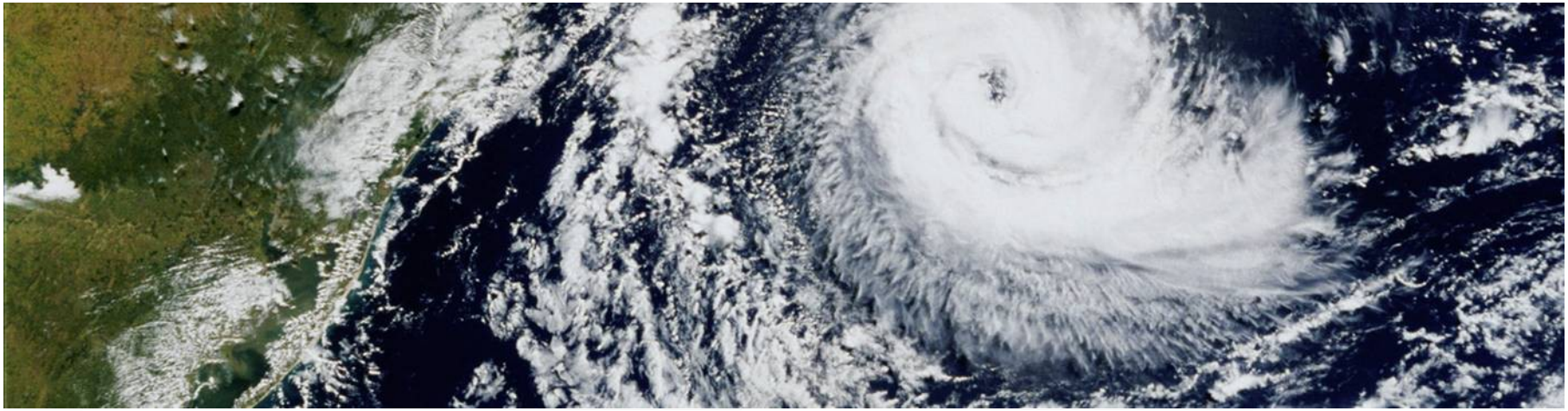
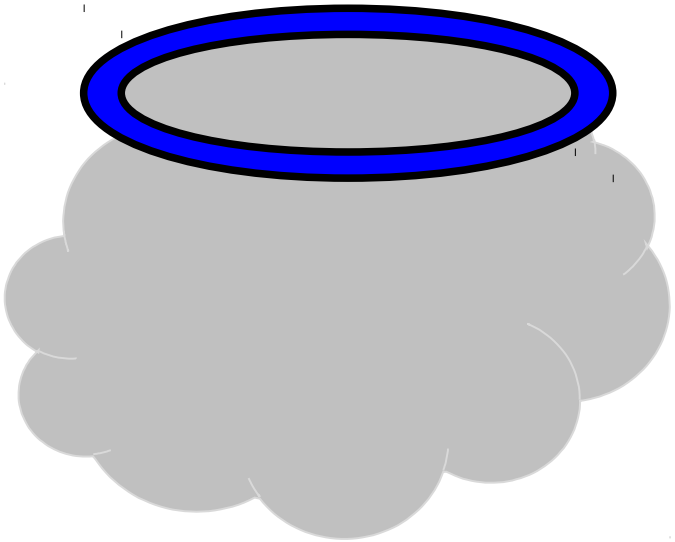
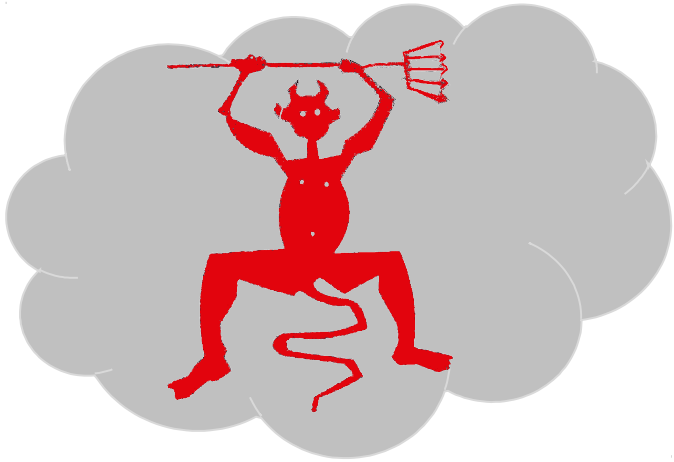
IBM Research – Zurich
Christian Cachin
12 September 2013

Towards Trustworthy Clouds



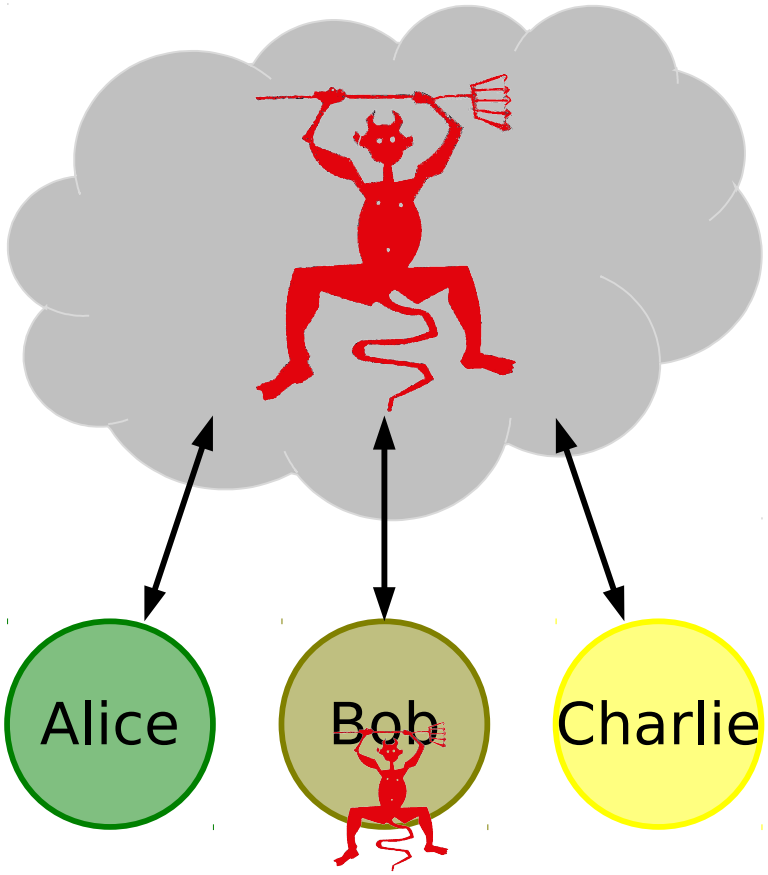
Cloud computing?





