Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

The Cloud Computing Challenge

Software and ICT Challenges in Legal Metrology

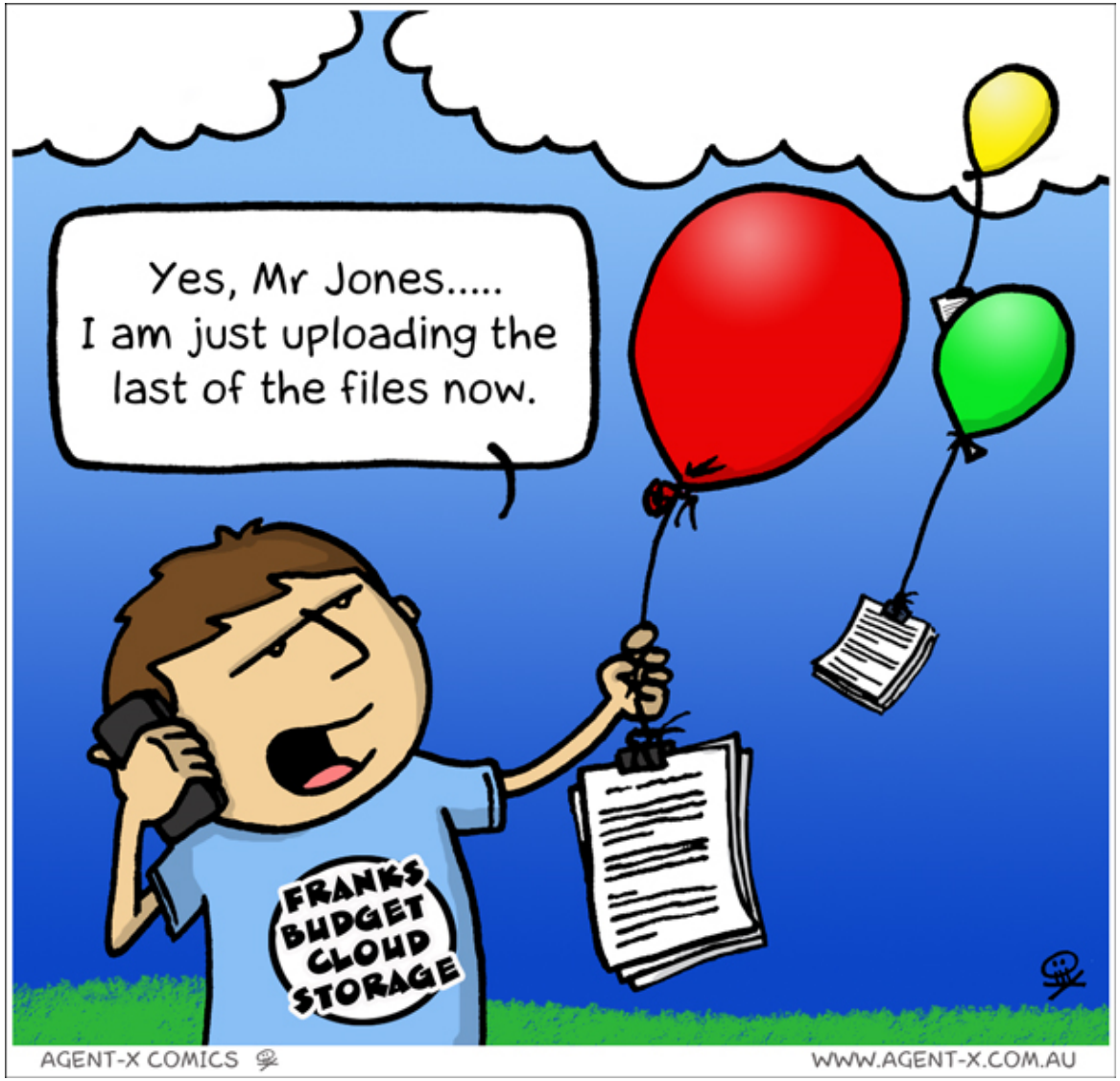
Alexander Oppermann, WG 8.52 Metrological ICT-Systems

Helmholtz Research School on Security Technologies

PTB Agenda

- Introduction and Motivation
- Cloud Architecture
- Platform Overview
- FHE Overview
- Summary

What is Cloud Computing?



General Concerns about Cloud Computing?

Is Cloud Computing disrupted by bad weather?

- In 2012, a survey states[1] that 51% Americans out 1000 think: **Y E S** .

Availability of Cloud Computing Services?

- Strong correlation between availability and power outages: 99,9974% or 13,43 minutes[1]
- Strong redundancy of Storage: 100% Availability[2]

