prisma cloud

Selected Cloud Security Patterns For Improving End User Security and Privacy in Public Clouds

Annual Privacy Forum 2016, Frankfurt/Main, 7. September 2016

Thomas Länger (A) thomas.laenger@unil.ch
Henrich C. Pöhls (B) hp@sec.uni-passau.de
Solange Ghernaouti (A) sgh@unil.ch

(A) Université de Lausanne; (B) Universität Passau

Overview of the Talk

Horizon 2020 Project PRISMACLOUD:

- Relation to current topical "cloud landscape"
- Project goals and
- Plans and strategies to reach them

Design Patterns and Cloud Security Patterns:

- What they are
- How and for what we use patterns in the project
- Specific patterns corresponding to PRISMACLOUD functionalities

prisma cloud

Project PRISMACLOUD

is part of HORIZON 2020 WORK PROGRAMME 2014–2015:

- Information and Communication Technologies Calls
- ICT 32 – 2014: Cybersecurity, Trustworthy ICT;
- Program Scope:
  - Security-by-design for end-to-end security
  - Cryptography
- Expected impact
  - new design and implementation paradigms
  - at marginal additional cost
  - provide built-in privacy and security
  - increase user trust and privacy protection;
  - empower user control (and detection)
  - provide more resilience for critical infrastructures

prisma cloud

Motivation / Intention

Cryptography is not widely used in current cloud offerings

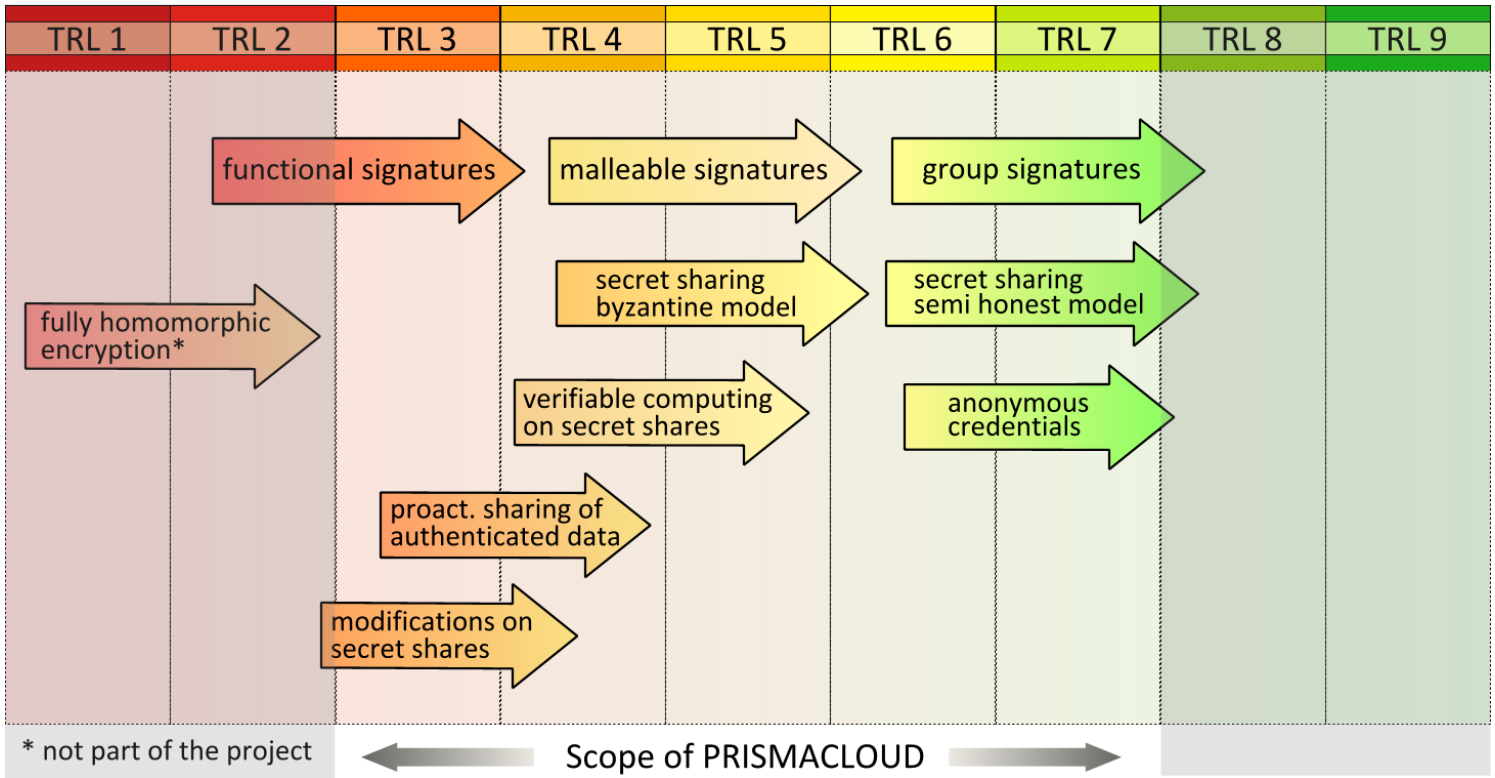
Use cryptography to address and mitigate several of the most common security threats and privacy threats in current cloud offerings