- Cloud services are convenient
  - No investment cost
  - Pay only for consumption
  - Scalable
  - No skills needed
  - Access from everywhere
  - Standardized services
- Clouds pose threats
  - Unknown exposure
  - Inherent risk of outsourcing
  - No established contracts
  - Loss of control
  - Fast and reliable network needed
  - Customization not possible

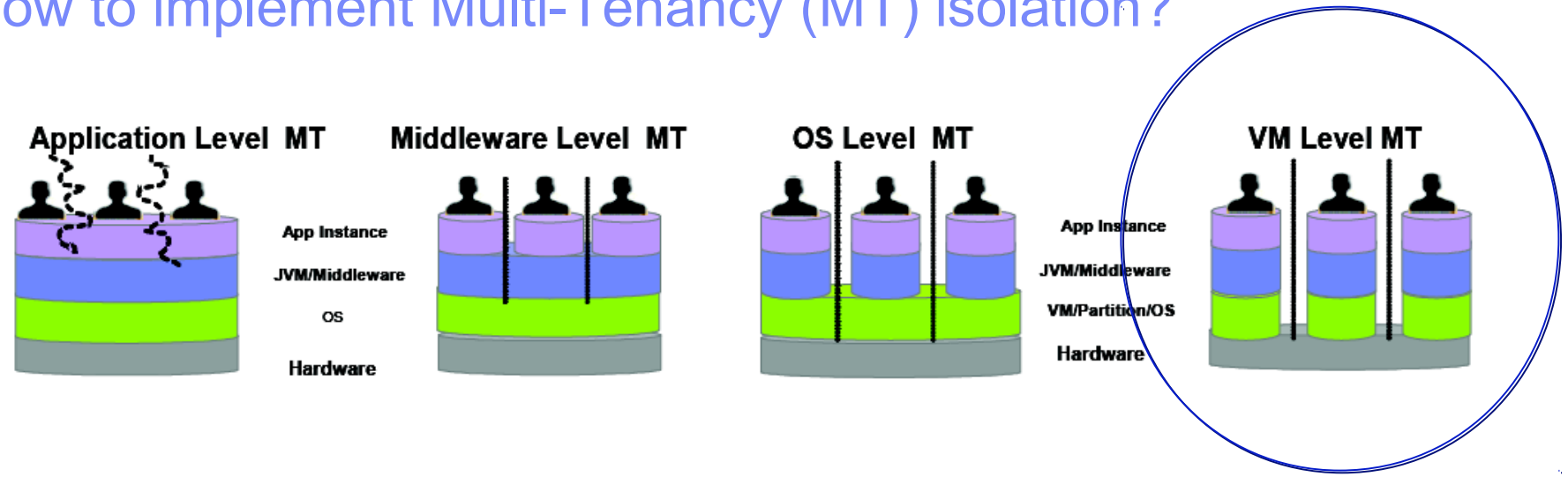
Cloud computing security



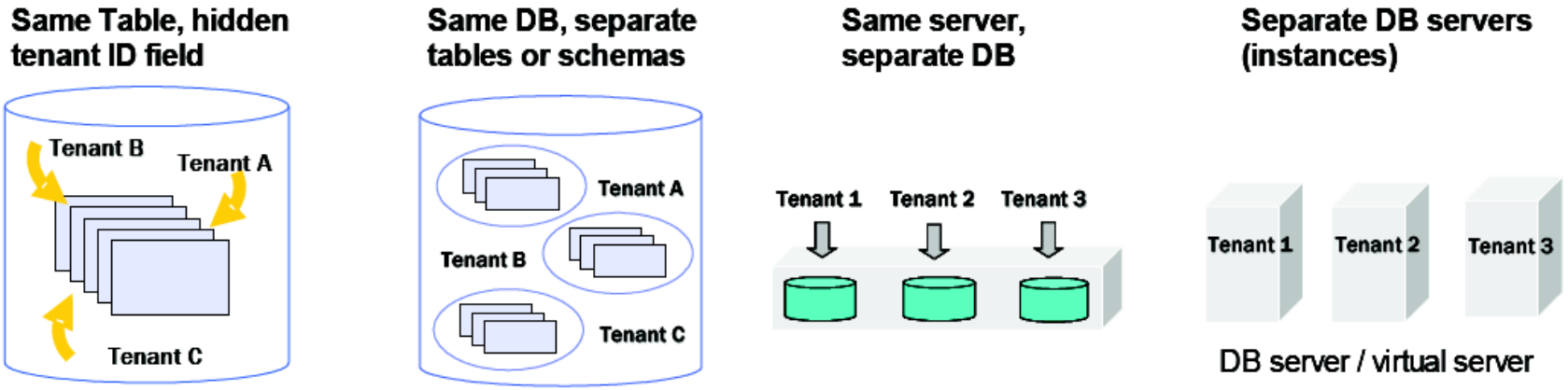
Security for the provider

- Isolation of different clients
  - Enforcement
  - Verification
- Protection of computing platform (TCB)
  - Integrity of hypervisors, kernels, and applications
  - Strong enforcement with trusted hardware
- Prevention of insider attacks
  - Operators have reduced privileges
  - Audits and logging
- Guarantees for service quality
  - Prevent abuse and DOS attacks by clients

How to implement Multi-Tenancy (MT) isolation?



