PRISMACLOUD

Privacy and Security Maintaining Services in the Cloud

Thomas Loruenser

AIT Austrian Institute of Technology GmbH

FOC2015

Vienna / 17.06.2015

# Challenges for Future ICT Systems

- Cloud computing will be at the heart of future ICT systems
- The cloud will pervade all aspects of our life
- New information security and privacy risks arise
- The cloud service provider necessarily needs to be trusted
- Cloud computing builds on a problematic trust model
- This inhibits many companies to make use of the cloud
- State of the art cryptography does not provide the agility to protect data in the cloud
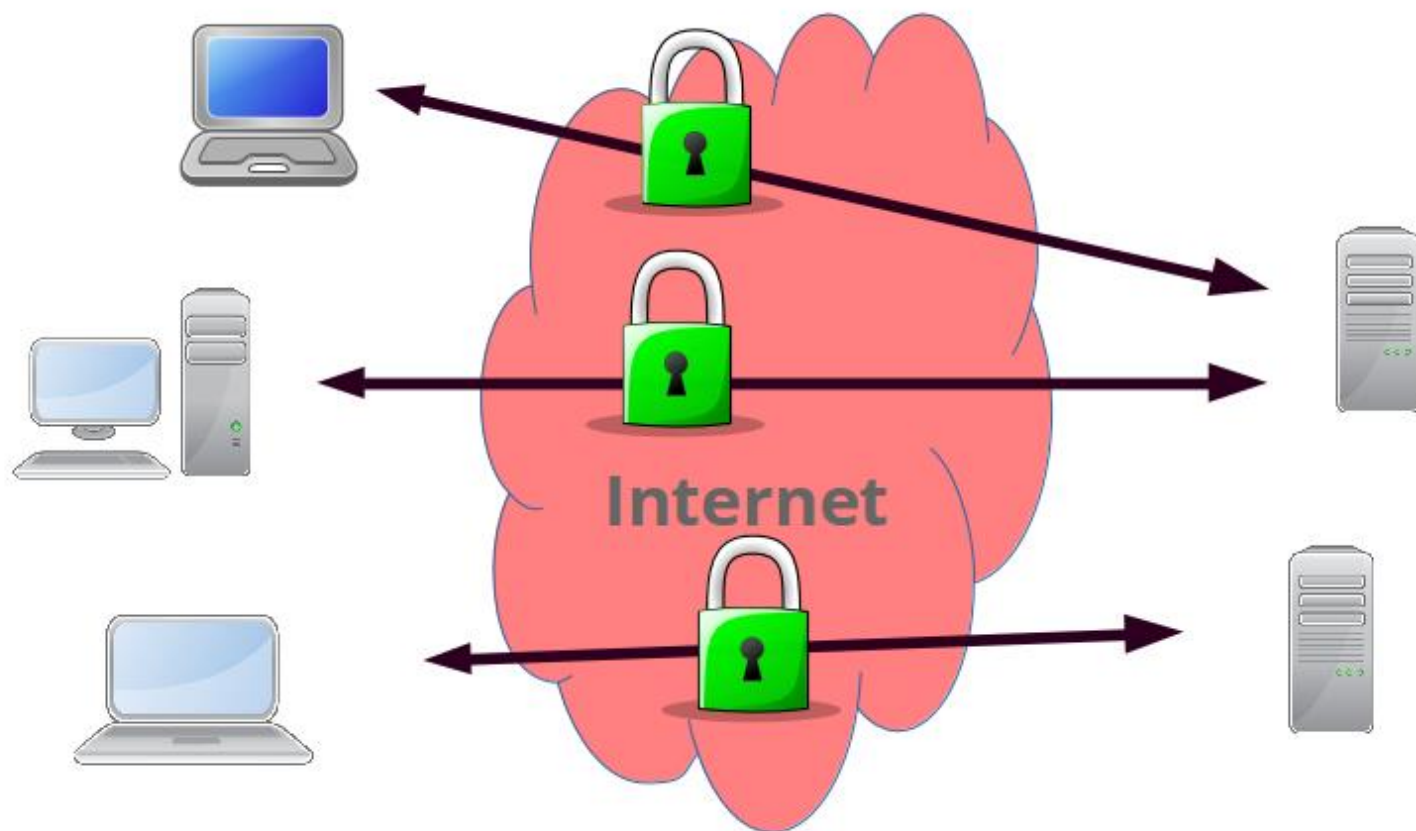- No end-to-end encryption/security available for cloud usage
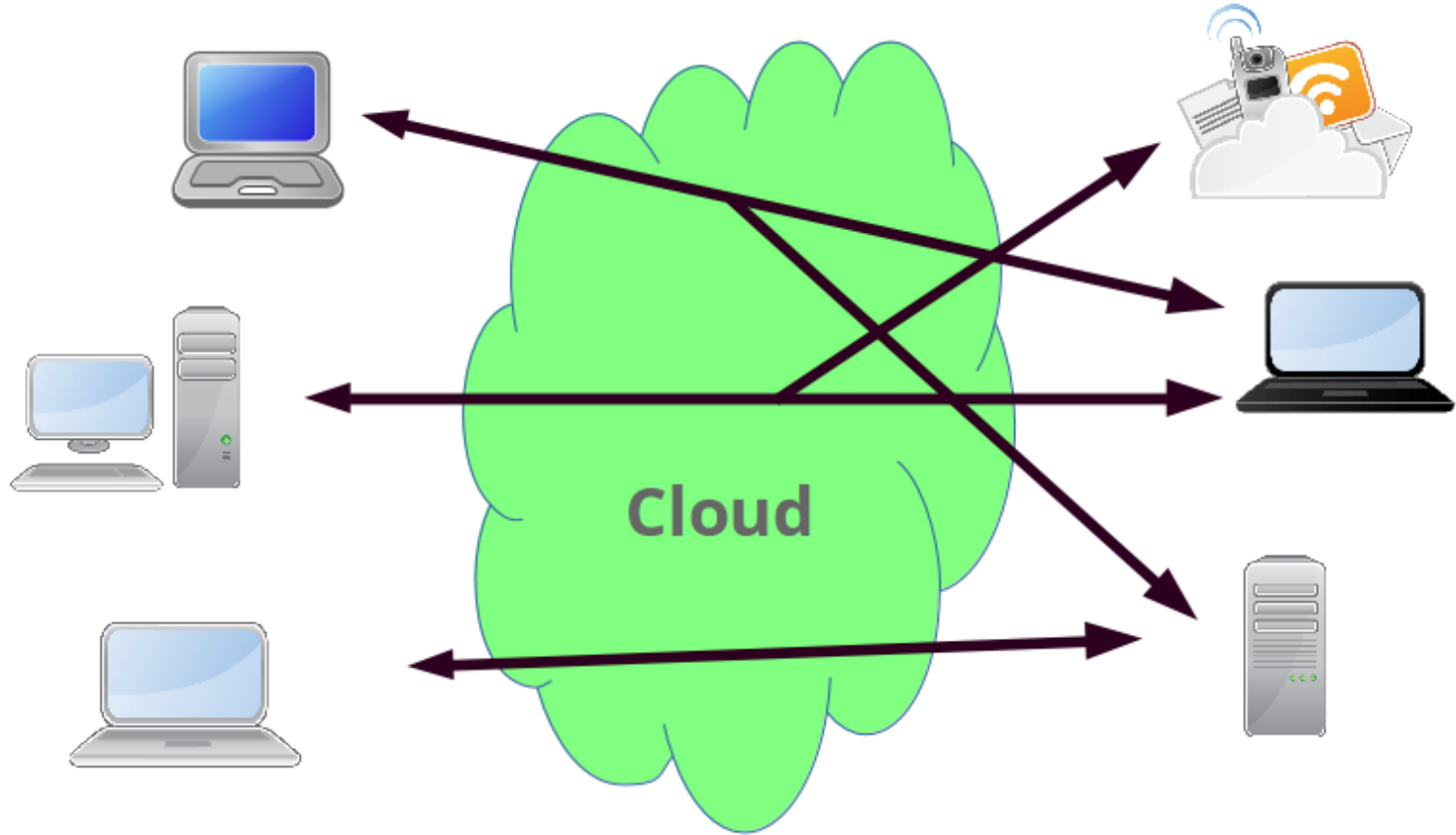
End-to-End Security
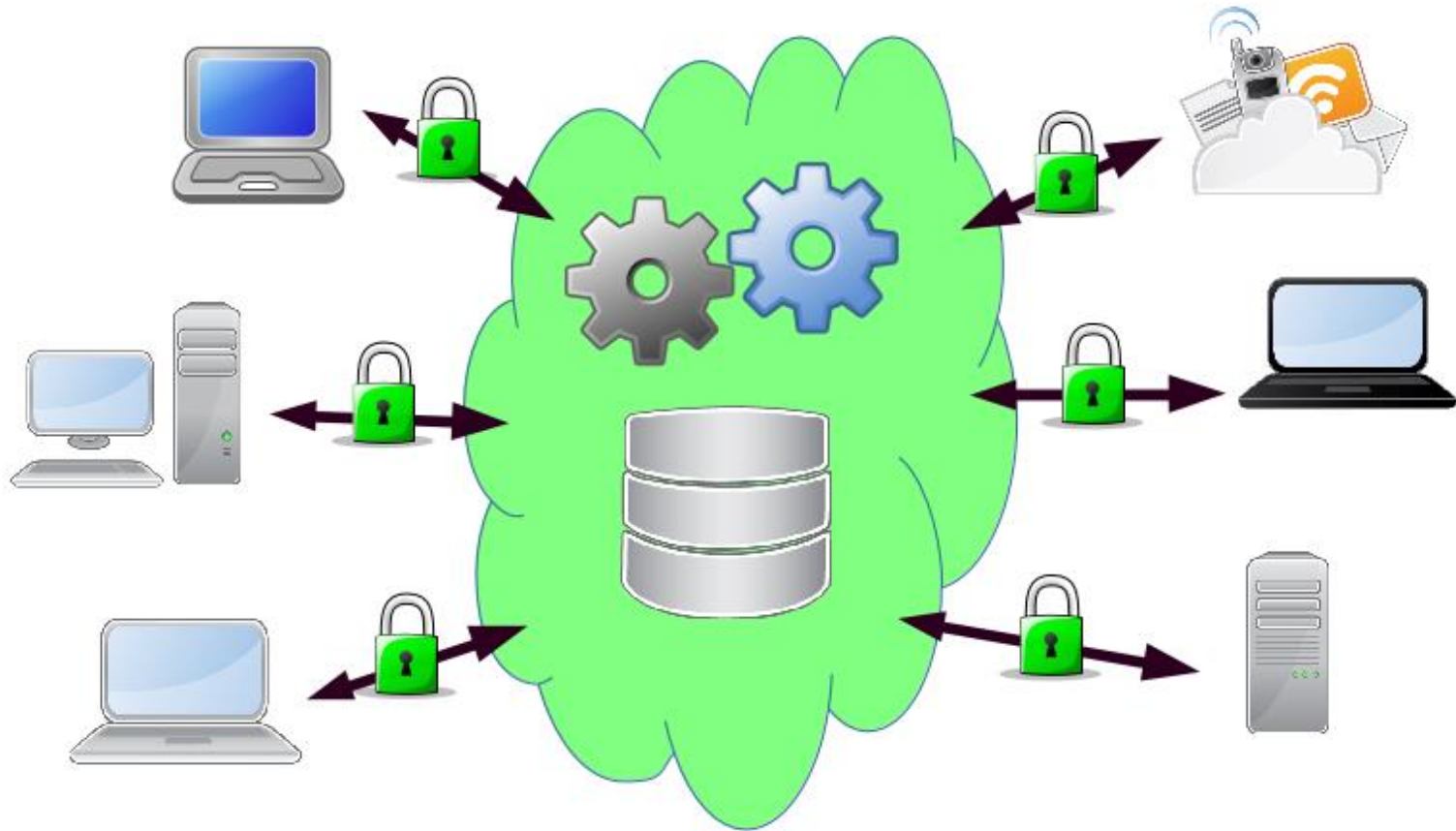