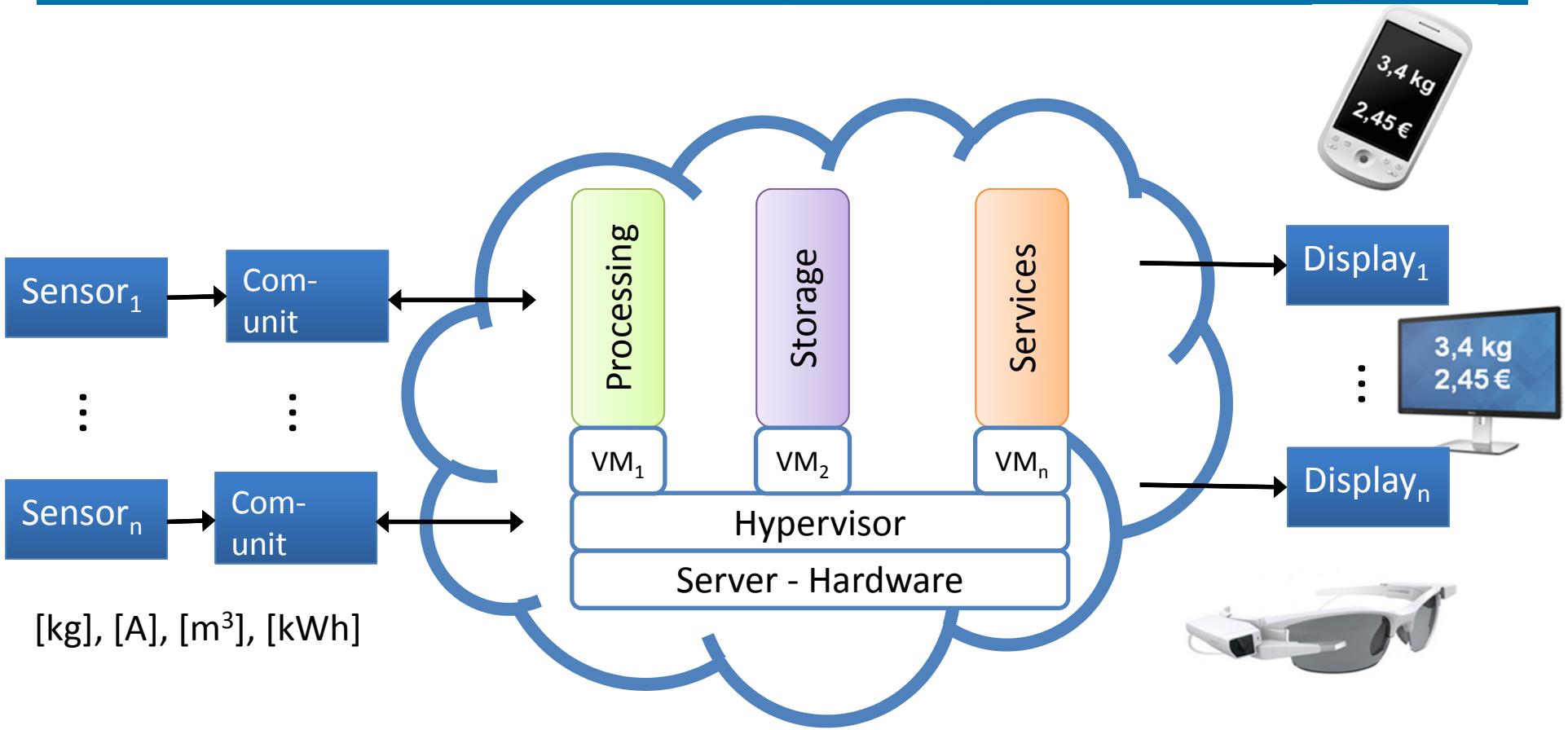
Is Cloud Computing secure?

- Higher security niveau through certification like ISO/IEC 27001
- Security updates with technical support

[1]Citrix Cloud Confusion Survey - http://s3.amazonaws.com/legacy.icmp/additional/citrix-cloud-survey-guide.pdf

[2]https://cloudharmony.com/status-in-eu

Cloud Computing in Legal Metrology

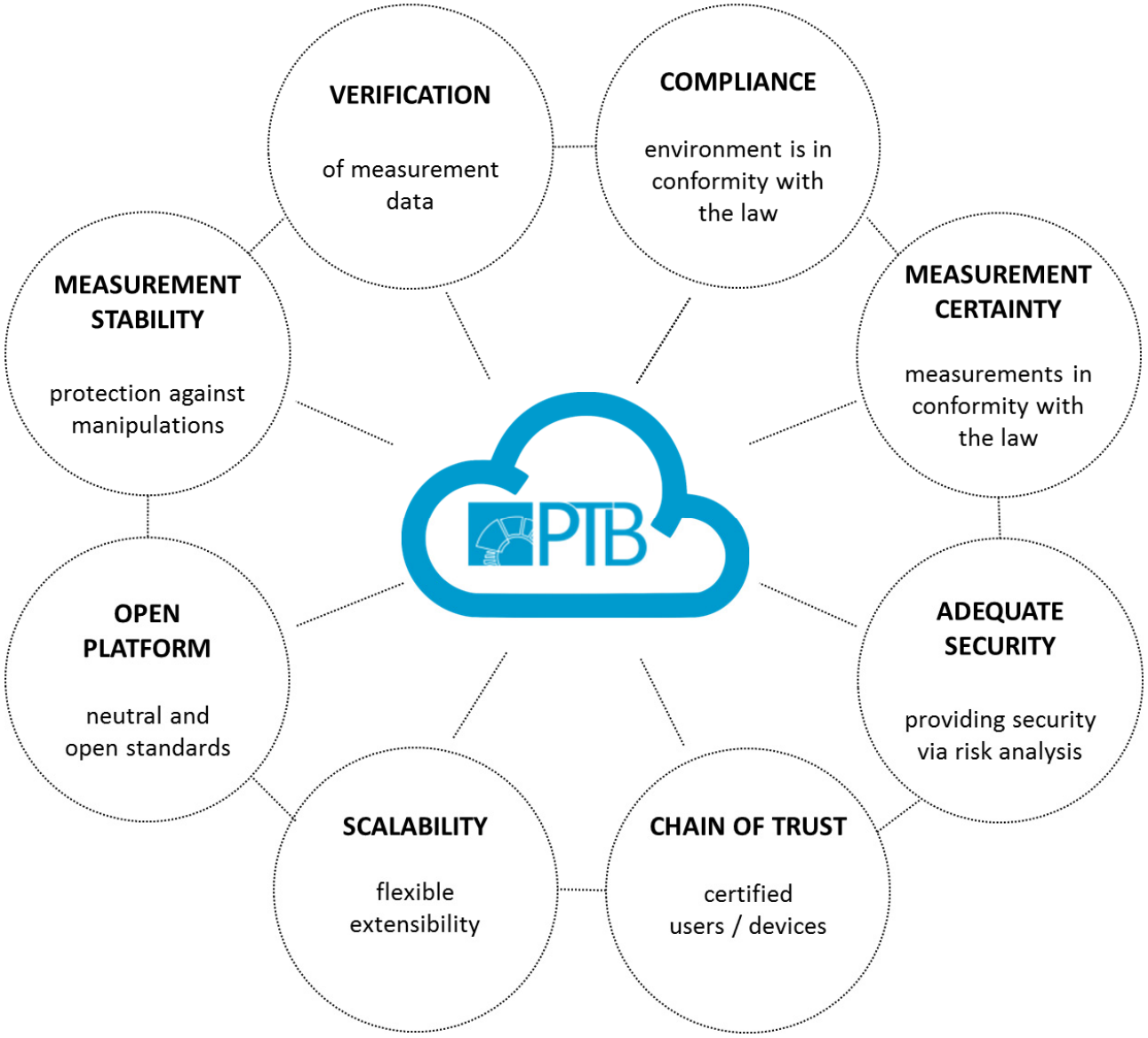


- **Transition** to distributed and virtualised components
- **Supply of** data based services