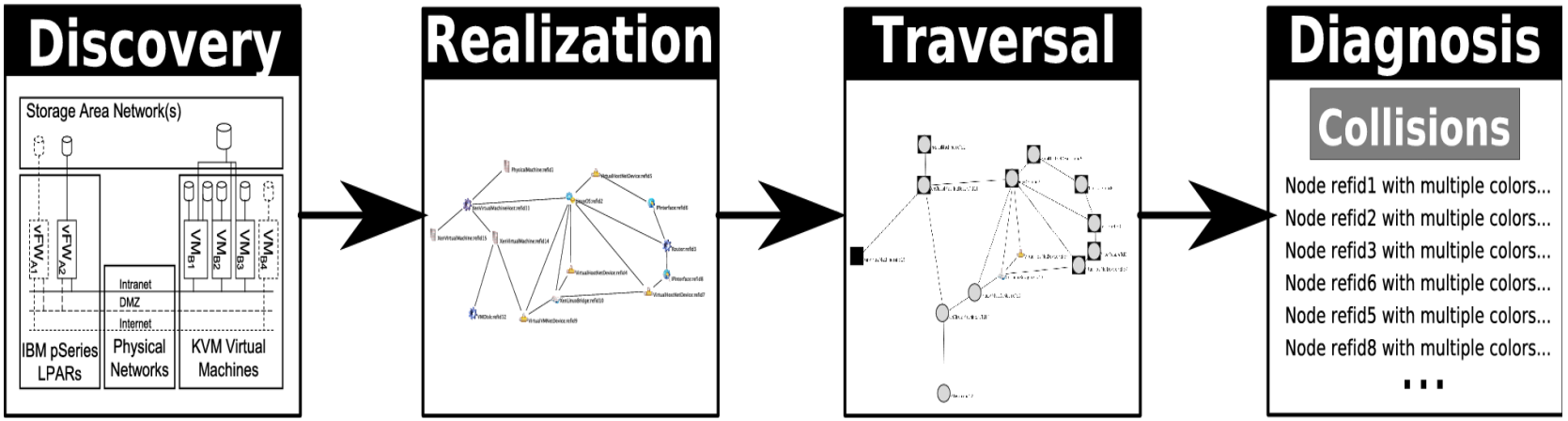
Example: Database multi-tenancy



Platform isolation enforcement and verification

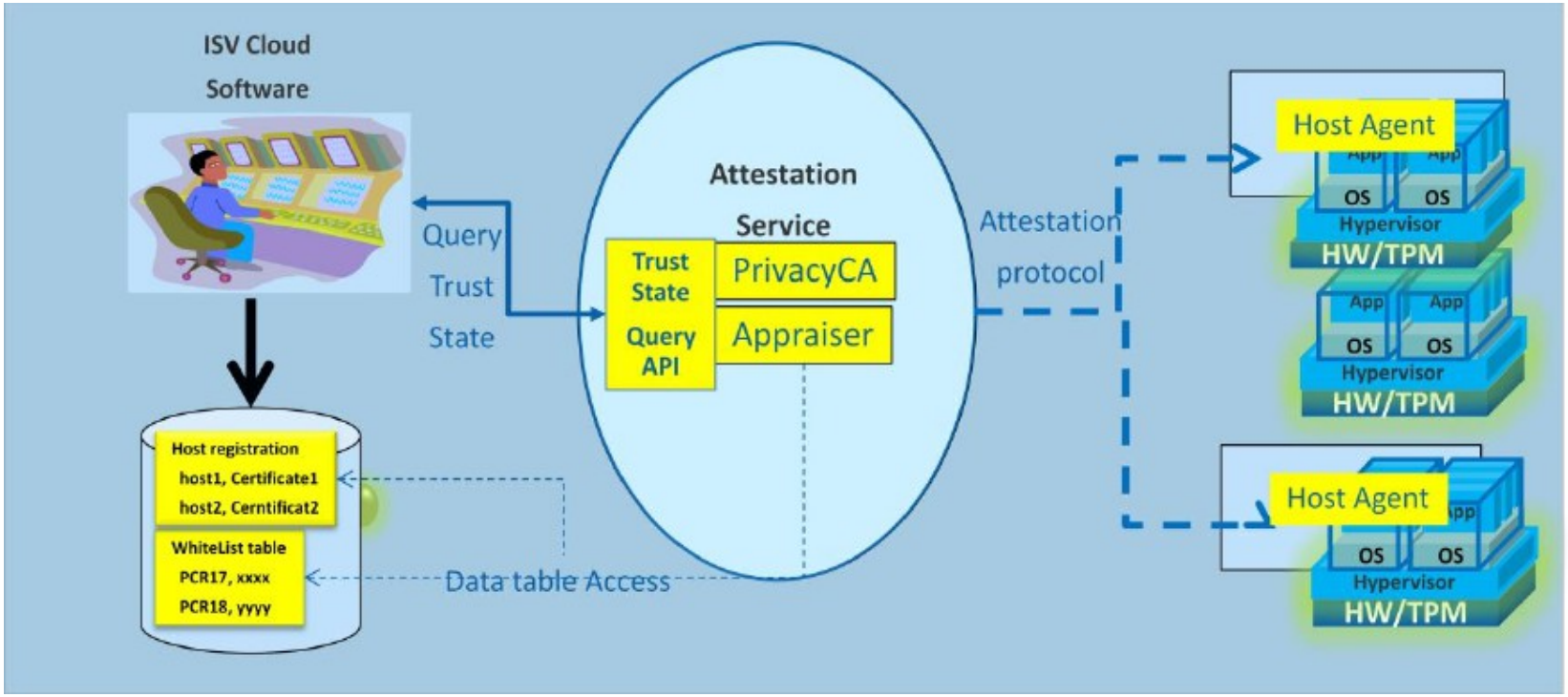
- Security analysis for virtualized environments (SAVE) [BGSE11]
  - Verify absence of connections across security zones