Use a security by design/privacy by design approach and build the cryptography into the heart of the services from the start

prisma cloud

Methodology

- **Survey existing cryptographic primitives** and protocols that can be applied in a cloud context—according to their Technology Readiness Level (TRL)



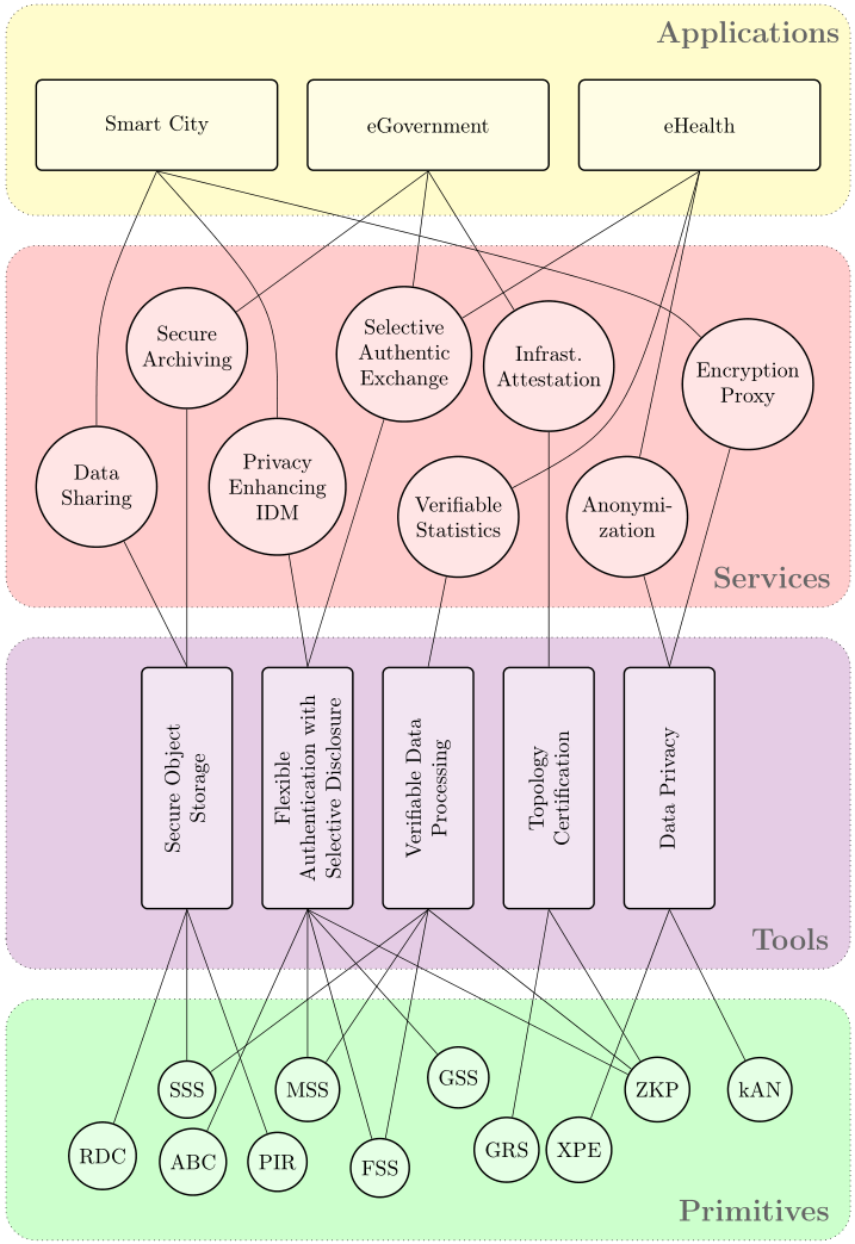
prisma cloud

Methodology

- **Select primitives** which can probably be advanced to **TRL7** (i.e. “system prototype demo in operational environment”) during timeframe of the project;
- Provide an implementation, as a **“kit of configurable tools”**, completely **encapsulating the cryptographic functions**;
- Provide a reference implementations for **sample cloud services** using the tools;
- **Validate** (services and tools) **in three real-world applications** in the fields of Smart Cities, e-Health, and e-Government.

