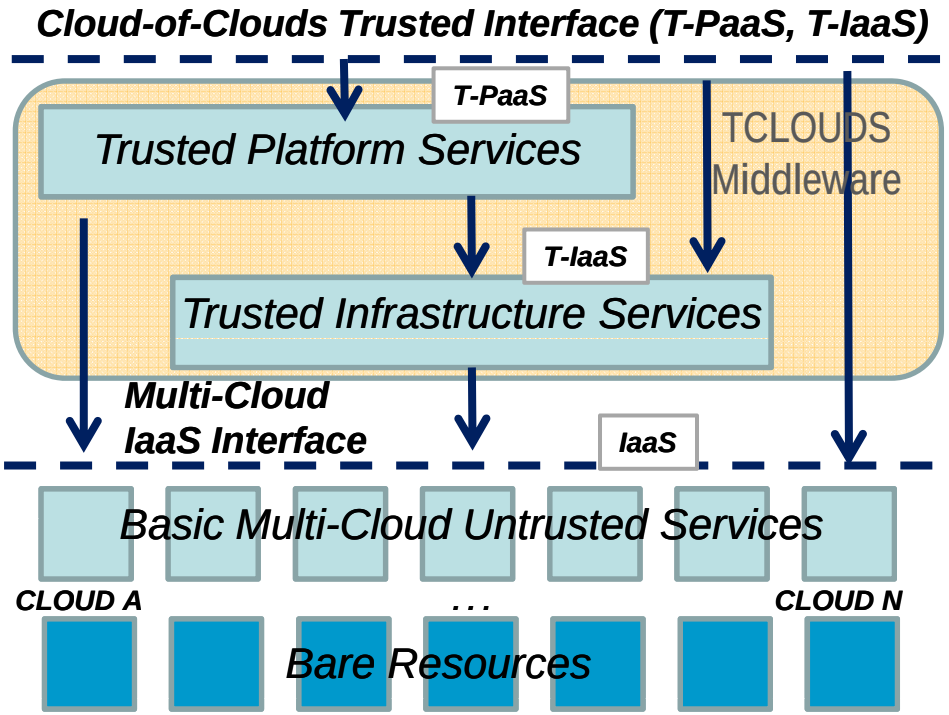
(interfaces)

- The TCLOUDS architecture thus provides applications with a **wealth of interfaces** to produce **incremental resilience solutions** with **single or multiple clouds** :
  - TCLOUDS Trusted Platform services (**T-PaaS)** on top of the middleware layer
  - TCLOUDS Trusted Infrastructure services (**T-IaaS)** from within the middleware layer
  - Infrastructure services (**IaaS)** from available commodity untrusted clouds



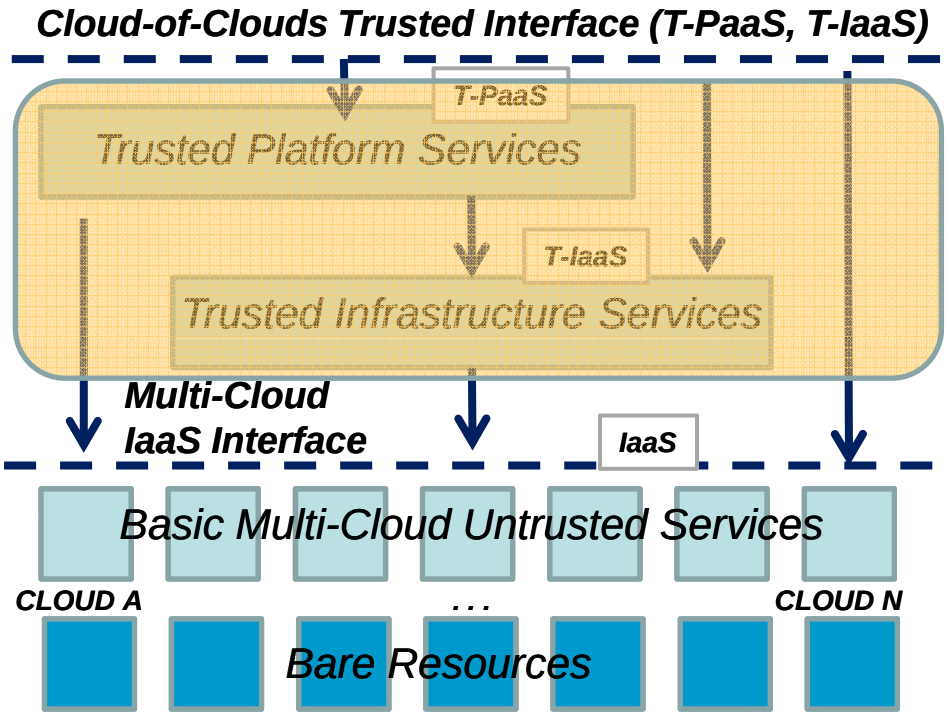
TCLOUDS design approaches

- The TCLOUDS architecture allows **several solutions for resilience** based on Trusted Platform or Infrastructure services (**T-PaaS, T-IaaS**) , with essentially a re-use of the same basic algorithms and mechanisms:
  - **T-PaaS, T-IaaS** implemented with a TCLOUDS resilient middleware layer on top of commodity clouds
  - Native TCLOUDS where resilience may also be built from scratch in the bare resources (e.g. with local low-level VM FIT mechanisms)
  - TCLOUDS middleware is by nature cloud-of-clouds, and **T-PaaS, T-IaaS** can be implemented with any mix of native TCLOUDS, "T-cloudified" commodity clouds with local resilience layer, and commodity clouds



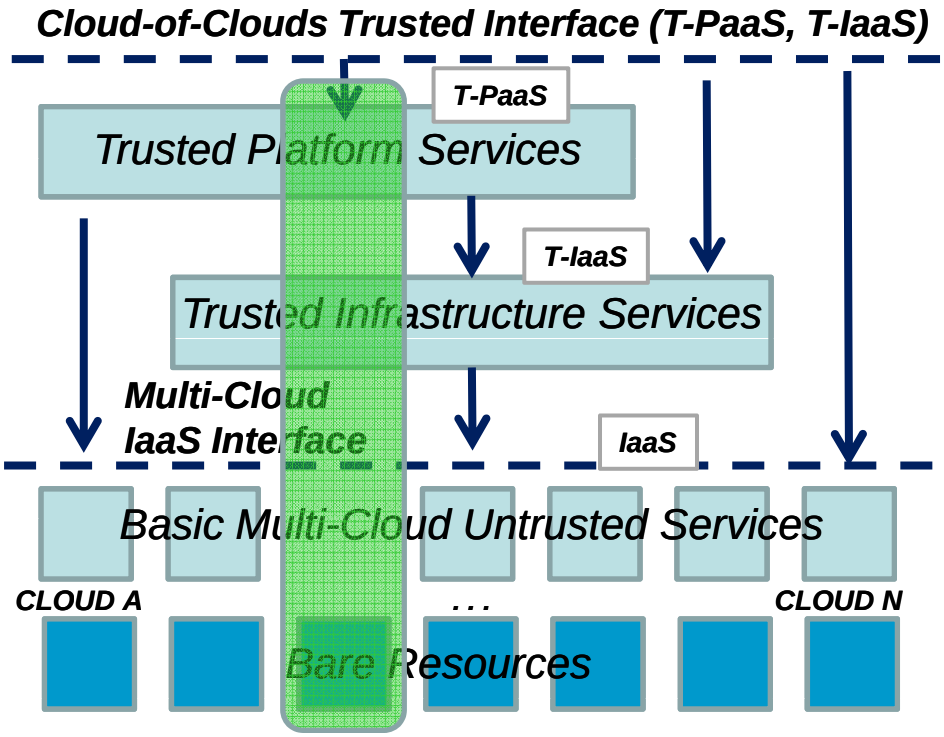
TCLOUDS design approaches

- The TCLOUDS architecture allows **several solutions for resilience** based on Trusted Platform or Infrastructure services (**T-PaaS, T-IaaS**) , with essentially a re-use of the same basic algorithms and mechanisms:
  - **T-PaaS, T-IaaS** implemented with a TCLOUDS resilient middleware layer on top of commodity clouds
  - Native TCLOUDS where resilience may also be built from scratch in the bare resources (e.g. with local low-level VM FIT mechanisms)
  - TCLOUDS middleware is by nature cloud-of-clouds, and **T-PaaS, T-IaaS** can be implemented with any mix of native TCLOUDS, "T-cloudified" commodity clouds with local resilience layer, and commodity clouds