Internet
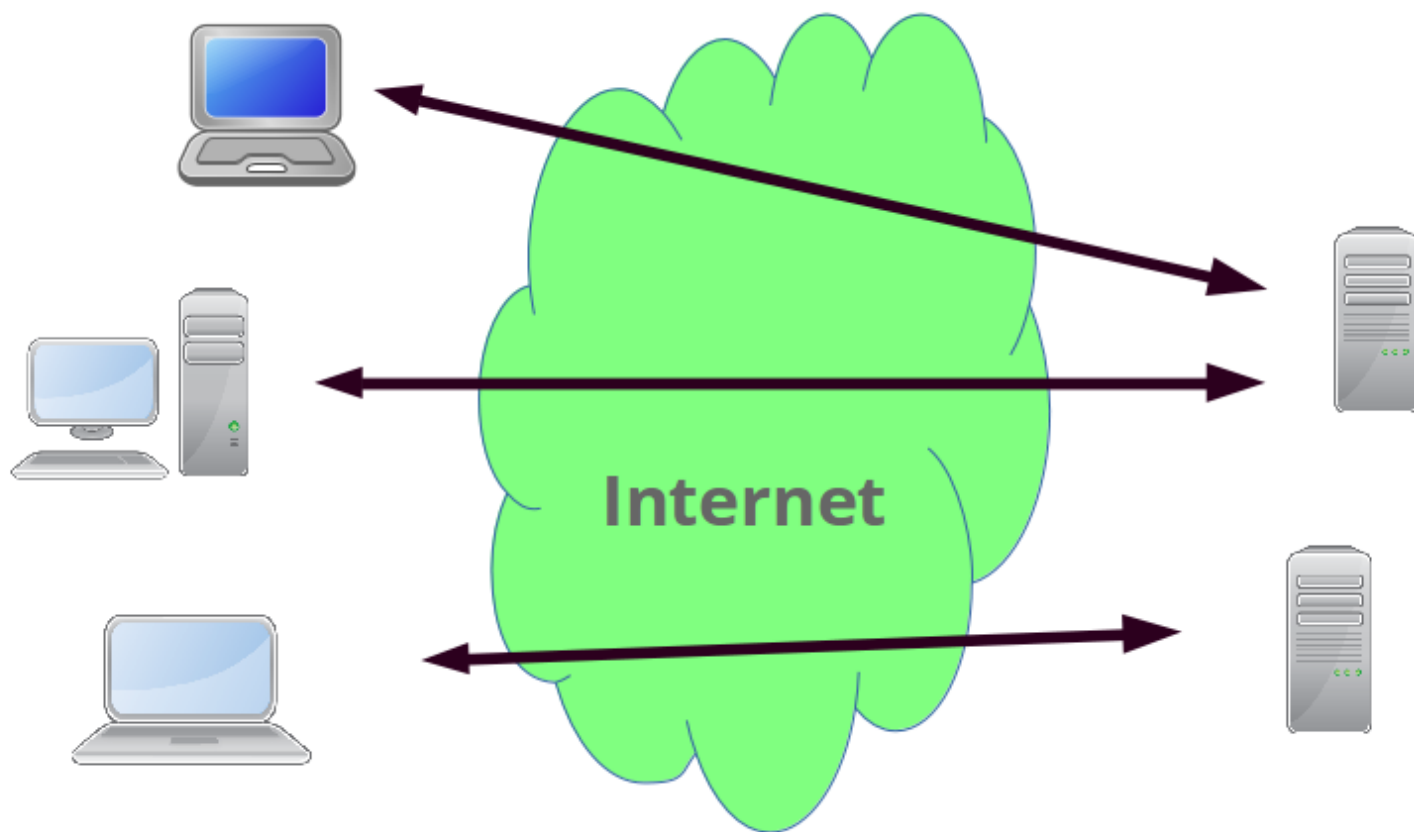
End-to-End Security (cont.)