[See previous presentation in workshop]



Platform integrity enforcement

- Trusted-computing-based remote attestation
  - Verify integrity of remote (cloud) service platform

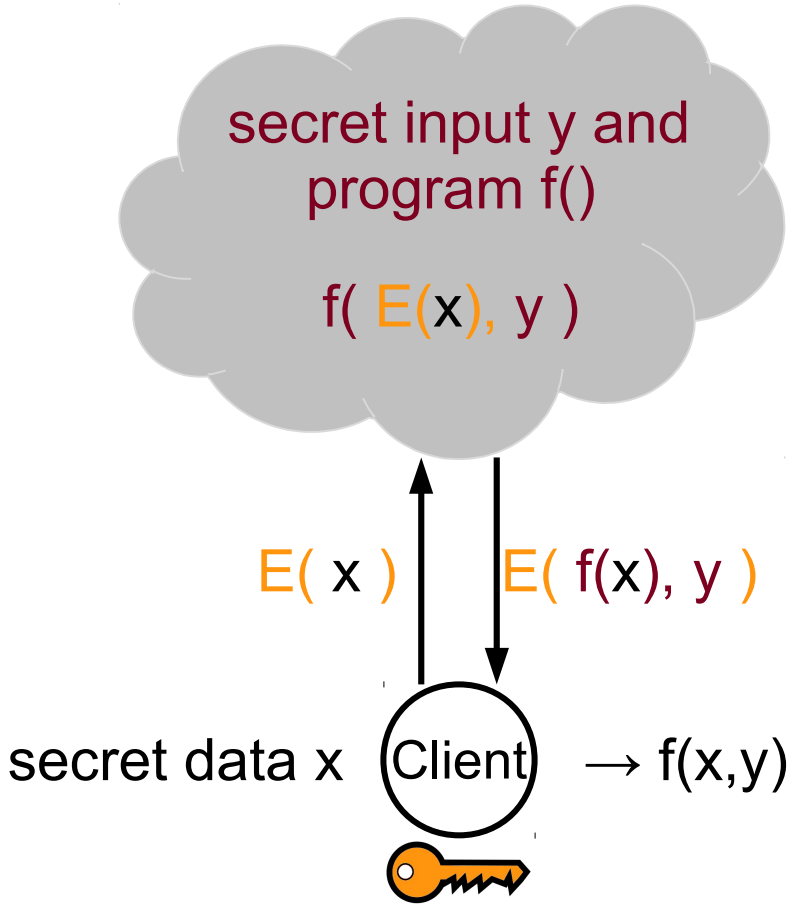


Security for clients

- Prevention of abuse by provider
  - Restriction of administrative privileges
  - Consideration of "legal" attacks by provider's jurisdiction
- Encryption of data and computations
  - Easy for stored data
  - Challenging for remotely running programs
- Integrity guarantees for responses
- High availability despite service outages

