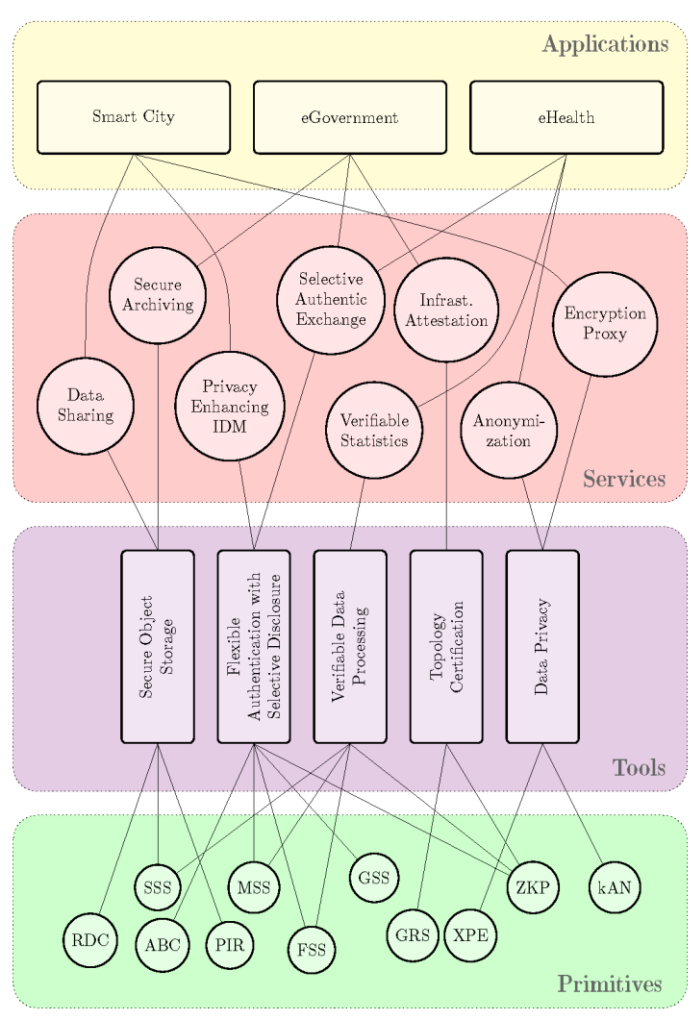
PRISMACLOUD

PRIvacy and Security MAintaining Services in the CLOUD

NEWSLETTER November 2016

This is the second issue of the PRISMACLOUD newsletter that will keep you updated about our scientific progress and achievements, about recent events arranged and venues where we were present. In particular, this second issue contains a short description of the PRISMACLOUD architecture, which has been introduced at the SECPID workshop, and highlights recent scientific achievements. Furthermore, we present an overview of the e-Health pilot – one of our three project pilots - and the newsletter is concluded with short reports from events which we organized, or participated in.

PRISMACLOUD Architecture



The PRISMACLOUD project is a huge undertaking and produces outcome in many different disciplines and layers. To structure and categorize the technical outcomes, we introduce the PRISMACLOUD architecture, which is organized in 4 tiers. On the uppermost (i) ***Applications layer*** are the end user applications. Applications use the cloud services of the (ii) ***Services layer*** to achieve the desired security functionalities. The cloud services specified there are a representative selection of possible services that can be built from the tools organized in the (iii) ***Tools layer***. In particular, they represent a way to deliver the tools to service developers and cloud architects in an accessible and scalable way. Together the tools constitute the PRISMACLOUD toolbox. Tools encapsulate the needed cryptographic primitives and protocols from the (iv) ***Primitives layer***, which is the lowest layer of the PRISMACLOUD architecture.