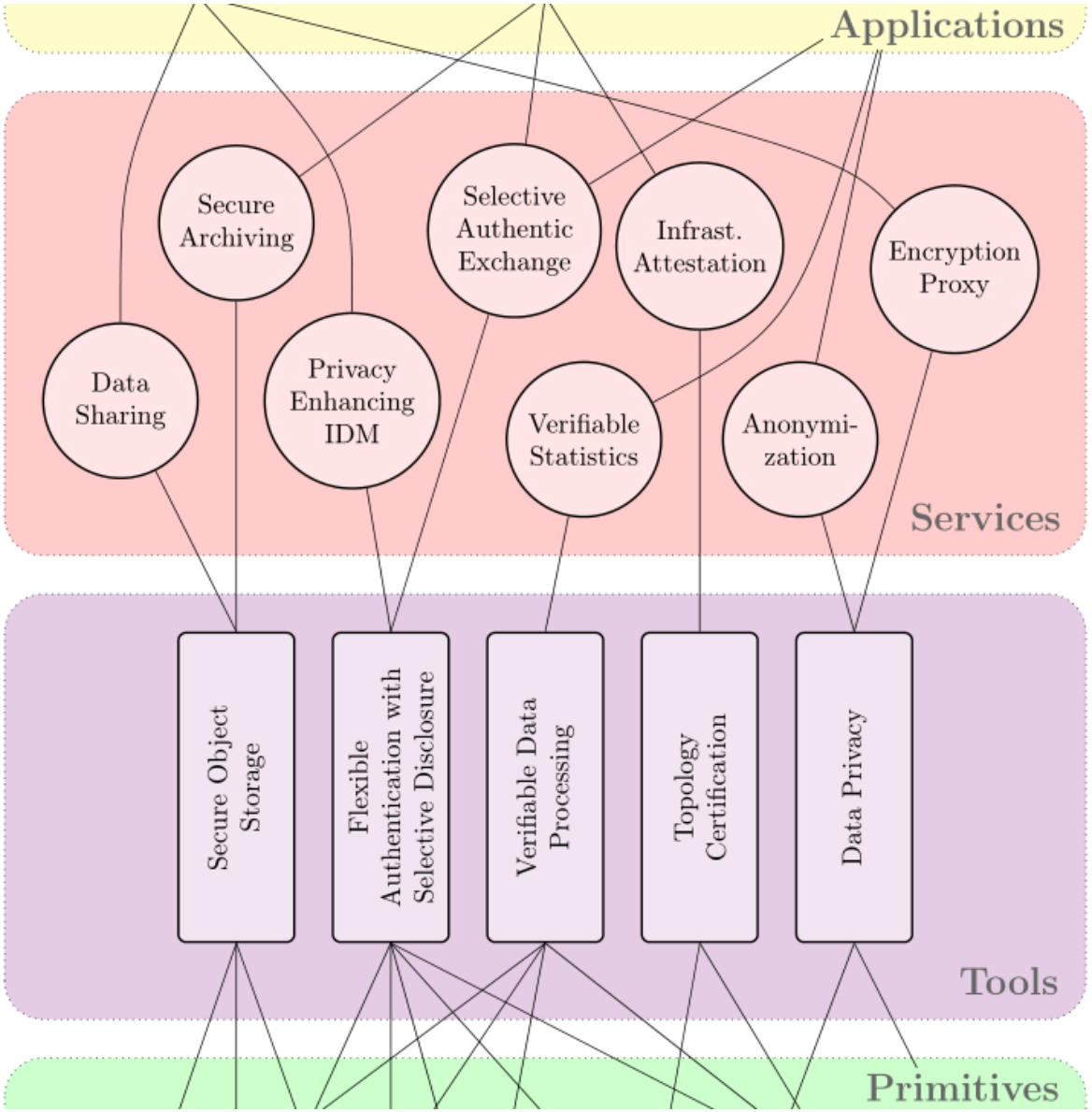
prisma cloud

PRISMACLOUD Architecture



prisma cloud

Zoom



prisma cloud

PRISMACLOUD Architecture

- structures and categorises technical outcomes,
- improves service development process,
- provides project context for r&d activities

prisma cloud

The Project also has a Development Methodology...

- "secure software development lifecycle"
- "derive requirements, translate requirements, and map to model" from top to bottom
- "proof security, deploy tool, and extract capabilities" from bottom to top

prisma cloud

Cloud Security Patterns

Cloud security patterns are used for describing **typical situations where information security and privacy problems occur**—and which cryptographic functionalities can be applied to mitigate these problems.

Cloud security patterns are an application of **design patterns**, which again describe re-usable, proven solutions (with the help of proposed "building blocks") for recurring problems

A design pattern is **characterised according to categories**, like, name of pattern, context, intention, problem, solution, consequences of their application.

prisma cloud

Cloud Security Patterns...

- ...are descriptive rather than normative
- communicate often conflicting security requirements of different involved parties
- make people aware of contradictory aspects
- support a discussion process
- describe generative solutions to common design contentions
- support a security by design approach

prisma cloud

“Re-using” Patterns in PRISMACLOUD

1. In the **requirements work package** (first project year) we established the first version of generic cloud security patterns:
   - to describe **situations where security and privacy problems generally occur**
   - we (approximately) **intended to cover these situation with particular cryptographic technology**