Agenda

- Introduction and Motivation
- Cloud Architecture
- Platform Overview
- FHE Overview
- Summary

Essential Requirements of a Cloud Architecture

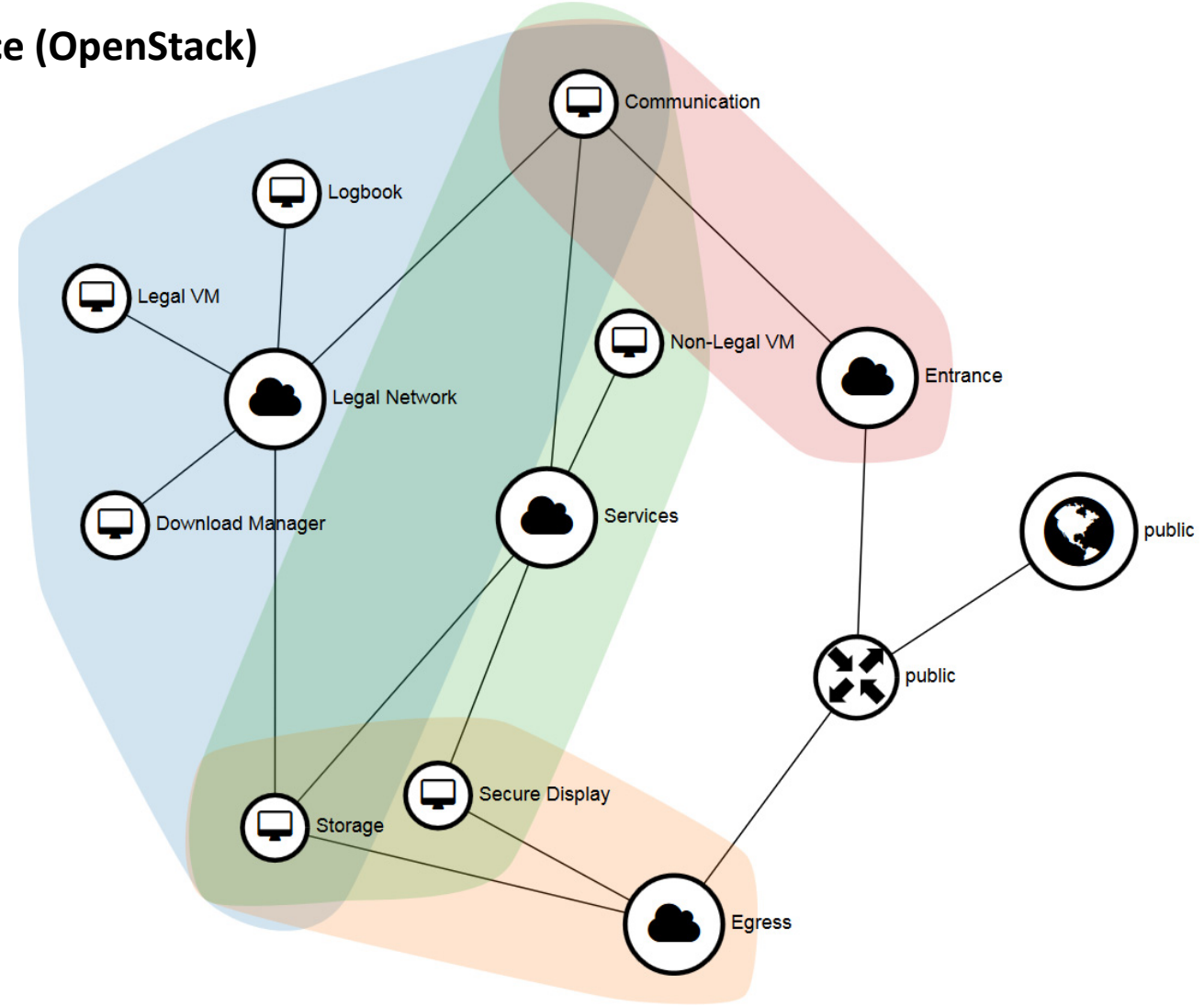


PTB Cloud-Architecture

Infrastructure as a Service (OpenStack)