Figure1: The PRISMACLOUD Architecture (Primitives abbreviations: RDC: Remote Data Checking; SSS: Secret Sharing Schemes; ABC: Attribute-Based Credentials; PIR: Private Information Retrieval; MSS: Malleable Signature Schemes; FSS: Functional Signature Schemes; GSS: Group Signature Schemes; GRS: Graph Signature Schemes; XPE: Format- and Order-Preserving Encryption; ZKP: Zero-Knowledge Proofs; kAN: k-Anonymity)

Scientific Publications

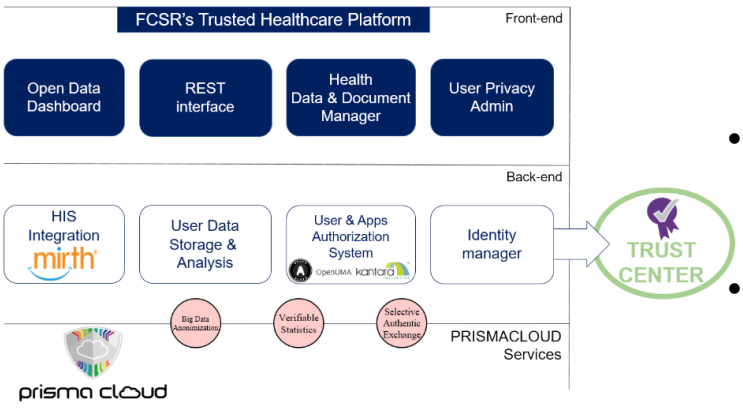
The consortium had a successful collaborative scientific work, developed within the project, available to the research community through numerous publications produced and presented in conferences around the world. Some of the publications are listed below.

- Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing (15th International Conference on Cryptography and Network Security, CANS 2016, Milan, Italy)
- Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds (ENISA Annual Privacy Forum, AFP 2016, Frankfurt, Germany)
- Dynamic and Verifiable Hierarchical Secret Sharing (9th International Conference on Information Theoretic Security, ICITS 2016, Seattle, USA)
- PRISMACLOUD Tools: A cryptographic toolbox for increasing security in cloud services (Security, Privacy, and Identity Management in the Cloud, SECPID 2016 @ ARES 2016, Salzburg, Austria)

The complete list of Scientific Publications is available on the PRISMACLOUD website.

E-Health Pilot: Data Sharing Portal for Health Records

The e-Health use case proposed inside the PRISMACLOUD Project aims to supporting secure and privacy-friendly interaction between patients and healthcare providers or between different hospital services and the clinicians. The figure below shows the architecture used for the e-Health use case based on the FCSR's Trusted Healthcare Platform (THP). The main objective of this use case is to add several privacy and security features based on PRISMACLOUD primitives to the THP.



In particular three of the PRISMALOUD Services will be used to extend the THP's features:

- The **Selective Authentic Exchange** permitting the THP to redact health documents on behalf of the patient according to user's privacy and recipient's need using malleable signatures.
- The **Big Data Anonimization** service with the aim of supporting open health data to the research community, i.e., by means of anonimized datasets.
- The **Verifiable Statistics** with the capibility to outsource computation on authenticated (and encrypted) data having the possibility to audit the correctness of the computations operation by a recipient.

Standardization Activities

One of the main actions defined in the PRISMACLOUD standards action plan is to seek contact with the ISO (International Organisation of Standardisation), particularly ISO/IEC JTC 1/SC 27 – IT Security Techniques (JTC - joint technical committee; SC - subcommittee).
Our project achieved to establish a liaison activity and we will participate in the upcoming meeting on 24-25 April 2017 in New Zealand.
Prior to contacting the ISO subcommittee several developments where triggered to get a clearer picture about the project outcome:

- the development of the layered architecture with its clear distinction between 'tools' and '(cloud) services';
- the detailed development and specification of the use cases
- active involvement in community events (see past events)
- feedback from UAB members

At ISO one standard was identified to be of special importance for the project (and also in the right draft stage for contributions): ISO/IEC 19086-4: 2015 'Information technology - Security techniques – Information technology – Cloud computing Service Level Agreement (SLA) framework - Part 4: Security and privacy (This International Standard specifies the Security and Privacy aspects of Service Level Agreements (SLA) for cloud services including requirements and guidance. This standard is for the benefit and use for both cloud service provider and cloud service customer).