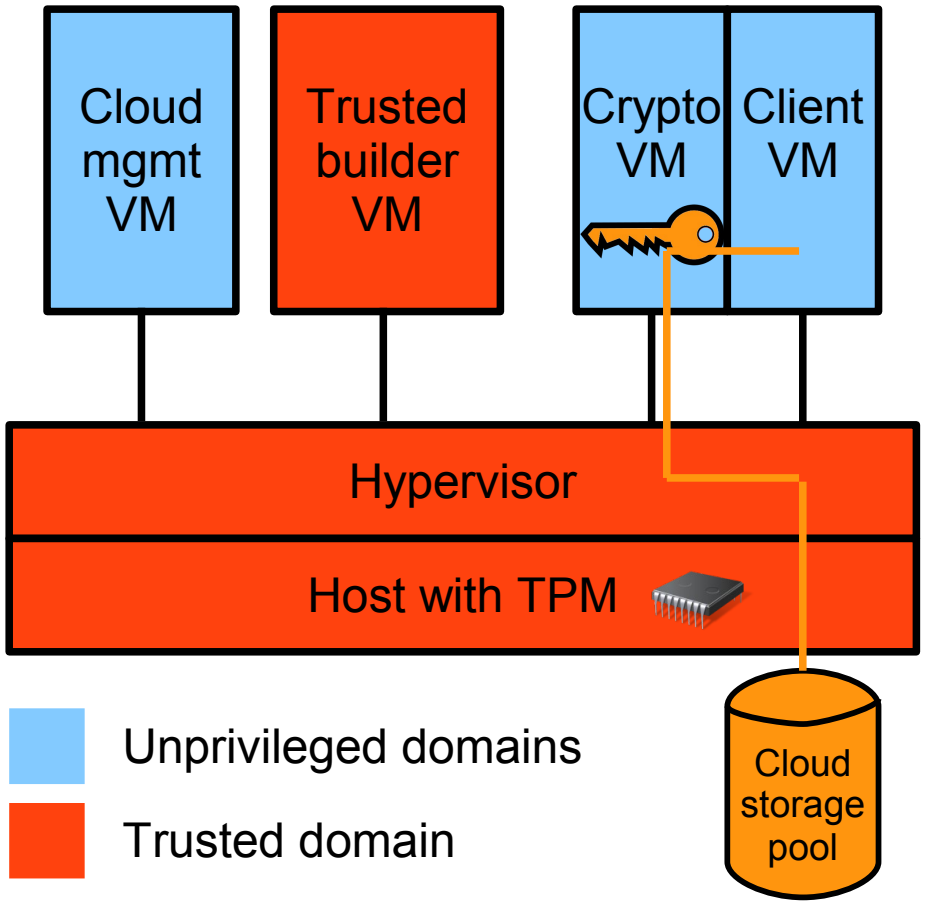
Computing on encrypted data

- How can one manipulate encrypted data?
- How can a computer run a program blindly?
- Celebrated research topic in cryptography
  - Identified in 1978
  - Yao's millionaires problem (1986)
- Secure two-party computation
  - Garbled circuits
    - Quite practical today for limited functions
  - Fully Homomorphic Encryption
    - Breakthrough result (Gentry 09) but very far from practical



Protection for cryptographic operations in VMs "Cryptography-as-a-Service" [BBINS13]

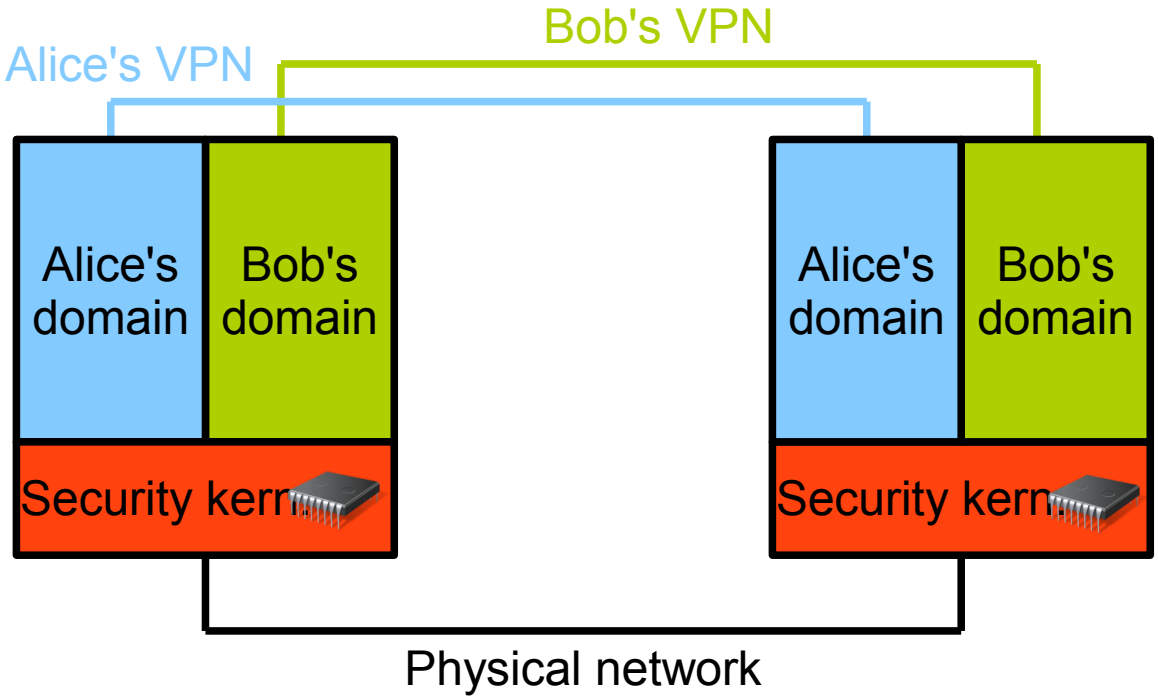
- Crypto VM protected by TPM and trusted VM builder
- Shields client-owned cryptographic keys and operations from mgmt VM