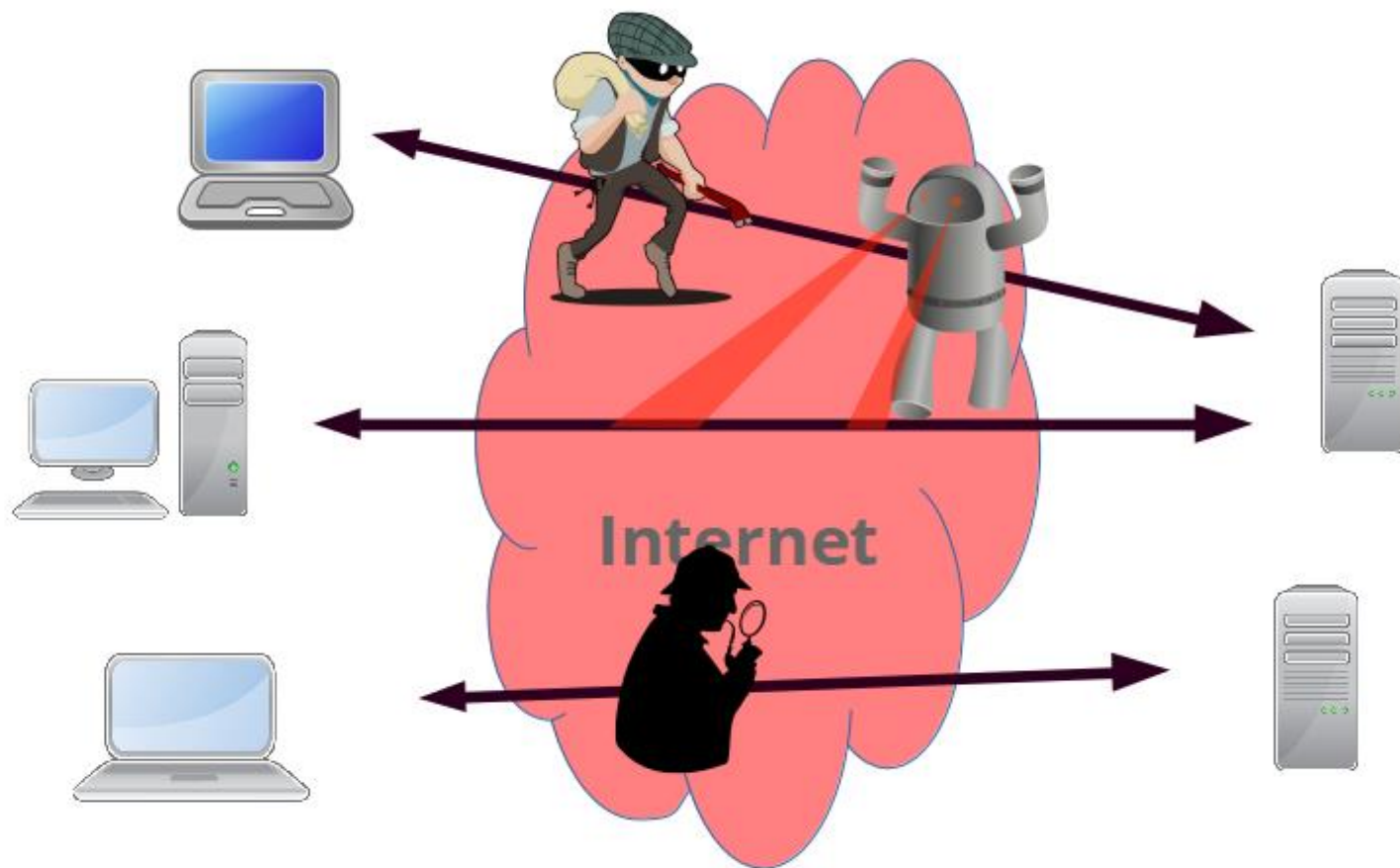
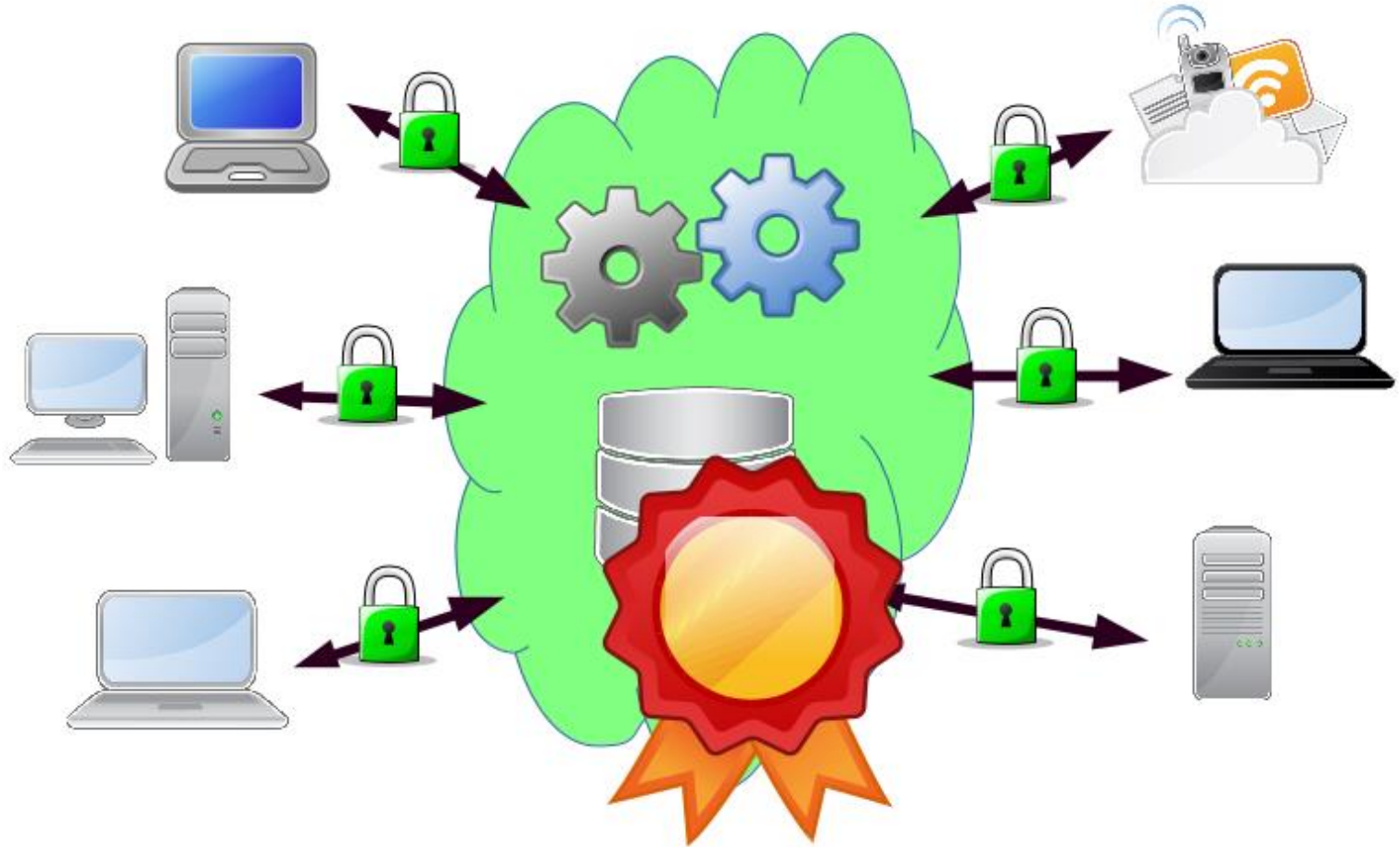