2. Later on, these patterns were used in support of the **development of the PRISMACLOUD architecture** (beginning project year 2).

prisma cloud

Use of Patterns in PRISMACLOUD II

3. Currently, we are modifying the design pattern technique itself—we want to abandon the commonly used generic nature of design patterns—and use them for **explicitly specifying the capabilities of the proposed services and tools for end users**.

4. We also intend to use the "new patterns" for specifying the **setting of configuration parameters** of the sample services for specific end user requirements (service level agreement–SLA).

prisma cloud

PRISMACLOUD Patterns - Synopsis

Field 1: Data Storage in the Cloud

P1: Secure cloud storage by default
P2: Moving a legacy application's database to the cloud

Field 2: User Privacy Protection and Data Minimisation

P3: Non-identifiable and untrackable use of a cloud service
P4: Minimise exposure of private data during authenticat. in the cloud
P5: Big data anonymisation

Field 3: Authentication of Stored and Processed Data

P6: Protect the authenticity of a data set and possible subsets
P7: Authorise controlled subsequent modifications of signed data
P8: Controlling the correctness of delegated computations
P9: Controlling your virtual infrastructures

For details on the patterns/secure cloud services/tools refer to:

- Publication (T. Länger et al.) in the APF2016 Proceedings
- **"PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services"** (Publication by Lorünser, Slamanig, Länger, Pöhls; in: Proceedings of the ARES 2016 conf; to be published on IEEEXPLORE Sept. 2016
  - please email me – I'll send you a preprint copy!
- Project deliverables and pubs on `https://prismacloud.eu`

Thanks for your Attention!

`thomas.laenger@unil.ch`

prisma cloud