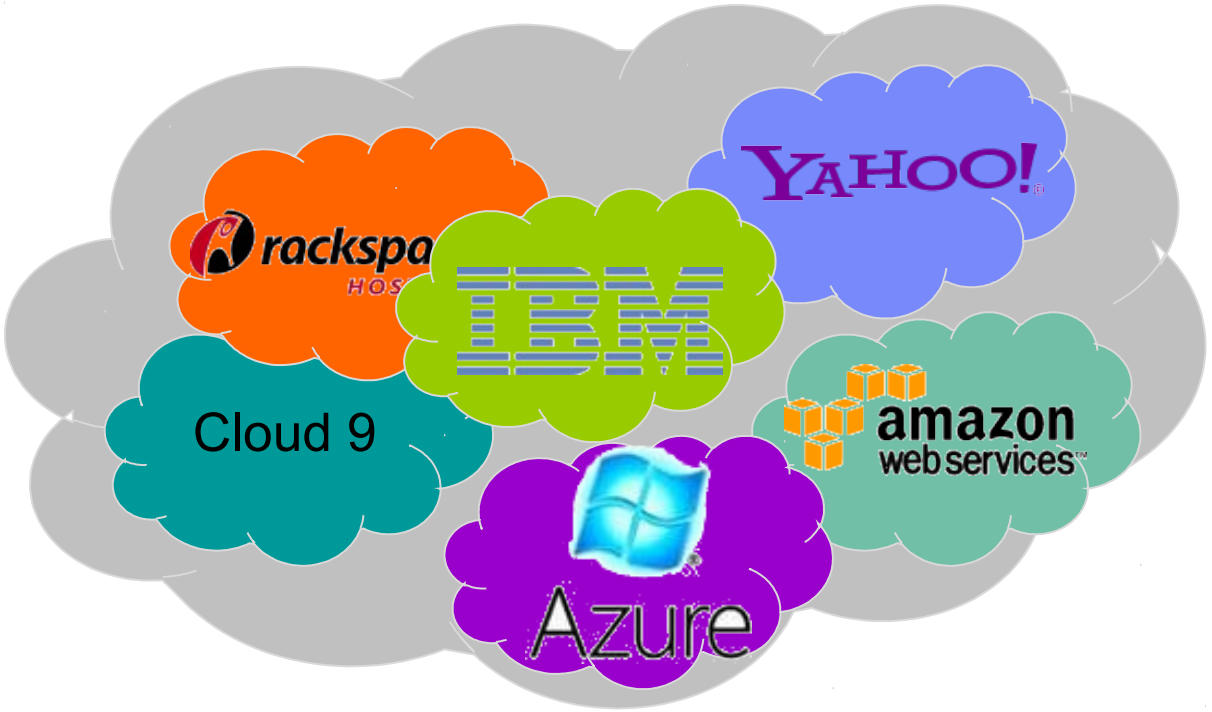
- TPM verifies hypervisor and Trusted builder VM
- Clients know sources of trusted components
- Client-owned cryptographic keys not exposed to cloud mgmt domain
- Examples
  - Encryption for virtual disk images or VMIs in cloud storage
  - Communication encryption (TLS, VPN ...)

Trusted virtual domains [GJPSvDC05]

- TPM-enhanced security kernel in hypervisor
  - Secure attestation protects interaction with remote hosts
- Domains are isloated
  - Encryption of all traffic between VMs inside domain
- Realized in TClouds' TrustedInfrastructure prototype



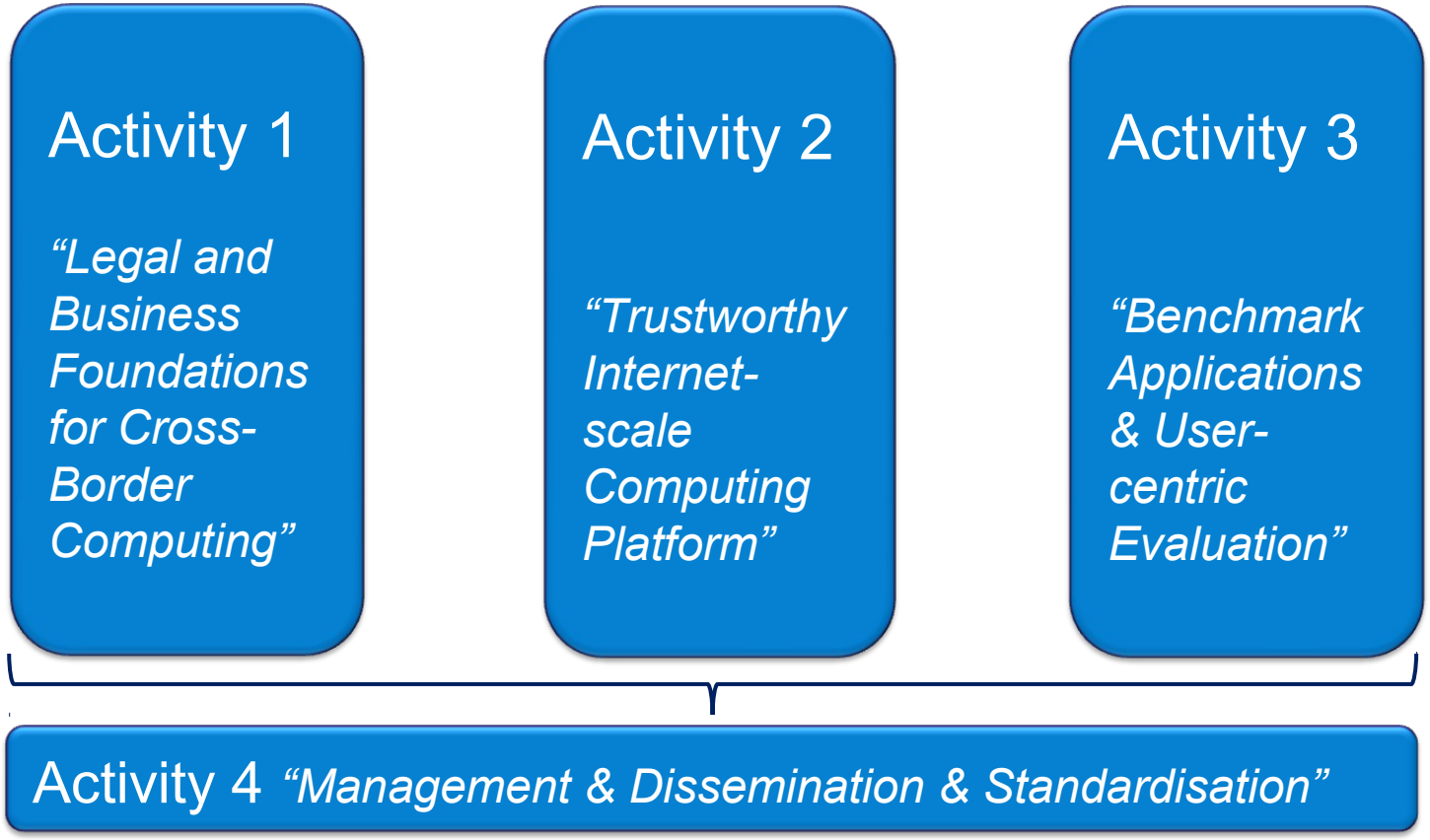
Higher resilience from a cloud-of-clouds