Virtual Network

- 1 Virtual Router
- Virtual NIC
- 4 Subnetworks
- 7 Virtual Machines



openstack™
CLOUD SOFTWARE

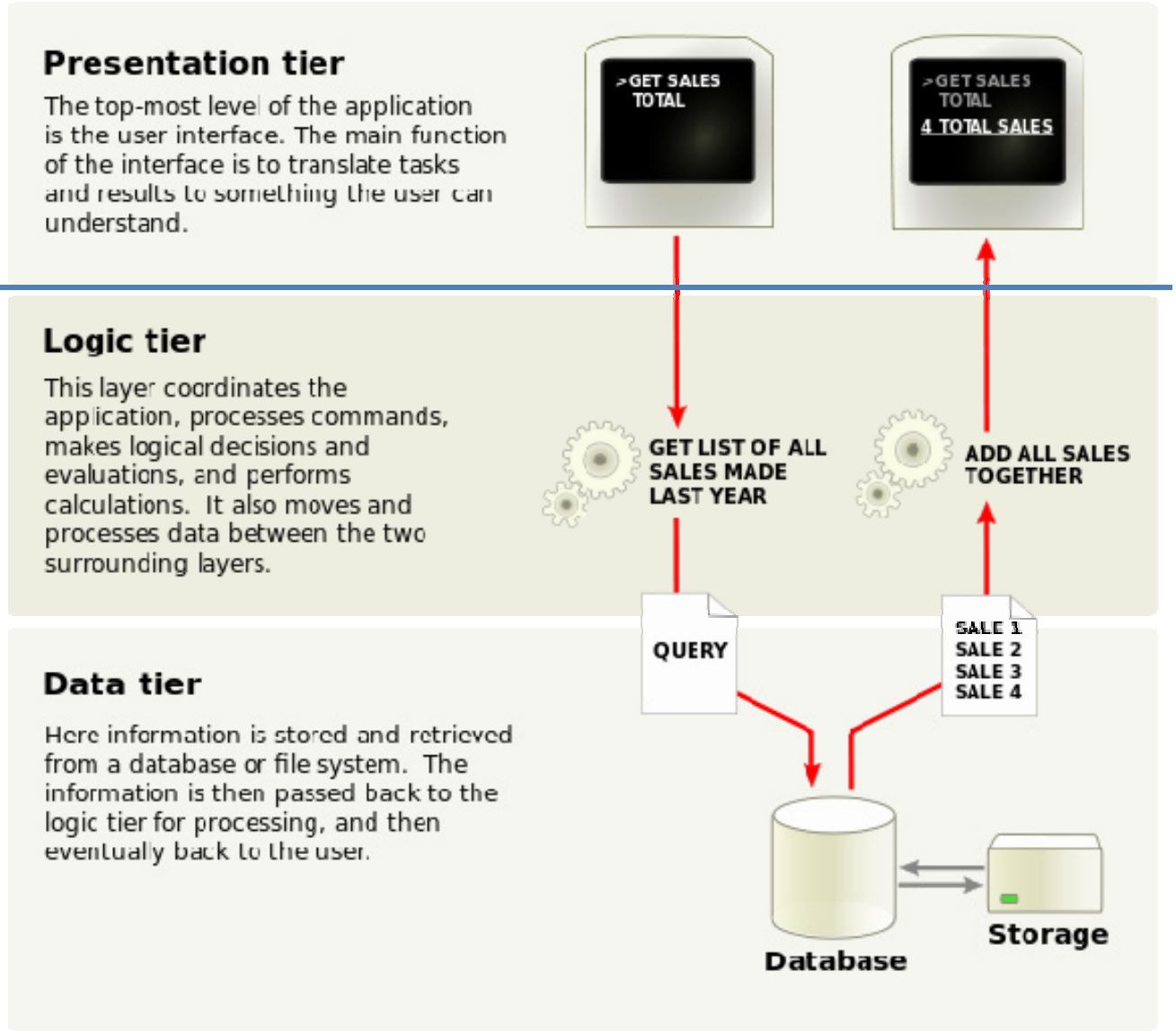
Multi Tier Architecture

Browser

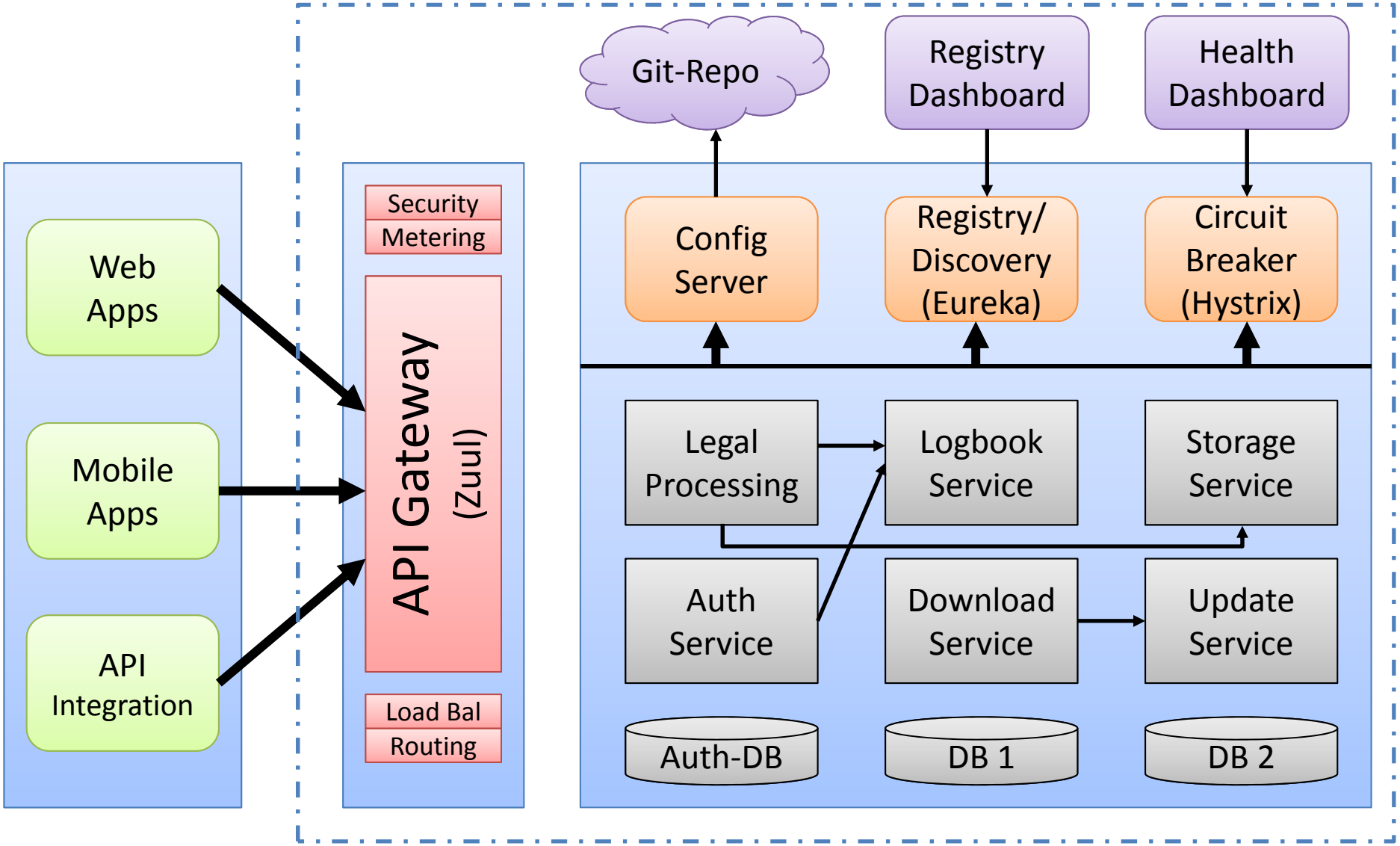
PaaS

Cloud

IaaS



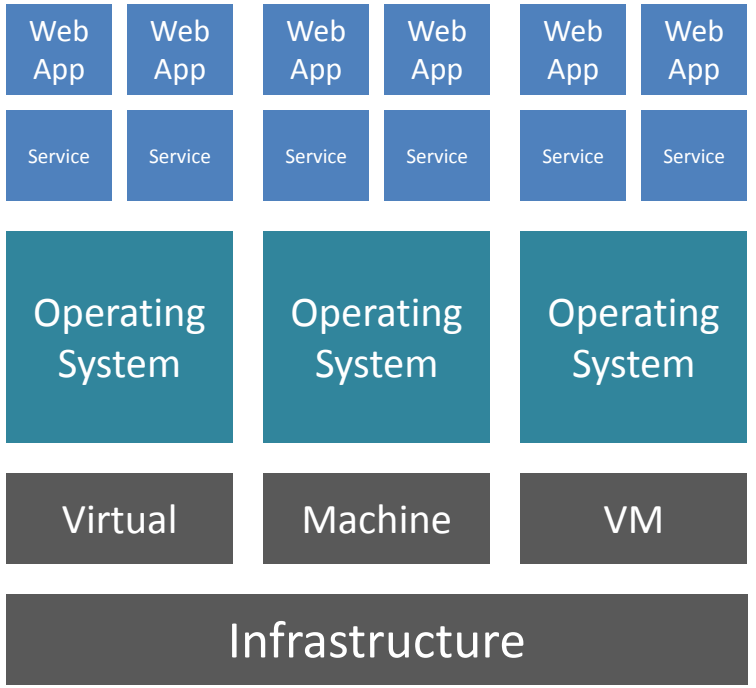
Platform Overview



