PRISMACLOUD

Privacy and Security Maintaining Services in the Cloud

Thomas Loruenser

CSP2015
Brussels / 29.04.2015

Challenges for future ICT

- Cloud computing will be at the heart of future ICT systems
- The cloud will pervade all aspects of our life (no opt-out)
- New information security and privacy risks arise
- The cloud service provider necessarily needs to be trusted
- Cloud computing build 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

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

Security Objectives

- **Develop next-generation cryptographically secured services for the cloud.**
- **Develop novel cryptographic tools, mechanisms, and techniques**
- ready to be used in a cloud environment, in order to:
  - **protect the security of data over its lifecycle,**
  - **protect the privacy of the users,**
  - **securely compose services,**
  - **base the security and privacy on 'by design' principles, and**
  - **to provide efficient implementations both at software and hardware level.**
- **Assess and test the results obtained within PRISMACLOUD.**
  - Three realistic use case scenarios in the areas of **e-government, healthcare, and smart city services** will be fully developed and implemented as technology demonstrators.
- A thorough analysis of the **security of the final systems**, their **usability**, as well as **legal and information governance aspects** of the new services will be carried out to ensure optimal dissemination of the project results.

Prj. Objectives / Results

Approach

Advance cryptography to support dynamicity and agility of cloud computing

- *Provide means to protect the results of computations*
  - *Maintain authenticity (functional / malleable signatures)*
  - *Enable verifiability (verifiable computation)*
- *Protect privacy of users*
  - *Data minimization (anonymous credentials and group signatures)*
  - *Data anonymization (k-anonymity)*
- *Protect data at rest*
  - *Secret sharing based storage solutions (secure information sharing)*
  - *Long-term security for data (proactive secret sharing on signed data)*
  - *Order and format preserving cryptography*
- *Infrastructure attestation (direct anonymous attestation)*

Approach (cont.)

Make it available, usable and economically relevant

- Efficient and secure implementations of cryptographic primitives and protocols in software and hardware
- Hardware based trust anchors for leaf connectivity
- Holistic security models and tools for secure service composition
- Standardization efforts (collaboration welcome)
- New business models for privacy preserving services (no provider access)

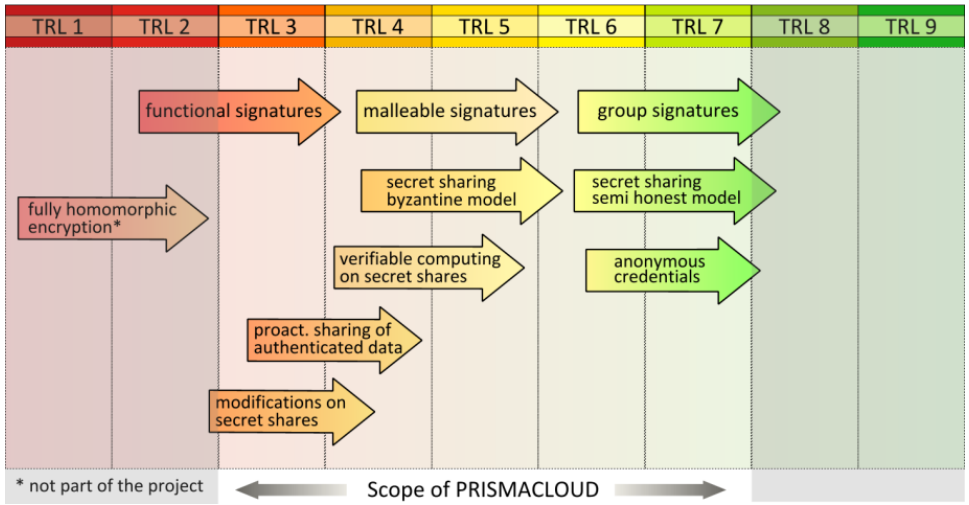
Evaluation of capabilities in real-life scenarios

- Evaluate and demonstrate methodology and tools in tree pilots
- Pilots are from areas with high security demands
- PRISMACLOUD tools will be integrated in various configurations to enhance security and privacy