- Move cloud services to a cloud-of-clouds
- Replicate data and services over multiple providers
  - Exploit independence among providers
  - Deliver one integrated and resilient service using distributed protocols
- TClouds components DepSky, BFT-SMaRt, and CheapBFT

TClouds - Trustworthy Clouds

The TClouds EU/FP7 research project (2010-2013)



TClouds geographical overview

Consortium

The consortium currently consists of 14 partners from 7 different countries (greyed background identifies former members): reputable universities and recognised companies from six European Union member states (Austria, Netherlands, Germany, Portugal, Italy and the United Kingdom) plus Switzerland. All partners are experts in their field. This partnership of experienced professionals is anticipated to result in a successful project.

1 Technikon Forschungs- und Planungsgesellschaft mbH (Villach/Austria)

2 IBM Research GmbH (Zurich/Switzerland)

3 Philips Electronics Nederland B.V. (Amsterdam/Netherlands)

4 Sirrix Aktiengesellschaft (Homburg/Saar/Germany)

5 Technische Universität Darmstadt (Darmstadt/Germany)

6 Fundação da Faculdade de Ciências da Universidade de Lisboa (Lisbon/Portugal)

7 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Kiel/Germany)

8 The Chancellor, Master and Scholars of the University of Oxford (Oxford/United Kingdom)

9 Politecnico di Torino (Torino/Italy)

10 Friedrich-Alexander Universität Erlangen-Nürnberg (Erlangen/Germany)
Project Exit Date: March 30, 2012

11 Fondazione Centro San Raffaele del Monte Tabor (Milan/Italy)

12 Energias de Portugal (Lisbon/Portugal)

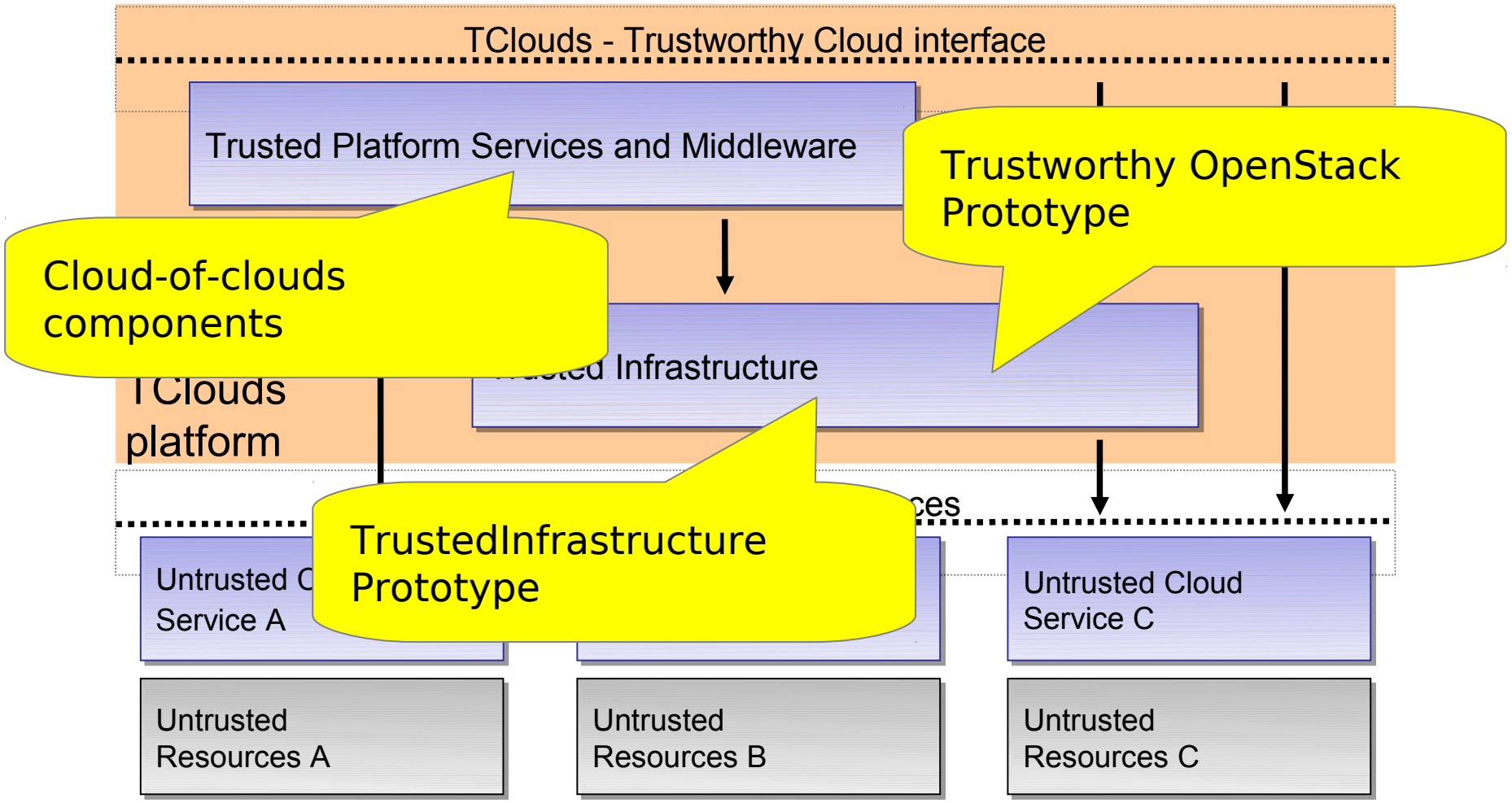
13 Universiteit Maastricht-Merit (Maastricht/Netherlands)
Project Exit Date: April 30, 2012