TCLOUDS design approaches

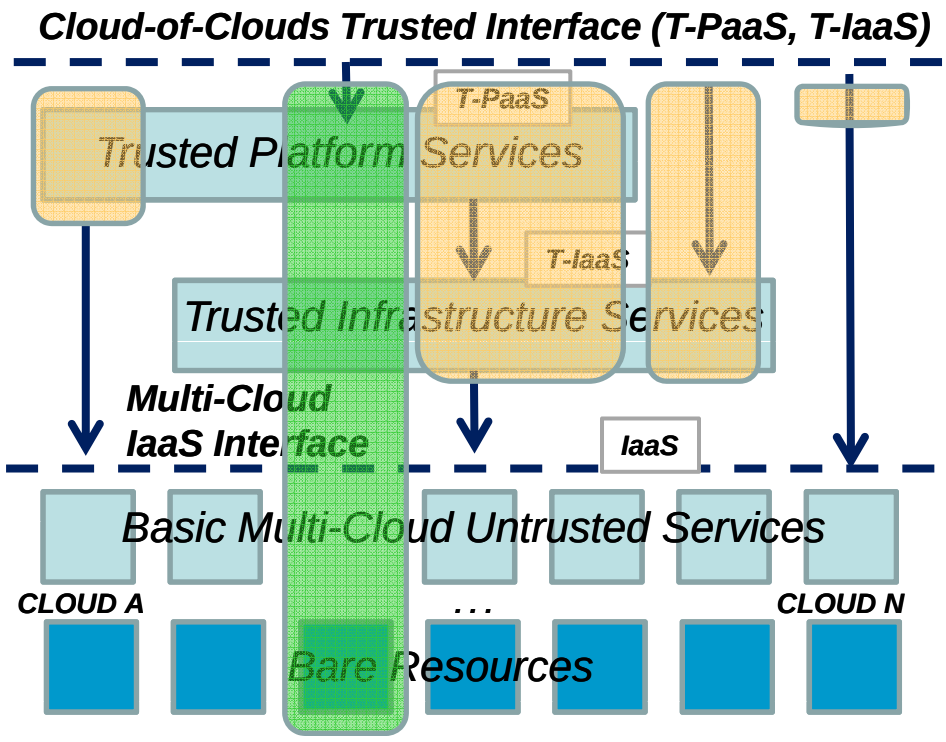
- The TCLOUDS architecture allows **several solutions for resilience** based on Trusted Platform or Infrastructure services (**T-PaaS, T-IaaS**) , with essentially a re-use of the same basic algorithms and mechanisms:
  - **T-PaaS, T-IaaS** implemented with a TCLOUDS resilient middleware layer on top of commodity clouds
  - Native TCLOUDS where resilience may also be built from scratch in the bare resources (e.g. with local low-level VM FIT mechanisms)
  - TCLOUDS middleware is by nature cloud-of-clouds, and **T-PaaS, T-IaaS** can be implemented with any mix of native TCLOUDS, "T-cloudified" commodity clouds with local resilience layer, and commodity clouds



TCLOUDS design approaches

- The TCLOUDS architecture allows **several solutions for resilience** based on Trusted Platform or Infrastructure services (**T-PaaS, T-IaaS**) , with essentially a re-use of the same basic algorithms and mechanisms:
  - **T-PaaS, T-IaaS** implemented with a TCLOUDS resilient middleware layer on top of commodity clouds
  - Native TCLOUDS where resilience may also be built from scratch in the bare resources (e.g. with local low-level VM FIT mechanisms)

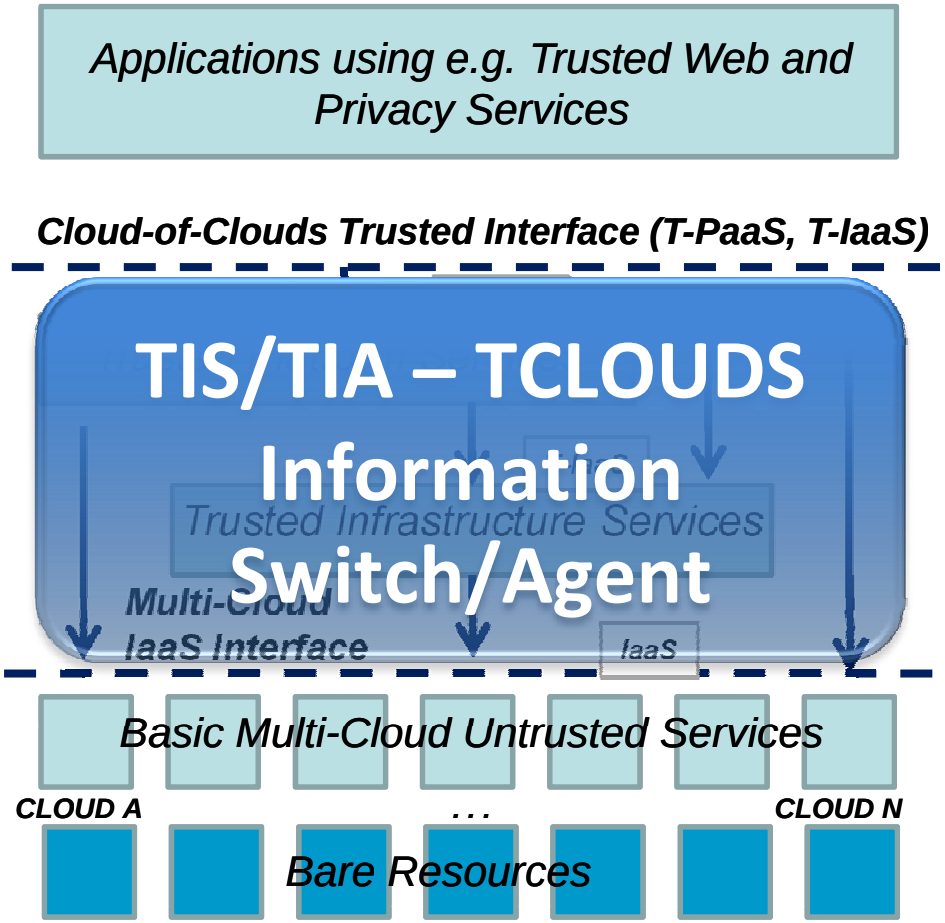
- TCLOUDS middleware is by nature cloud-of-clouds, and **T-PaaS, T-IaaS** can be implemented with any mix of native TCLOUDS, "T-cloudified" commodity clouds with local resilience layer, and commodity clouds