What are Microservices?

A pattern to build distributed systems:

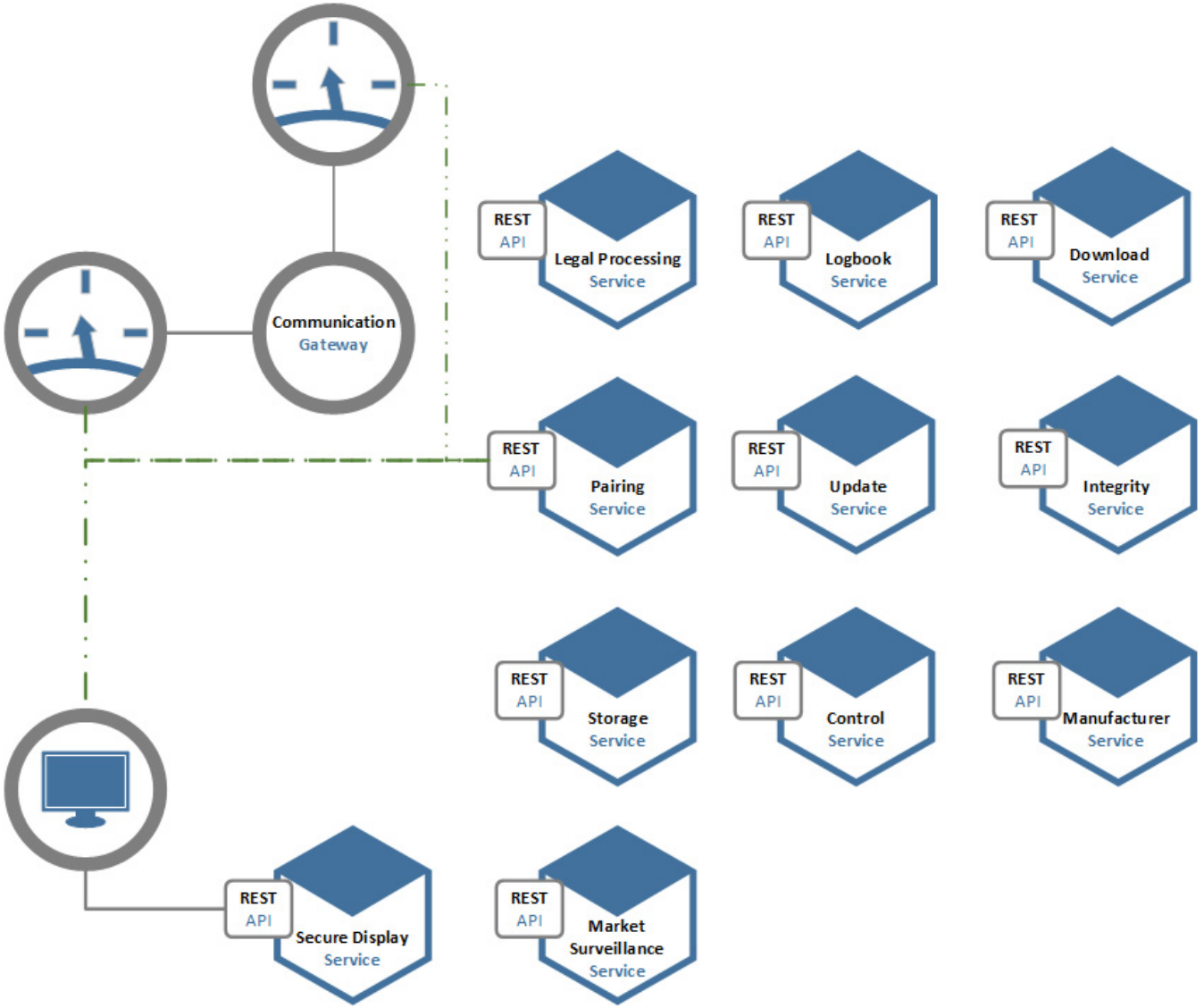
- A set of services, with separate processes, that have an API
- Can be developed independently of each other
- Can be indenpendently deployed of each other
- Each service is focused of one task