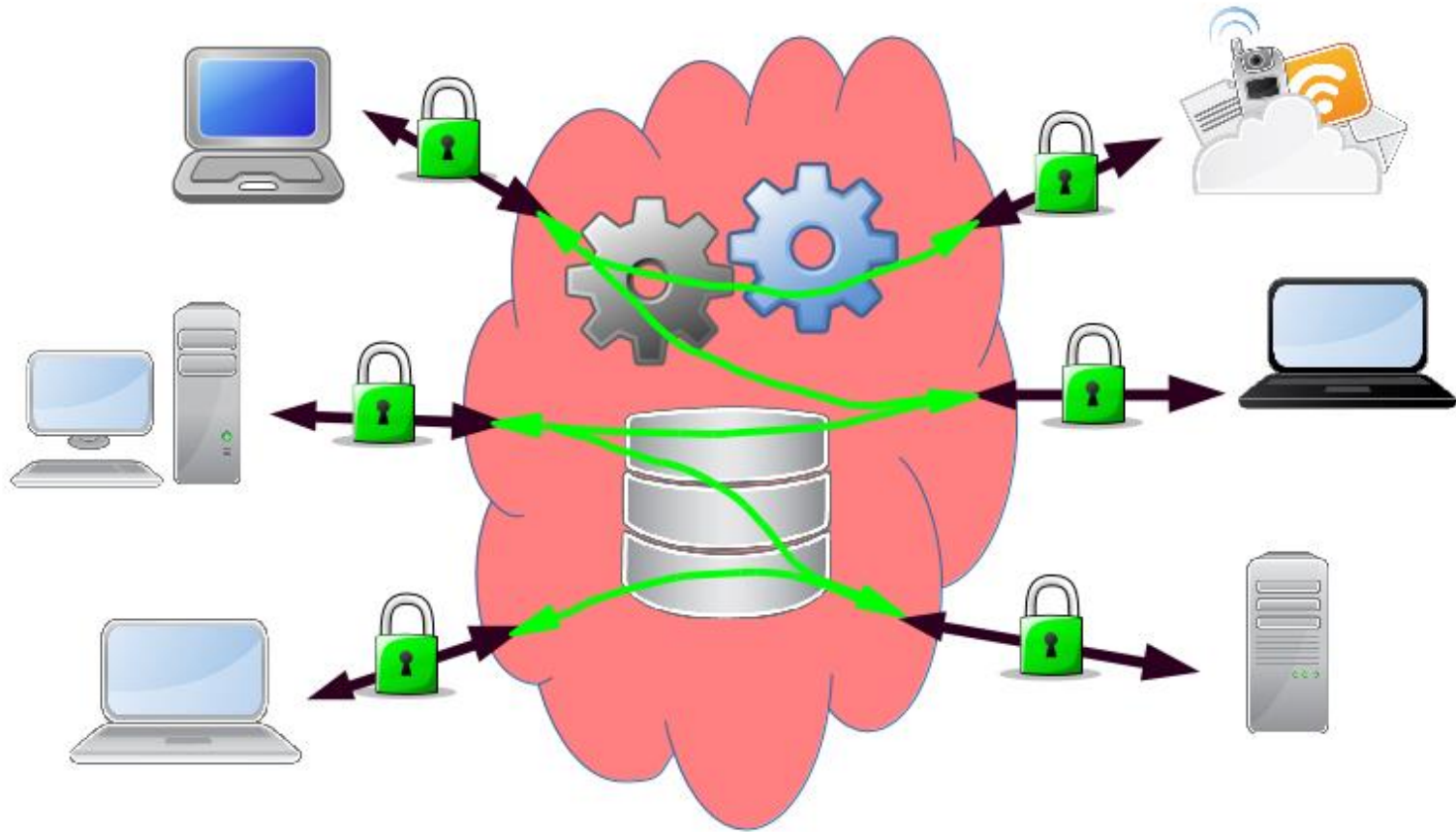# End-to-End Security (cont.)