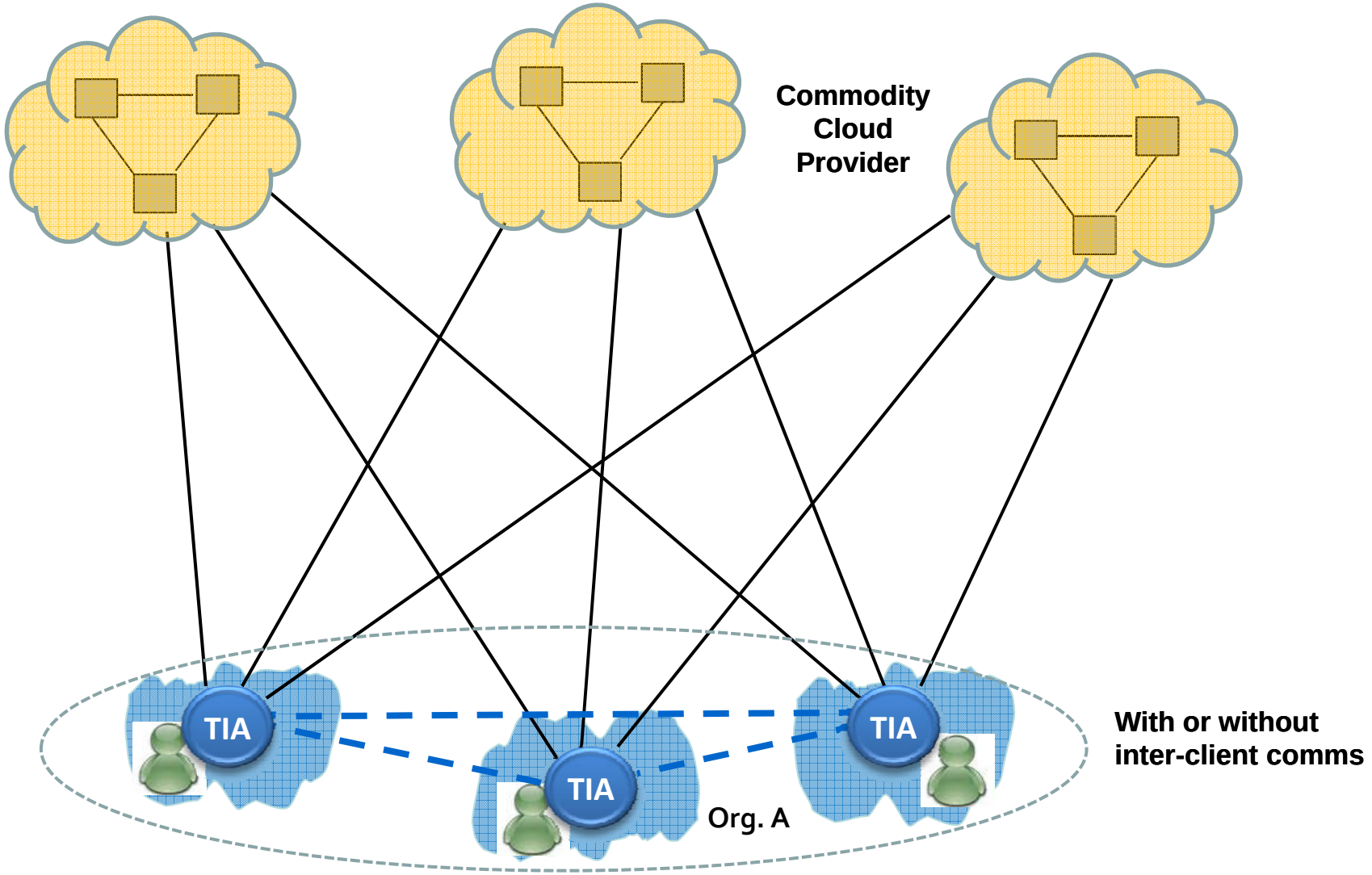
TCLOUDS Architecture

TIS – key to modularity and encapsulation

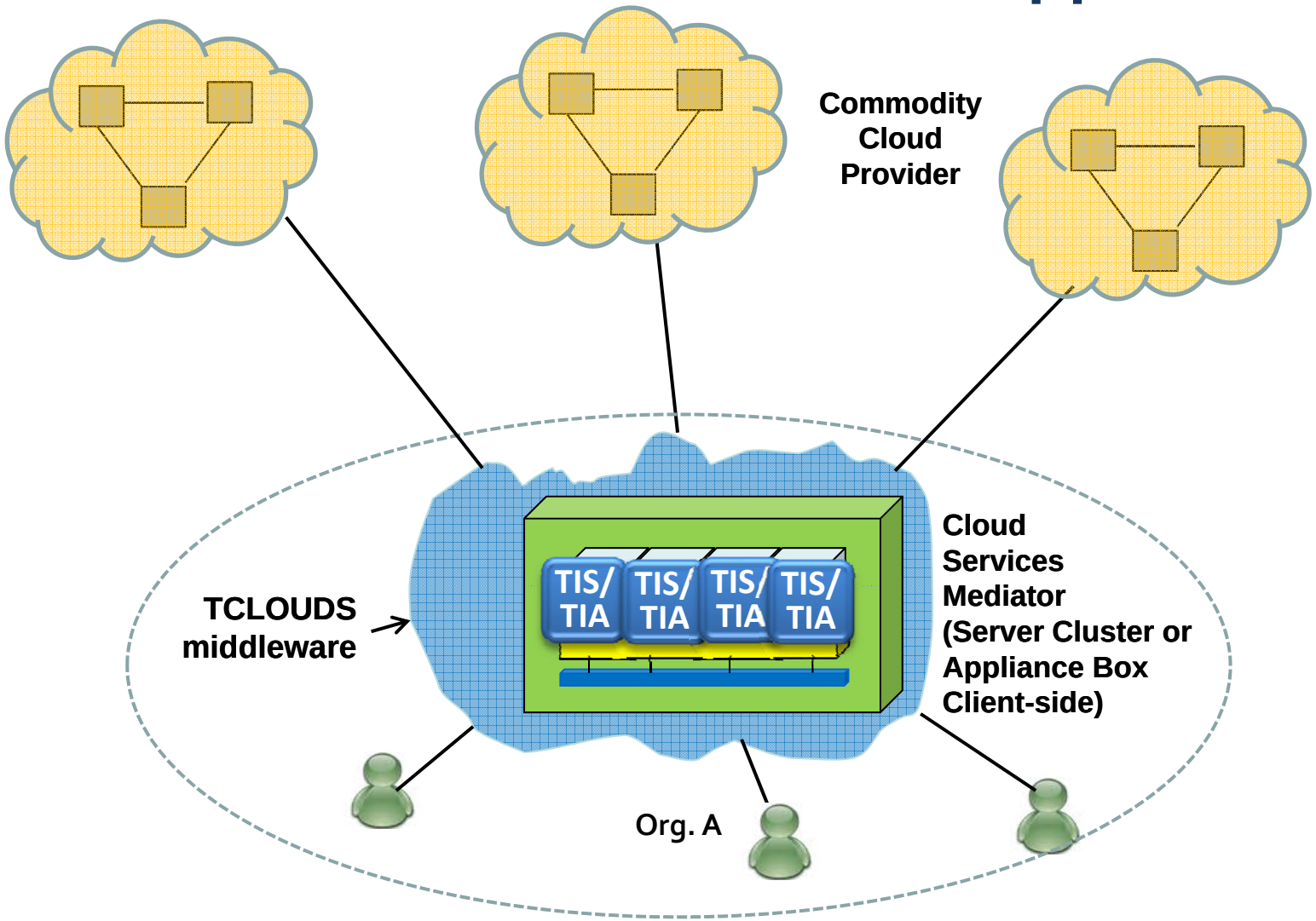
- TCLOUDS can either be **deployed by final users, third-party providers, or commodity providers** wishing to directly offer some form of cloud resilience
- To allow **seamless deployment** of these instantiations, we introduce the ***TIS – TCLOUDS Information Switch*** concept, which encapsulates all or part of the services defined in the TCLOUDS architecture
- These units, with the adequate configuration and placement, materialize the several TCLOUDS incarnations in a modular way