14 EFACEC Engenharia e Sistemas, S.A. (Maia/Portugal)

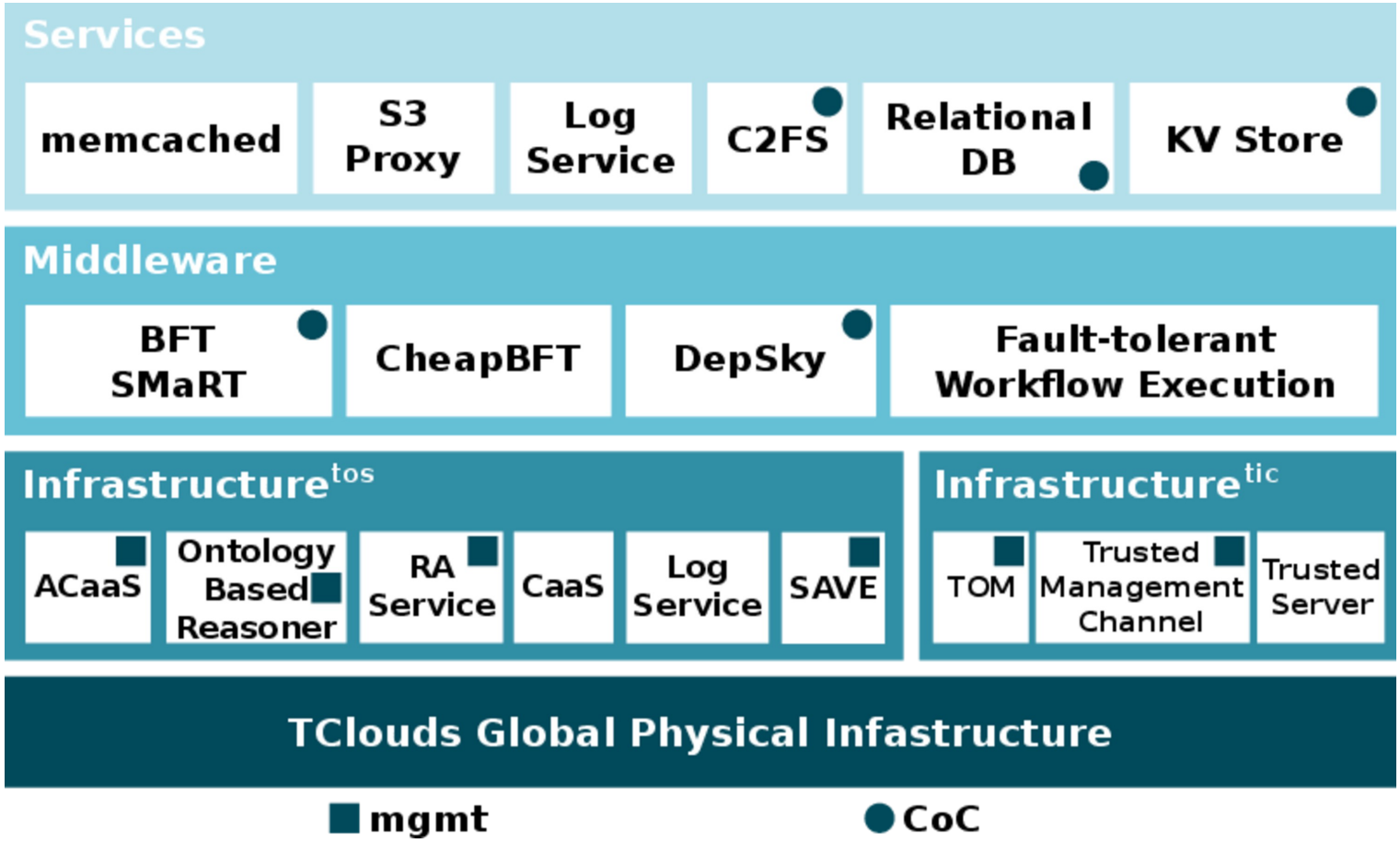
15 Technische Universität Braunschweig (Braunschweig/Germany),
Project Entry Date: April 1, 2012

16 INNOVA SpA (Rome/Italy),
Project Entry Date: June 1, 2012

TClouds architecture overview



The TClouds Trustworthy Cloud Platform



TClouds demonstration scenarios

- Home healthcare
  - Patient-centered home health-care functions
  - Supporting multiple actors, remote monitoring and diagnosis of patients
  - Support the lifecycle of a complete drug prescription via web-based cloud application
  - Partners Ospedale San Raffaele (IT) and Philips (NL)
- Smart lighting system
  - Control over public infrastructure in smart grid from a cloud environment
  - Collect SCADA data, manage and monitor municipality street lights
  - Partners Energias de Portugal (PT) and EFACEC Engenharia (PT)

Conclusion

- Cloud security has two goals
  - Protect the provider
  - Protect the clients

  These two goals are sometimes orthogonal, sometimes dependent

- TClouds integrates multiple security technologies
  - Trusted computing technology
    - Exploit hardware root-of-trust
  - Cryptography for encryption, integrity protection
    - Data-at-rest protection
  - Replication increases resilience of data and services
    - Deployment in a cloud-of-clouds

Thank you

- Christian Cachin
  - www.zurich.ibm.com/~cca/
- Security research
  - www.zurich.ibm.com/csc/security/
- IBM Research - Zurich
  - www.zurich.ibm.com
- Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure, EU FP7 No. 257243
  - www.tclouds-project.eu