Cloud Computing

Current Situation in the Cloud

Trustworthy Cloud Computing

Cloud Security 2.0

What about Privacy?

- Cloud computing is also an outsourcing model
- Centralized data collection and aggregation can lead to privacy issues
- If personal data is stored and processed data privacy regulations have to be fulfilled
- *"Safe Harbor"* before the EU Court of Justice (CJEU)

    http://www.europe-v-facebook.org

- Big Data wants as much data as possible – contradicts privacy requirements
- EU data protection rules are currently tightened
- ENISA recommends privacy and data protection by design

Project Metadata

Call: H2020-ICT-2014-1

Acronym: PRISMACLOUD

Type of Action: RIA

Number: 644962

Partners: 16

Duration: 42 months

Start Date: 2015-02-01

Estimated Project Cost: approx. 8.5M Euro

Requested EU Contribution: approx. 8M Euro

Coordinator: Austrian Institute of Technology GmbH

Project Objectives

Development of cryptographic tools to protect the security of data during its lifecycle in the cloud. Development of cryptographic primitives, protocols and schemes for application in cloud environments.

Development of cryptographic tools and methods to protect privacy of users. Development of cryptographic mechanisms to preserve privacy of user interacting with cloud services to only reveal necessary information.

Creation of enabling technologies for cloud infrastructures. Provision of software and hardware implementations of relevant cryptographic mechanisms and techniques to certify the structure of cloud topologies.

Development of a methodology for secure service composition. Development of a holistic security model methods for secure service composition. Examination of usability aspects as well as novel business models for secure services.

Experimental evaluation and validation of project results. Evaluation and validation of project results in different domains dealing with sensitive data. Provisioning of baselines and best practices for tool usage.