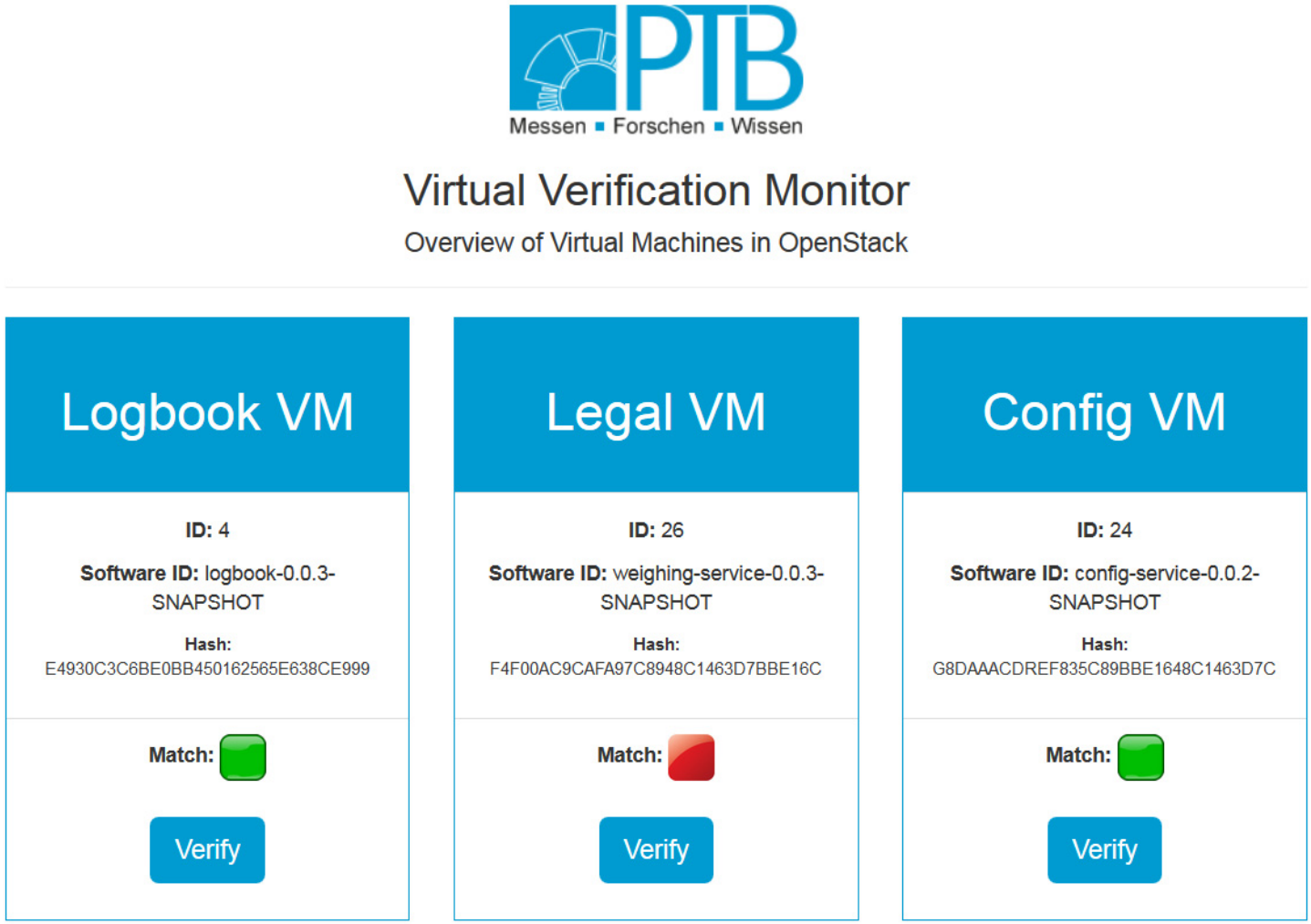
(Source: Mesosphere, 2017)

„Gather together things that change for the same reason, and separate those things that change for different reasons.“
- Robert Martin