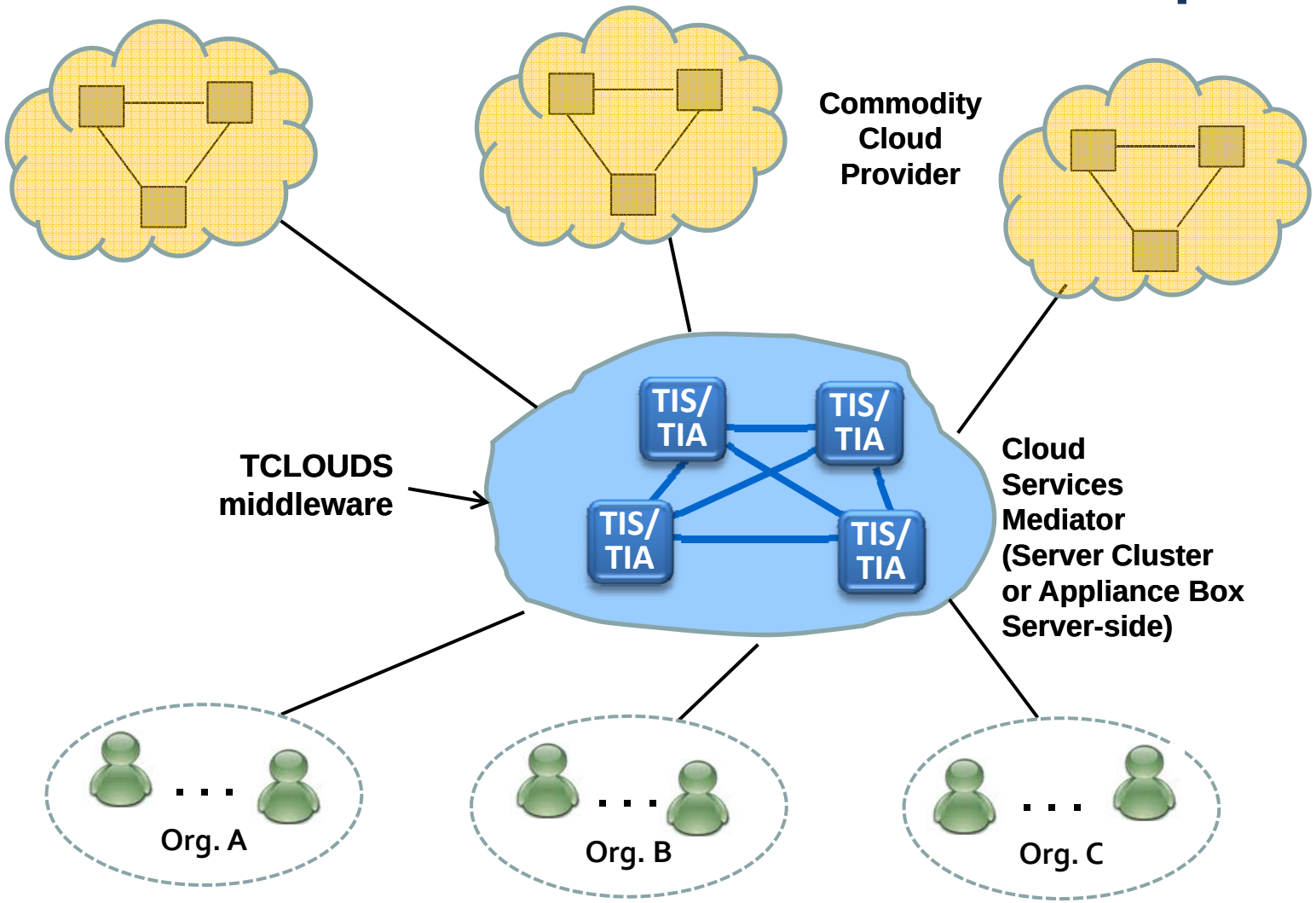
Macro view: Arch. with Client-resident SW



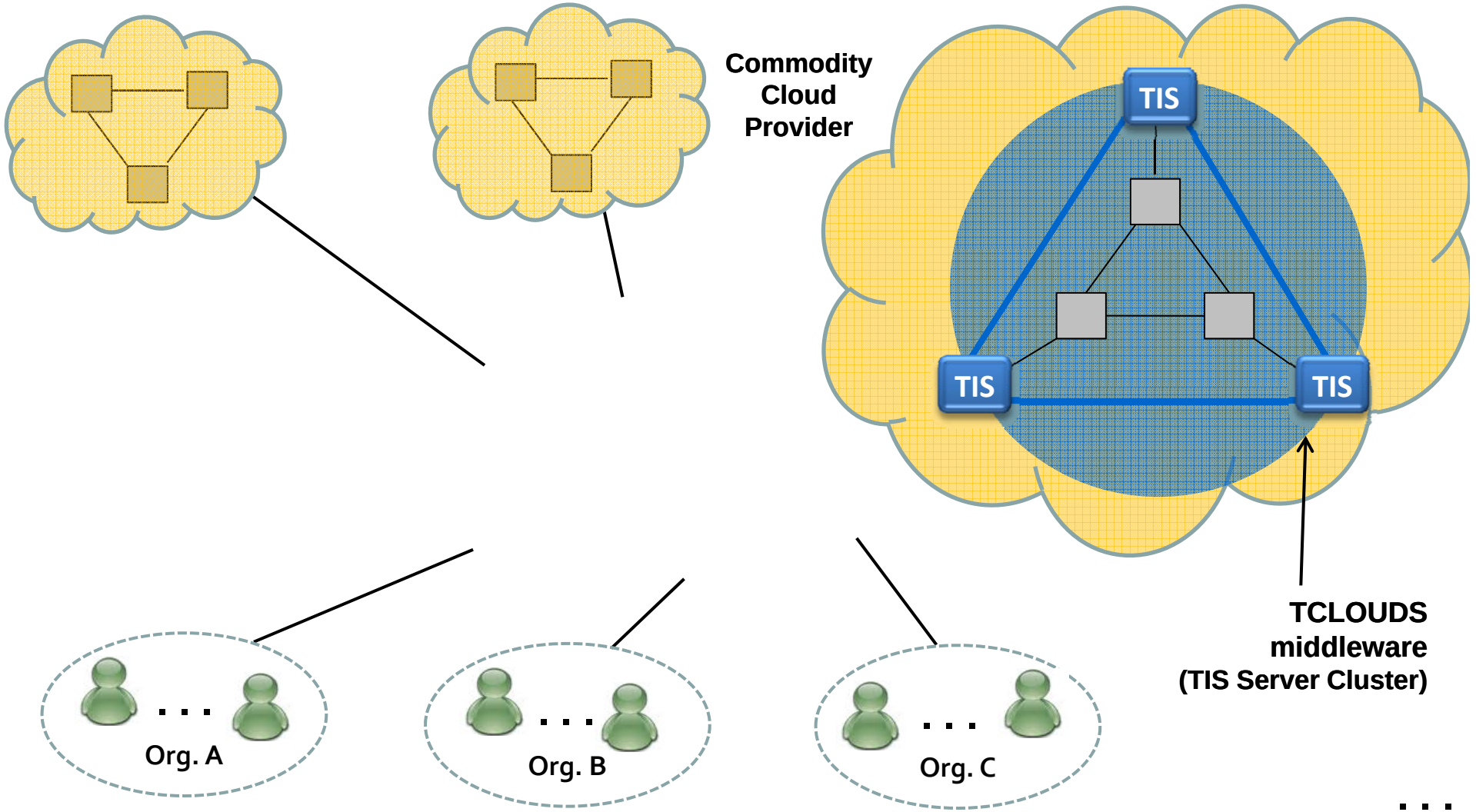
Macro view: Arch. with OEM Appliance box



Macro view: Arch. with OEM Cloud provider



Macro view: Arch. with TCLOUDS-enabled Cloud Provider



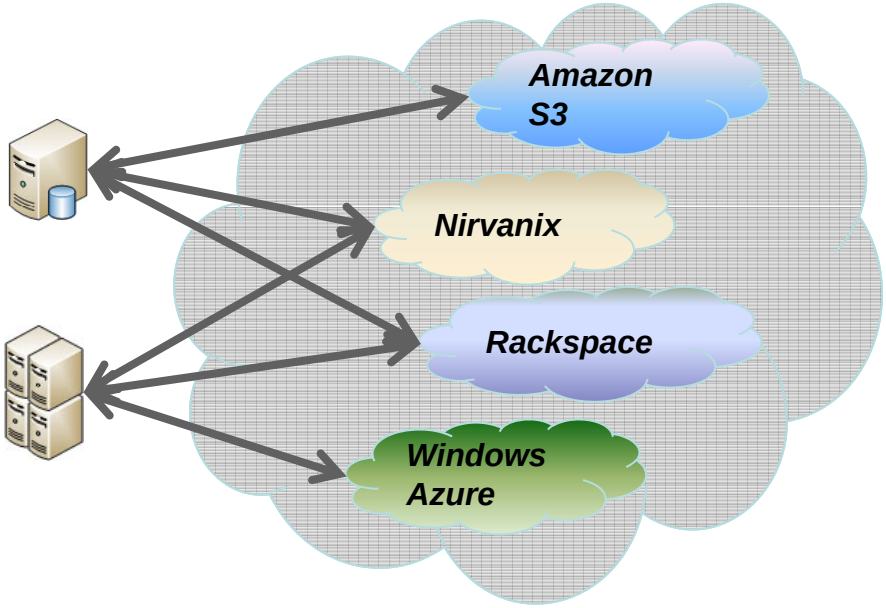
TClouds

SEVENTH FRAMEWORK PROGRAMME

A concrete proof-of-concept result with the TCLOUDS architecture:

DepSky – Dependable and Secure Storage in a Cloud-of-Clouds

[Bessani et al., ACM Sigops Eurosys 2011]



DepSky Design Principles

1. No trust on individual cloud providers

Distributed trust is built by independent mechanisms over commodity multi-cloud environments

2. Use storage clouds as they are

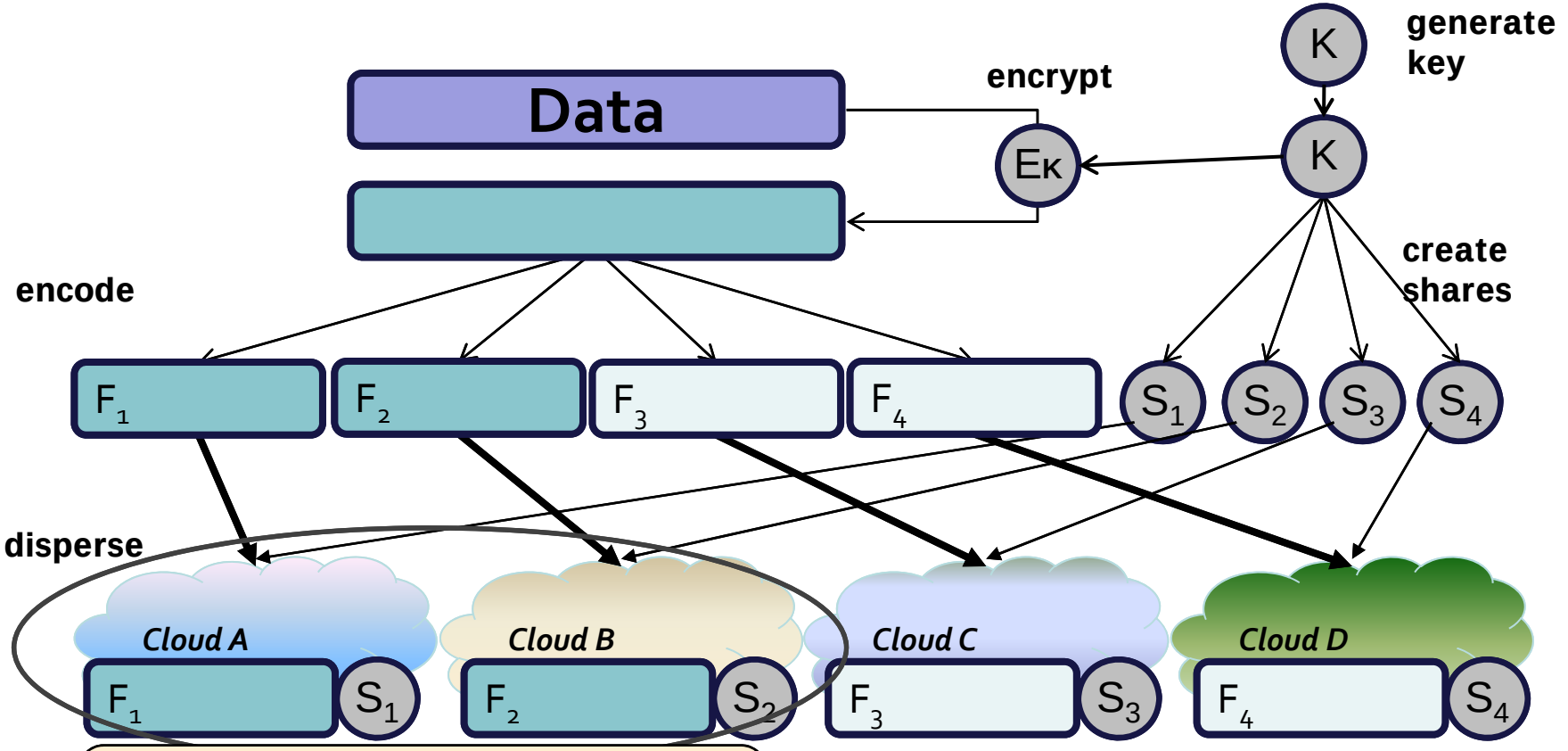
No server-side code needed on the cloud

3. Data is updatable

Quorum replication protocols for consistency

Storage Confidentiality, Availability and Efficiency

Combining Erasure Codes and Robust Secret Sharing [Krawczyk 1993]

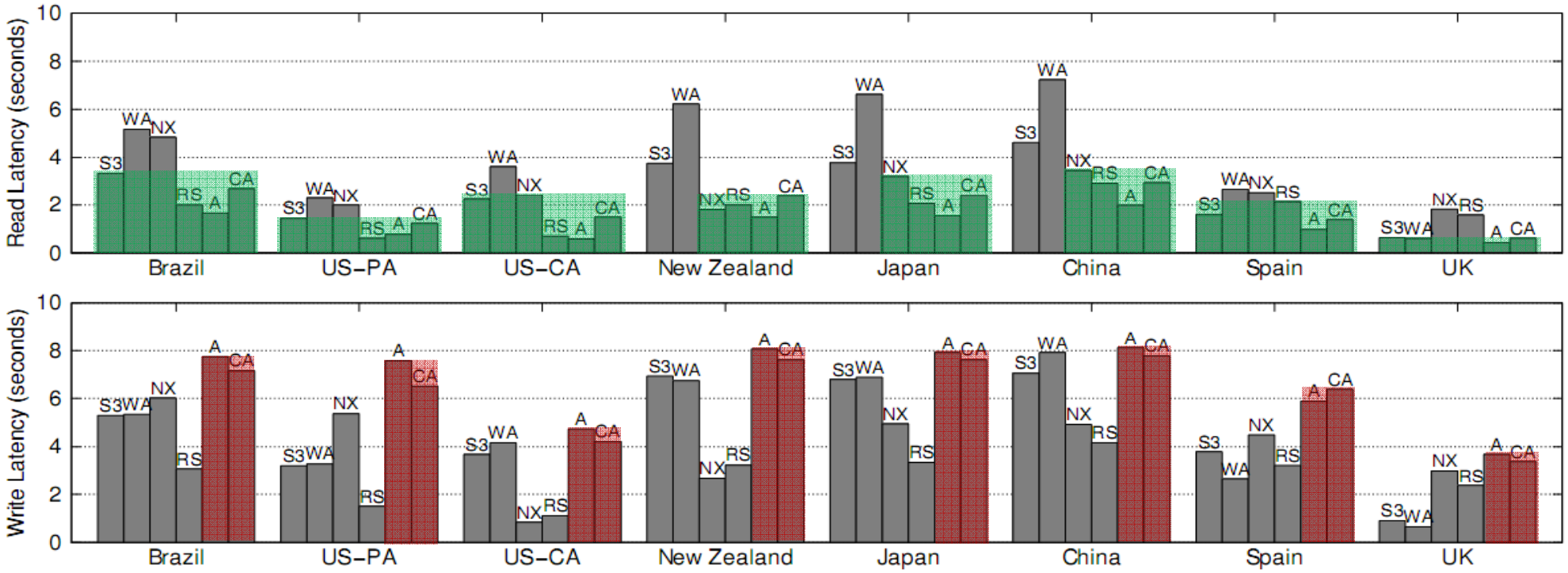


Inverse process for reading from *f+1* shares/fragments.