At the moment, we are preparing our participation via the Austrian delegation and getting support through the German and Swedish delegation. In preparation for our next meeting we are going to have a project internal workshop for the initial preparation of a detailed contribution to ISO/IEC 19086-4, i.e., for service level agreement configuration for the newly developed secure cloud services and also involve a consultation with our UAB.

Upcoming Events – We will be there!

Our project partners will participate in the following events and are happy to meet and discuss with you!

- **Mycrypt 2016: Paradigm-shifting Crypto -** Kuala Lumpur, Malaysia, 1 - 2 December 2016
https://foe.mmu.edu.my/mycrypt2016/

- **ASIACRYPT –** Hanoi, Vietnam, 4 - 8 December 2016
http://www.asiacrypt2016.org/

- **SLA-Ready Impact Workshop –** Brussels, Belgium, 15 December 2016
http://www.sla-ready.eu/news/sla-ready-impact-workshop-15-december-2016-brussels

Past Events

In the last period the PRISMACLOUD consortium was very active and organised/participated in several events. In the following we present the most important ones.

SECPID - International Workshop on Security, Privacy, and Identity Management in the Cloud
Salzburg, Austria, August 31, 2016

Together with our partner project CREDENTIAL, we organized an EU Symposium at the 11th International Conference on Availability, Reliability and Security – ARES 2016. The workshop entitled "SECPID – International Workshop on Security, Privacy, and Identity Management in the Cloud" was intended to offer a platform to present visions and results of FP7 and H2020 projects. The program featured 6 contributed talks (selected by the program committee from 12 submissions) covering presentations from the H2020 SUNFISH, WITDOM, CREDENTIAL and PRISMACLOUD projects as well as an invited talk given by Dr. Hugues Mercier (Université de Neuchâtel) discussing challenges within the H2020 SAFECLOUD project. The workshop was very well attended by scientific community related to the projects but also by many people interested in the respective projects and lead to many inspiring discussions among the attendees. All papers presented at SECPID are included in the official ARES 2016 proceedings.

IPEN - Internet Privacy Engineering Network
Frankfurt, Germany, September 9, 2016

IPEN was established in 2014 as a platform that brings together developers and data protection experts with a technical background from different areas in order to launch and support projects that build privacy into everyday tools and develop new tools which can effectively protect and enhance our privacy. The high-quality audience of this year's IPEN event was led by Achim Klabunde, head of IT Policy sector of the European Data Projection Supervisor (EDPS).

Other participants included representatives from data protection authorities like ENISA and ULD, industry like Deutsche Telekom and the SME signatu from Norway, as well as researchers. PRISMACLOUD was one of two H2020 projects offering financial support to the non-profit organizers. In his presentation, Thomas Länger (UNIL) presented the PRISMACLOUD architecture, and gave a first account on the newly developed methodology (cf. D7.5 'First version of guidelines and architecture for secure service composition'). Of particular interest for the audience were the privacy-by-design methods, and how they are integrated in the structured development process (http://link.springer.com/book/10.1007%2F978-3-319-44760-5).

SECODIC - International Workshop on Secure and Efficient Outsourcing of Storage and Computation of Data in the Cloud

Salzburg, Austria, August 31, 2016

The H2020 projects TREDISEC and WITDOM organized an EU Symposium at the 11th International Conference on Availability, Reliability and Security - ARES 2016. The workshop featured 10 contributed talks and an invited talk by Prof. N. Asokan (Aalto University). PRISMACLOUD contributed a talk on "Malleable Cryptography for Security and Privacy in the Cloud" held by Daniel Slamanig (Graz University of Technology). The workshop was a very good opportunity learning about the interesting challenges our partner projects are working on and to exchange ideas and discuss open problems with other researchers in this field.