Innovations

Verifiability of data and infrastructure use

protect the results of computation (maintain authenticity, enable verifiability), enable methods for infrastructure attestation

User privacy enhancing technologies

data minimization technologies, data anonymization

Securing data at rest

secure distributed information sharing, long-term security, security for structured data

Secure and efficient implementations

high-quality software and hardware implementations of primitives with prototyping, security testing of developed components

**Methodology, tools and guidelines for fast adoption**

holistic security models and tools for secure service composition, business models and standardization

Technology Readiness Level

The **main idea and ambition** of PRISMACLOUD is to **enable end-to-end security for cloud users** and provide tools **to protect their privacy** with the best technical means possible - **by cryptography**.

- Verifiability of data and infrastructure use

- User privacy and anonymization

- Securing data at rest

- Secure and efficient implementations

- Methodology, tools and guidelines for fast adoption
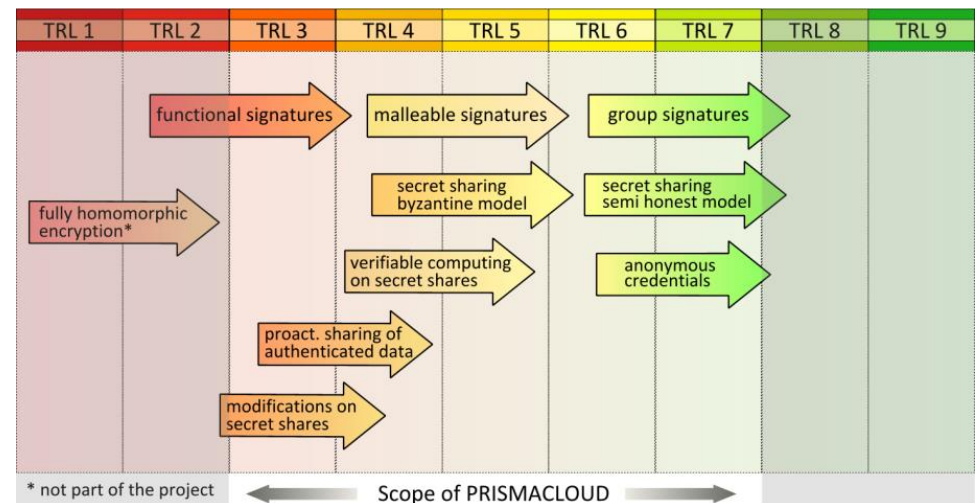
# Demonstration

Smart City Pilot:

- ICT implementation of the European Disable Badge (http://www.simon-project.eu)

- Surveillance CCTV cameras for law enforcement units (http://http://www.paris-project.org)
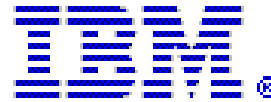
E-Government Pilot:

- Advance electronic identity system

- Digital archiving

- Security for open data

E-Health Pilot:

- Enable shift of parts of existing healthcare IT systems to the cloud (Healthcare TPaaS, http://www.tclouds-project.eu)
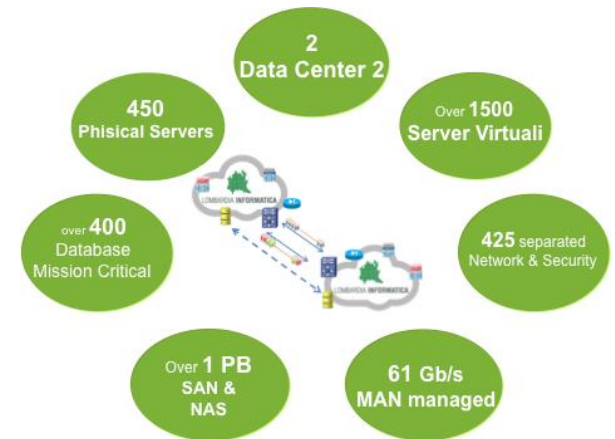
PRISMACLOUD Partners

Contact

Website:

https://www.prismacloud.eu

Coordinator Contact:

Thomas Loruenser

thomas.loruenser@ait.ac.at

PRISMACLOUD is also on:

LinkedIn: https://in.linkedin.com/in/prismacloud

Twitter: https://twitter.com/prismacloud (@prismacloud)