DepSky Latency (100kb DU)

A (avail.+integrity)
CA (+confidentiality)

DepSky **read** latency is close to the cloud with the **best** latency



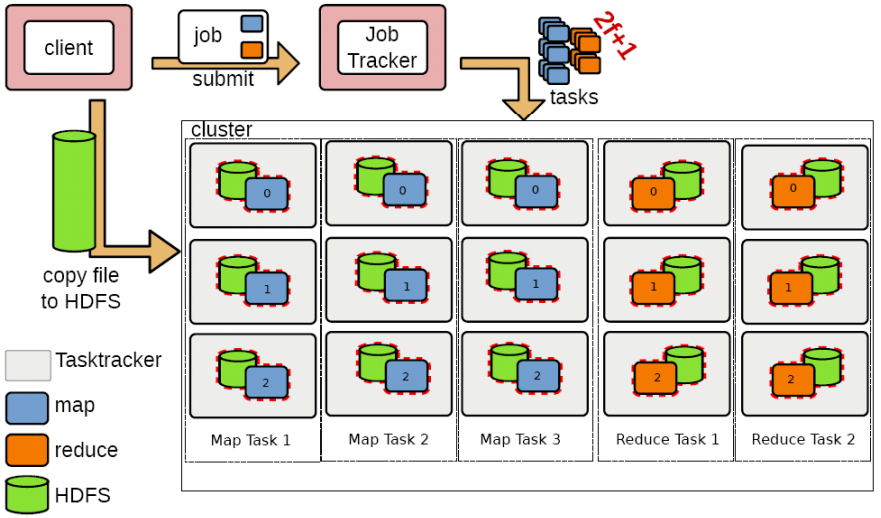
DepSky **write** latency is close to the cloud with the **worst** latency

TClouds

Other results:

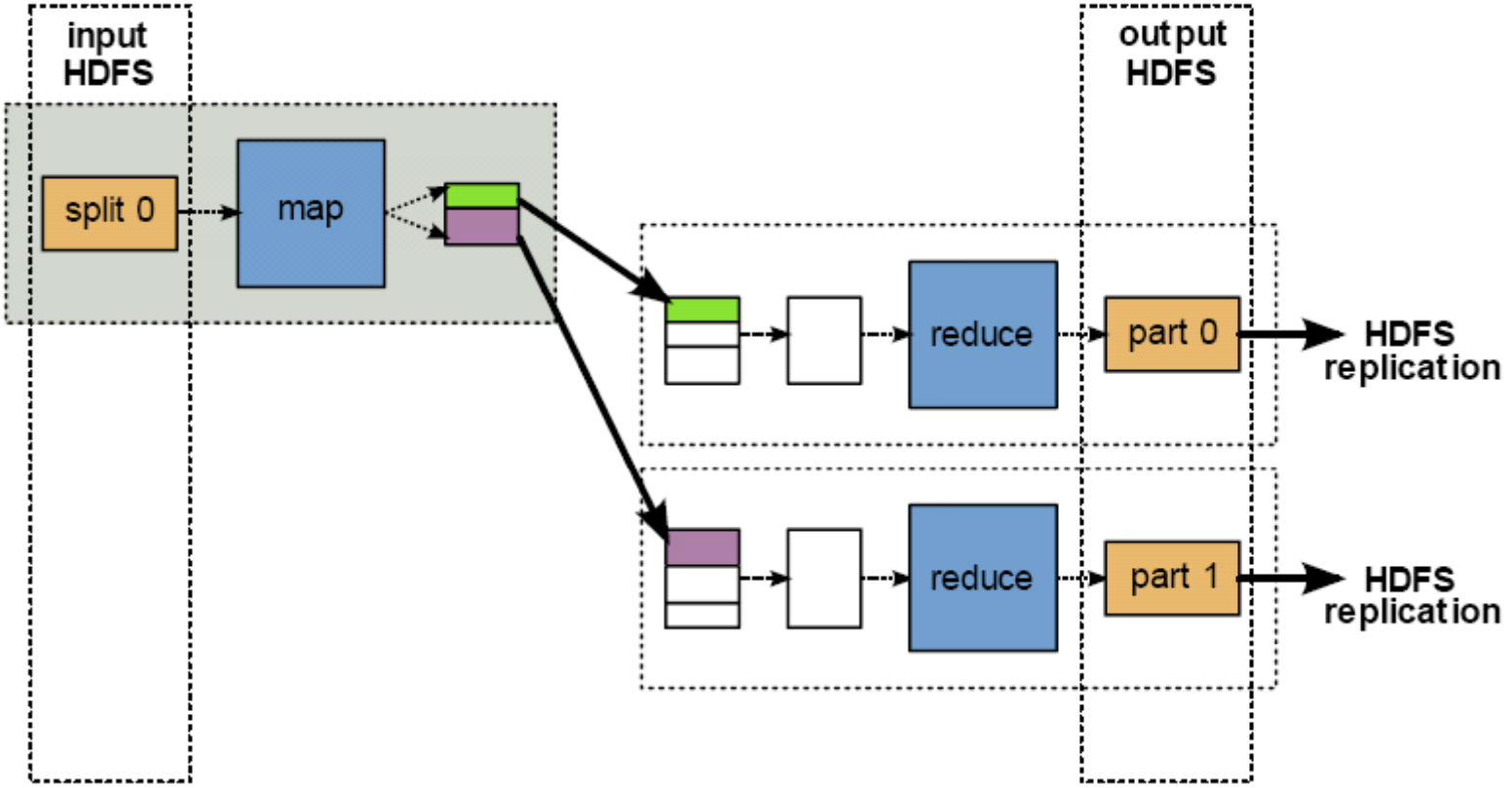
Byzantine Fault-Tolerant MapReduce: Faults Are Not Just Crashes

[Costa et al., IEEE CloudCom 2011, Best Paper Award]



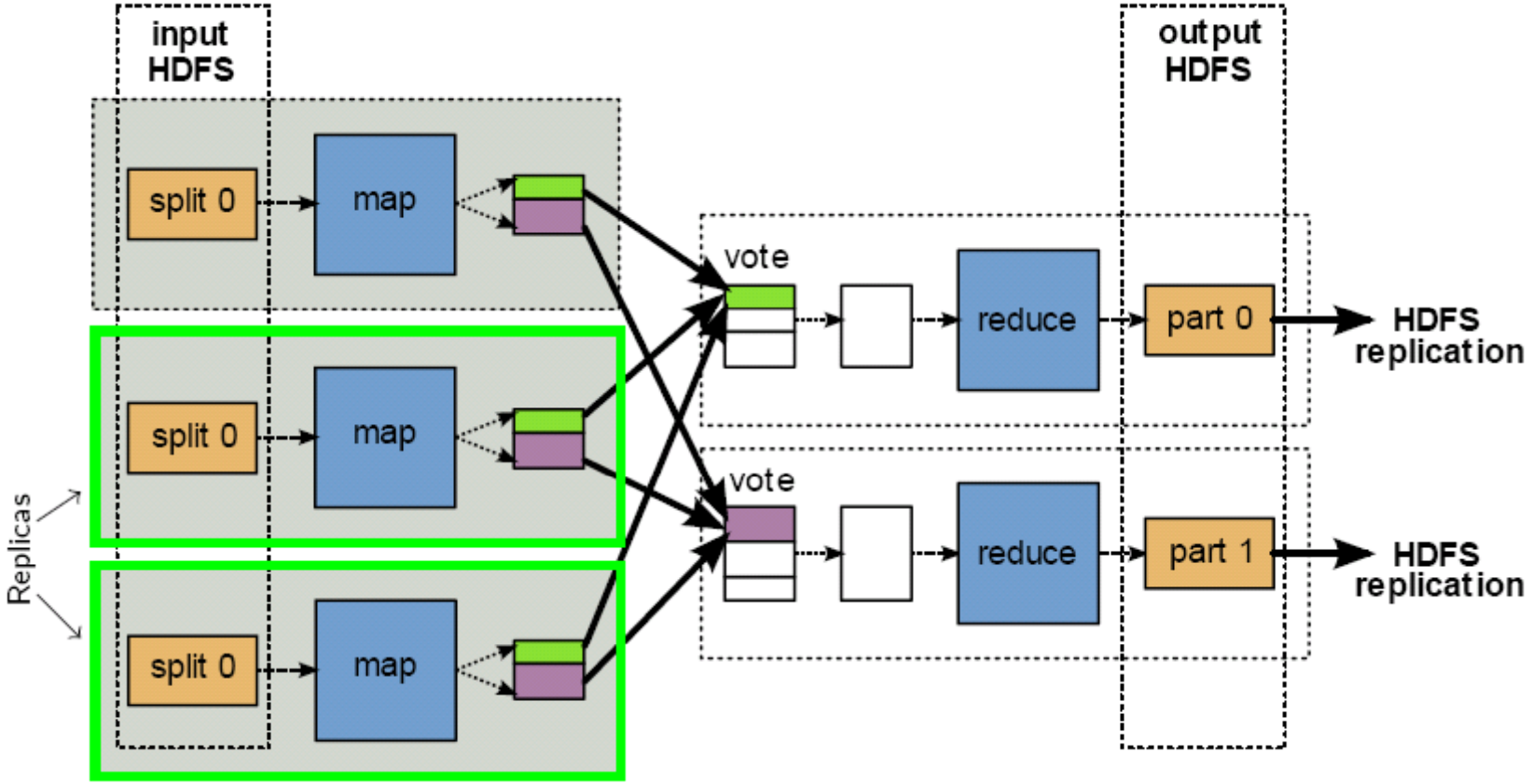
MapReduce

(Map perspective - original)