ENISA Annual Privacy Forum 2016

Frankfurt, Germany, September 7-8, 2016

Thomas Länger presented the (peer reviewed) publication "Thomas Länger, Henrich C. Pöhls, and Solange Ghernaouti: Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds".

The presentation was received with great interest and sparked an intense discussion on the possibilities and potential impact of cloud services augmented and equipped with end-to-end security and privacy (https://www.enisa.europa.eu/events/annual-privacy-forum-2016).

CAST Workshop

Darmstadt, Germany, October 13, 2016

Current trends in technology, such as cloud computing, and legal regulations by the legislator have a significant influence on the requirements and opportunities when developing modern digital archiving systems. On the one hand, this poses new challenges, such as ensuring security properties like authenticity, integrity and confidentiality of documents even in the long-term. On the other hand, the technological process allows developing novel solutions, which provide a higher flexibility, more functionality and a better performance.

In this CAST Workshop several representatives of science, industry, and public administration come together to discuss legal, technical and functional aspects of digital archiving schemes. The event was organised by our project colleague Denise Demirel from TU Darmstadt.

(https://www.cast-forum.de/workshops/programm/223).

PRISMACLOUD

PRIvacy and Security MAintaining Services in the CLOUD

PLLS 2016 - Protection of Long-Lived Systems

Darmstadt, Germany, July 18-19, 2016

With increasing digitization, the number of long-lived systems and services increases rapidly. For example, digital archives such as genomic databases will have to operate for many decades or even centuries. The protection of such long-lived systems against security risks is indispensable.

Most of the security technology used today appears to be inappropriate for protecting long-lived systems. This is particularly true for cryptography. Keys chosen today will be too short in the future or they may leak over time. Researchers may find new attacks against schemes that are considered secure today. Therefore, the protection of long-lived digital systems is an important scientific and technological problem.

Several researchers have proposed partial solutions. For example, there are security models for long-lived systems; there is quantum key distribution and one-time pad encryption, which offer information theoretic protection of the confidentiality of data in transit; there are time-stamp-based solutions that ensure long-term integrity of data in archives. However, there is no comprehensive solution of the problem yet.

The workshop will bring together researchers from the relevant technology and application areas to discuss important scientific challenges that need to be addressed in order to find theoretically sound and practical solutions that provide protection of long-lived systems. The event was organised by our project colleague Denise Demirel (TUDA). More: https://www.securityweek2016.tu-darmstadt.de/plls-2016/

5th annual Cloud Security Alliance EMEA Congress

Madrid, Spain, November 15-16, 2016

On November 14-15th 2016, Atos participated in Cloudwatch2 Cloud Security Plugfest, an event organized by CloudWatch2 project (a European Cloud observatory supporting cloud policies, standard profiles & services) in cooperation with Cloud Security Alliance (CSA) and collocated with CSA EMEA Congress 2016 in Madrid. Atos represented PRISMACLOUD at both events, where other related DPSP projects were also presented. In addition to representing a communication opportunity, the outcomes of both events are relevant to PRISMACLOUD as they respectively focus on gaining from the cloud research and industrial communities different perspectives related respectively to maximizing the adoption of and contribution to security standards in cloud projects and on addressing the current and coming changes in cloud security and privacy, where PRISMACLOUD is enabling remarkable technological advances beyond the state of the art, with high potential for beneficial impact across Europe and beyond.

https://csacongress.org/event/emea-congress-2016

Further information about the PRISMACLOUD Project

Website: https://prismacloud.eu/
Twitter: https://twitter.com/prismacloud | @prismacloud
LinkedIn: https://linkedin.com/in/prismacloud | PRISMACLOUD Project
CORDIS: http://cordis.europa.eu/project/rcn/194266_en.html
Additional information can be requested via admin@prismacloud.eu

Topic: ICT-32-2014
Type of Action: RIA
Partners: 16
Duration: 42 months
Start Date: 01.02.2015
Coordinator: AIT Austrian Institute of Technology GmbH