Innovation

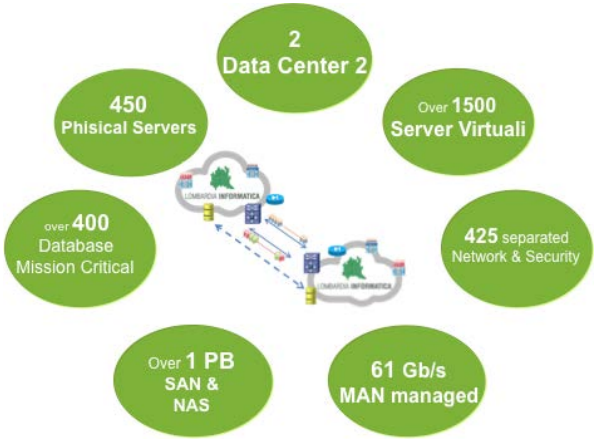
The **main idea and ambition** of PRISMACLOUD is to **enable end-to-end security for cloud users** and provide tools **to protect their privacy** with the best technical means possible - **by cryptography**.

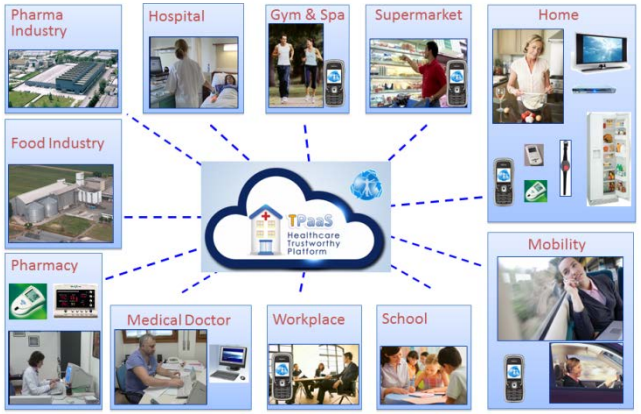
- Verifiability of data and infrastructure use
- User privacy and anonymization
- Securing data at rest
- Secure and efficient implementations
- Methodology, tools and guidelines for fast adoption



Demonstration

- Smart City Pilot:
  - ICT implementation of the European Disable Badge (http://www.simon-project.eu)
  - Surveillance CCTV cameras for law enforcement units
- 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

AIT Austrian Institute of Technology – Tomorrow Today

Karlstads Universitet

CEA Leti

etra I+D

Newcastle University

Atos

FCSR Fondazione Centro San Raffaele

IBM

Unil – UNIL | Université de Lausanne

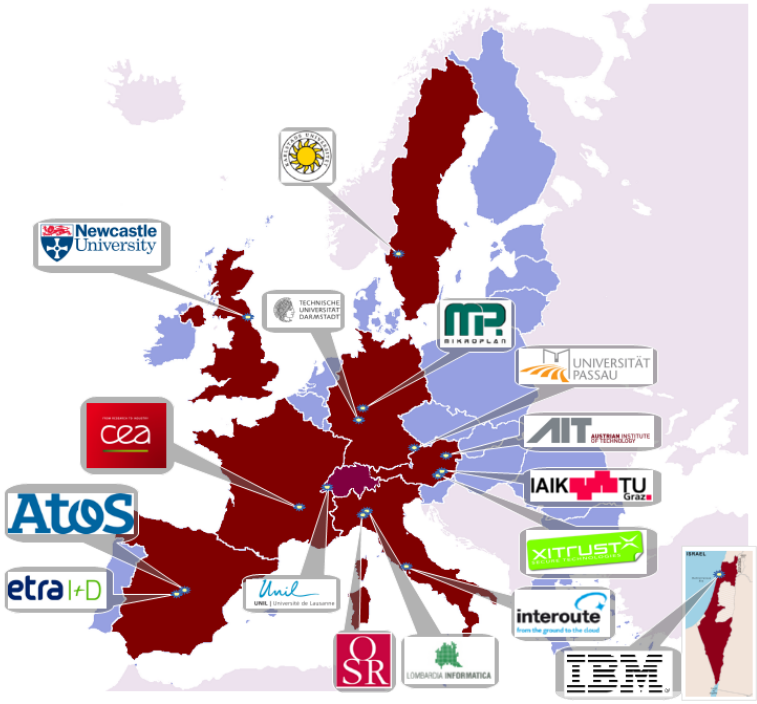
interoute – from the ground to the cloud

Lombardia Informatica

MP Mikroplan

IAIK TU Graz

Universität Passau



Technische Universität Darmstadt

XITRUST Secure Technologies

Contact

Website:

http://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)