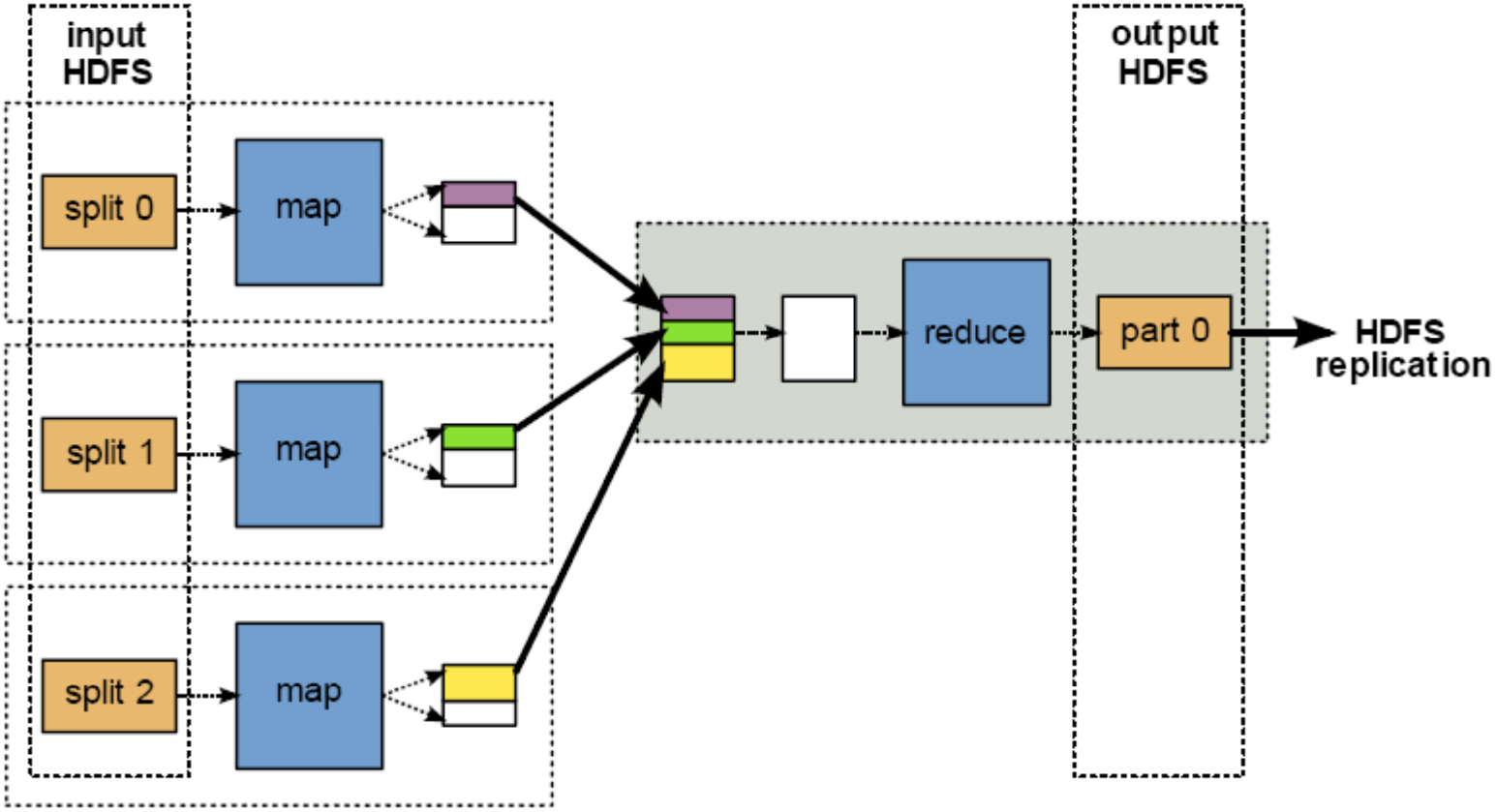
MapReduce

(Map perspective - BFT)



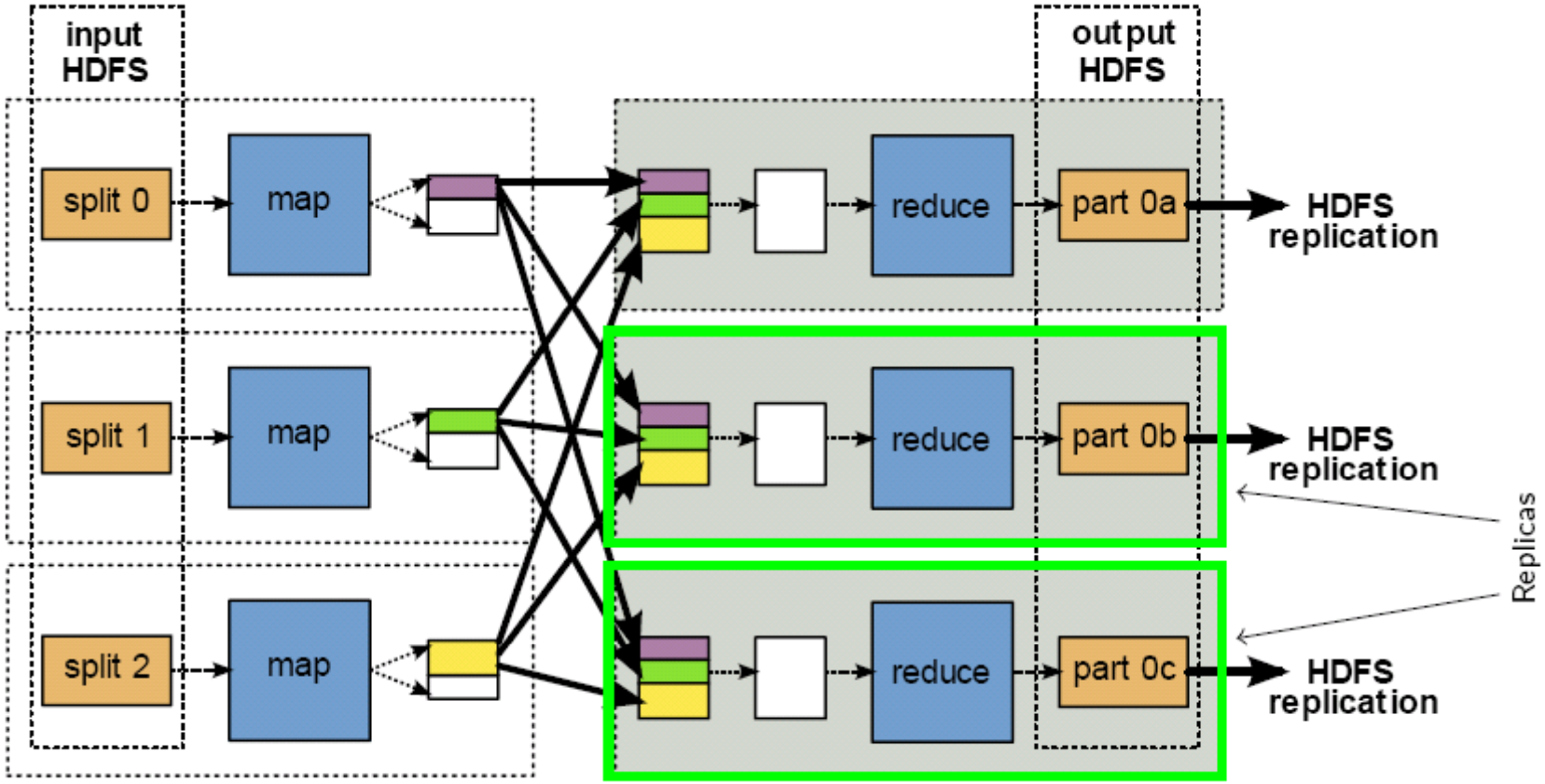
MapReduce

(Reduce perspective - original)