Overview of Microservices



Verification Monitor

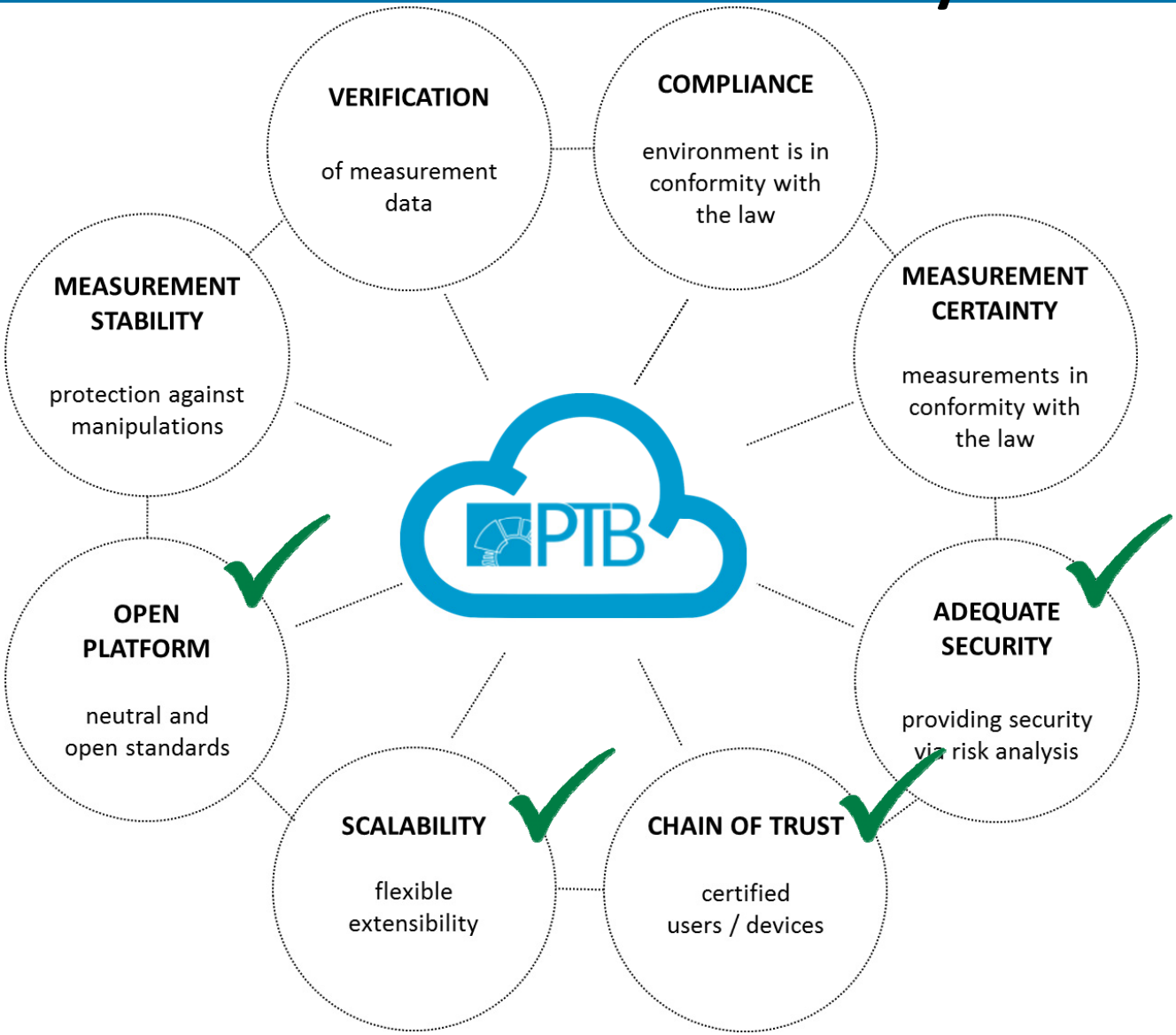


Intermediate summary of the cloud platform

Cloud-Computing :

- created a infrastructe with OpenStack
    - created a virtual network with subnetwork to ensure separation on a low level
- created a platform with Microservices
    - that enable a easy way to extend the prototype later on
    - a very scalable and flexible approach
    - services are very small and therefore easier to be veriefied
- Verification Tool to verifiy and monitor the state of legally relevant software

Intermediate Summary



Important Research Goals

Prevention of **data manipulation** by an insider [1]

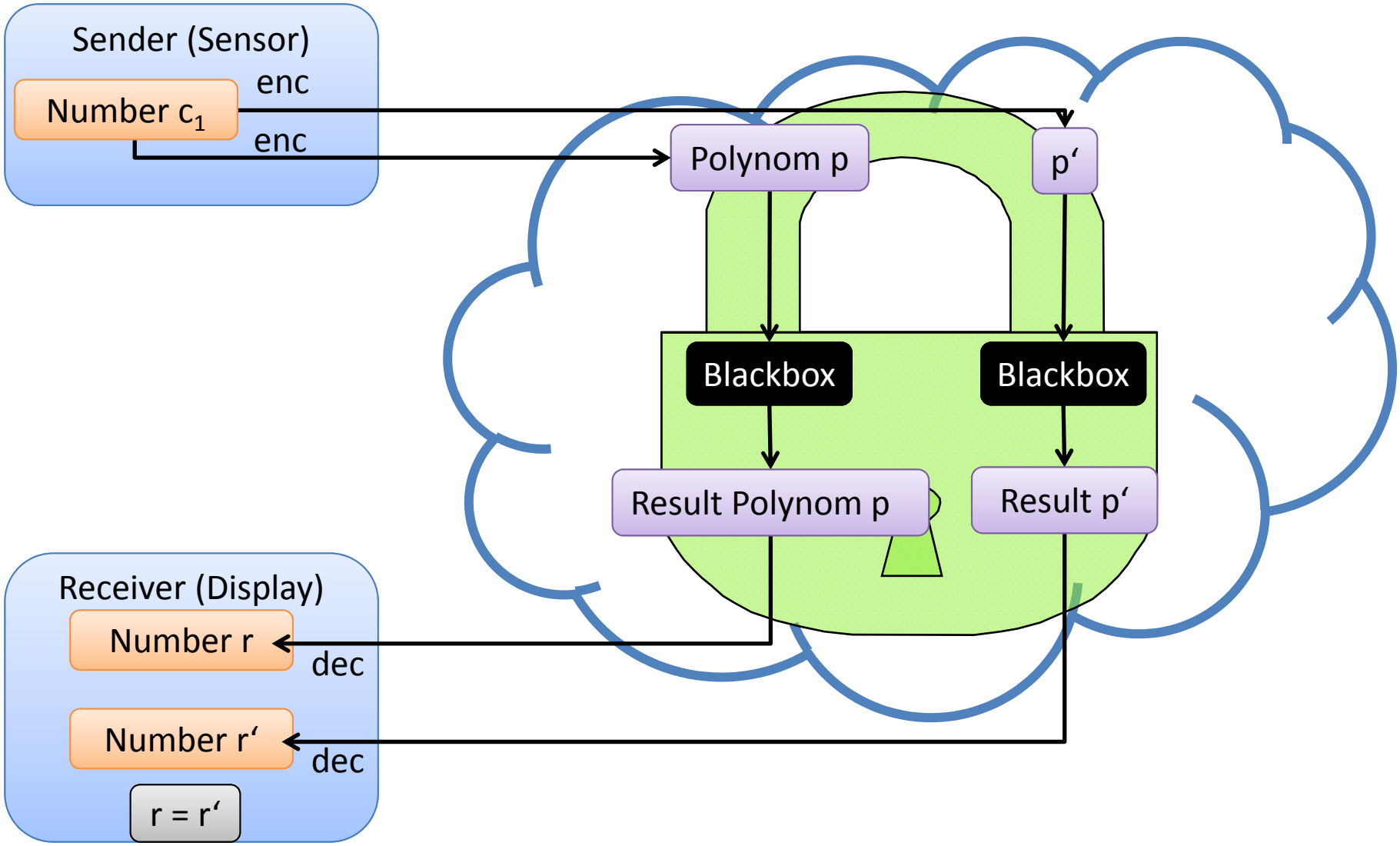
Prevention of **data espionage** by a corrupted VM [1]

Increase of **data security** in the Cloud [1]

Approach: Fully Homomorphic Encryption allows it to calculate data in the encrypted domain.