MapReduce

(Reduce perspective - BFT)

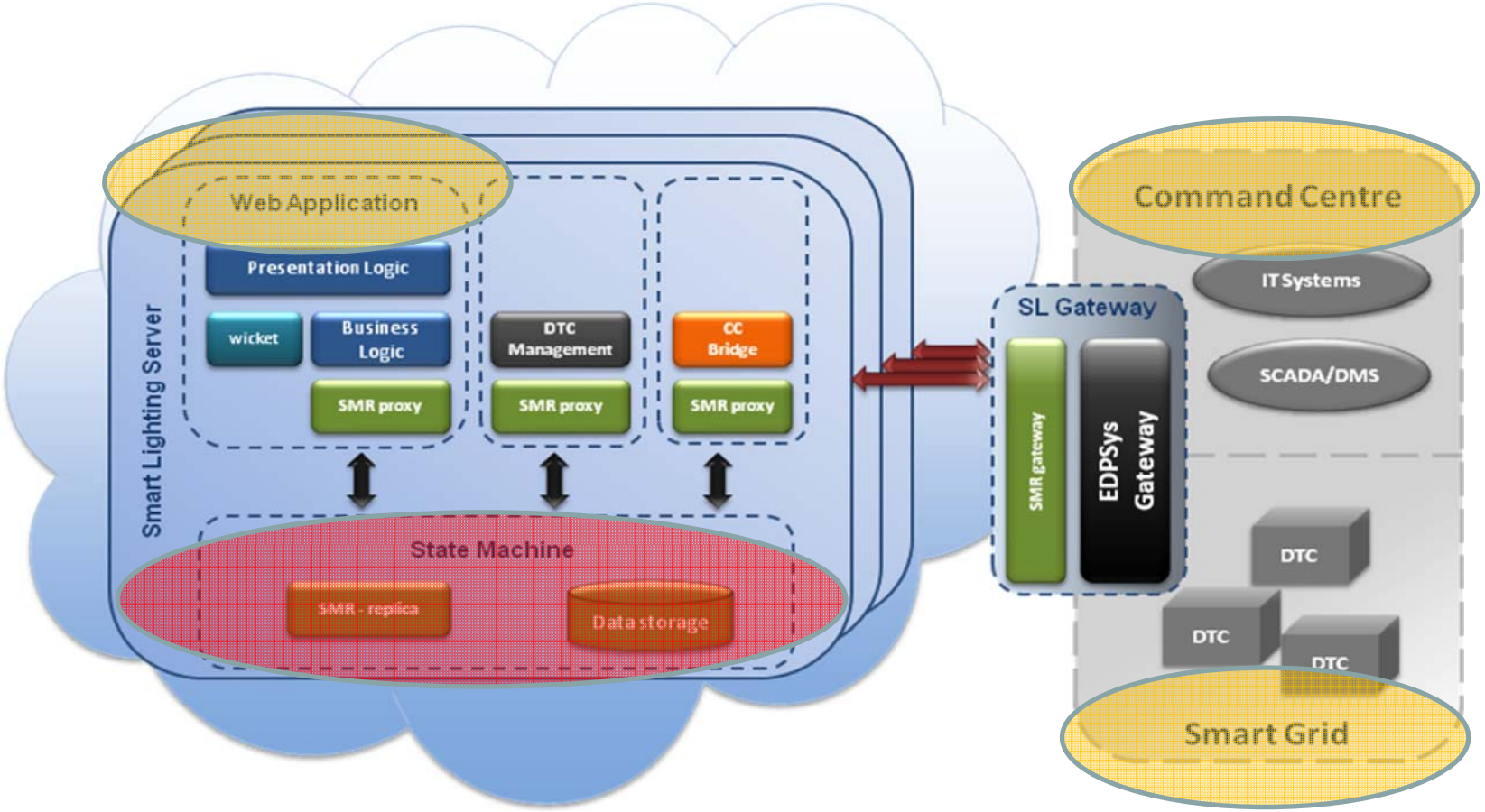


Other results:

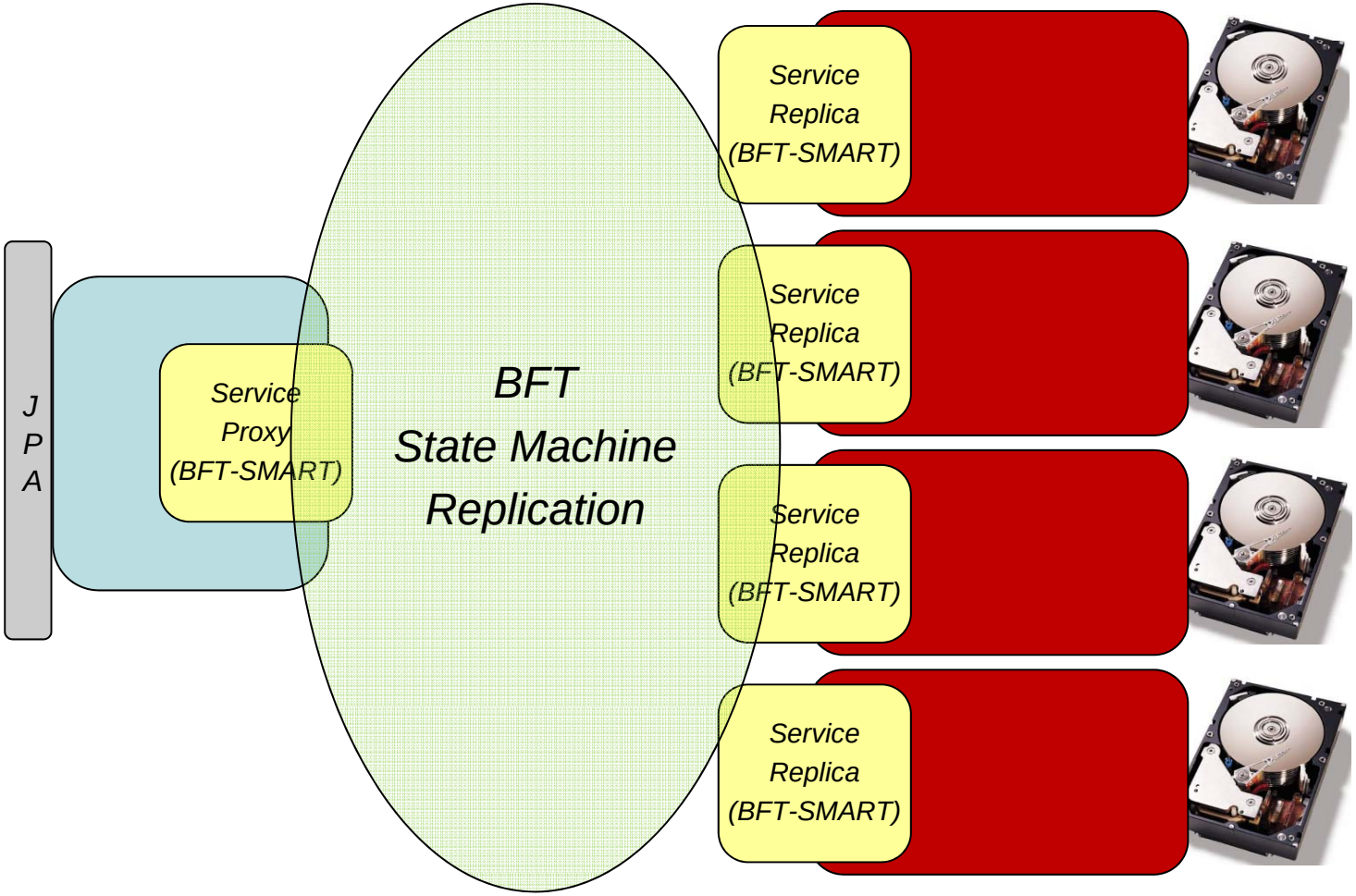
JPA(*)-compatible Cloud-of-Clouds Dependable Storage System for Smart Grid applications (together with Efacec and EDP)

(*) Java Persistence API

Smart Lighting Use Case Components



Custom JPA-compatible storage



Mnemonic for Contacts

google “Navigators home page”

http://navigators.di.fc.ul.pt

Thank you!