[1] Top Threats Cloud Computing: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Encrypted communication path



LSIM[1] - LibScarab extended for Integer arithmetics and Multithreading

- is based on the libScarab implementation of M.Brenner[2]
- has been extended to:
  - to calculate not only bitwise but whole **32bit** and **64 bit numbers**
  - **Division** and **subtraction** in order to fit the needs of tariff application in legal metrology.
  - **Zero comparisons**
  - **Decisions** to direct program flow
  - **Parallelization** and **multithreading**

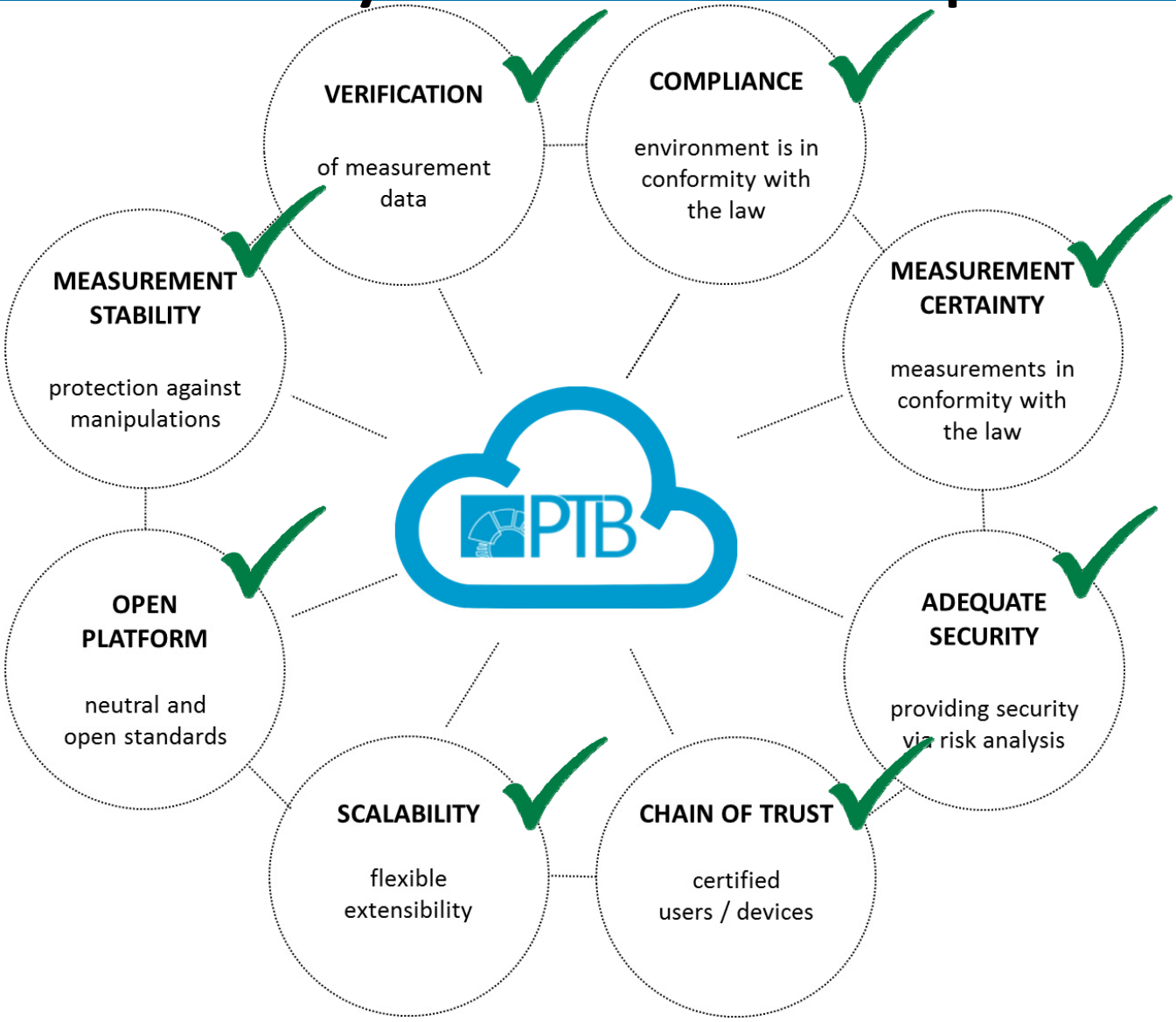
[1]Oppermann, A., Yurchenko, A., Esche, M. and Seifert, J.-P. „Secure Cloud Computing: Multithreaded Fully Homomorphic Encryption for Legal Metrology." *submitted to International Conference on Intelligent, Secure and Dependable Systems in Distributed and Cloud Environments, ISDDC 2017.*.

[2]Perl, Henning, Michael Brenner, and Matthew Smith. „An implementation of the fully homomorphic Smart-Vercauteren crypto-system." *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011.

Agenda

- Introduction and Motivation
- Cloud Architecture
- Platform Overview
- FHE Overview
- Summary

Summary of the cloud platform



Thank You for your Attention

Questions?

Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Abbestr. 2-12
10587 Berlin

Alexander Oppermann
Telefon: +49 30 3481-7483
E-Mail: Alexander Oppermann
www.ptb.de

Stand: 06/17