PRISMACLOUD

PRIvacy and Security MAintaining Services in the CLOUD

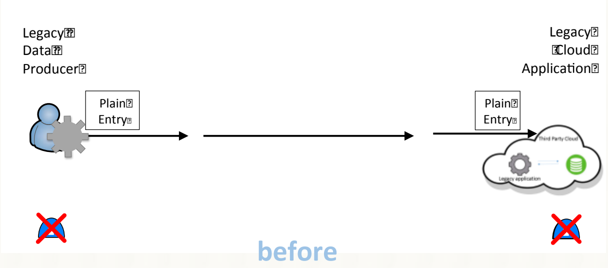
NEWSLETTER January 2018

This is the fourth issue of the PRISMACLOUD newsletter that will keep you updated about our scientific progress and achievements, and future events where we will participate. In particular, this fourth issue contains a short description of the PRISMACLOUD Services, a summary of the Smart City pilot, our progress in standardization activities and details about the upcoming SECPID workshop.

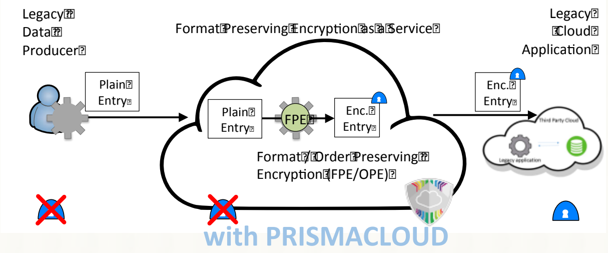
PRISMACLOUD Services

PRISMACLOUD has designed and implemented in software/hardware a number of cryptographic mechanisms. The implementations, called PRISMACLOUD Tools, offer the highest possible degree of freedom when it comes to configuration of cryptographic parameters. This allows to use them to increase the security and privacy in a broad number of services usually offered in the cloud environment. In the following we present how the PRISMACLOUD Services are enhanced in terms of four main security and privacy goals: Confidentiality (🔒), Integrity (🏅), Availability (▷) and Privacy-Enhancements (☺). Below the impact of an encryption proxy:

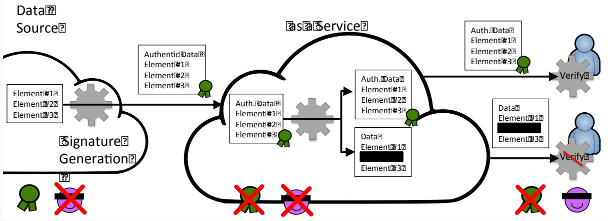
Using a legacy cloud service that manages your structured data would not protect the confidentiality of the data stored.

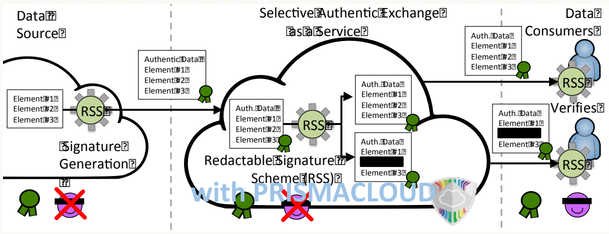


Instrumenting the Format Preserving Encryption (FPE) implementation your structured data is encrypted before it reaches the legacy cloud. This increased confidentiality.



Another PRISMACLOUD service decreases the trust in respect to the integrity put into intermediate services:





Above see the removal of data from a signed data-set. This increases privacy, but breaks conventional digital signatures. All integrity and authenticity guarantees given by the signature are lost. With an implementation of advanced signature primitives of redactable signatures (RSS) PRISMACLOUD retains a valid signature over the redacted data without the need of a secret key in the cloud and without the ability to generate new data. This removes the necessity to trust the intermediate data-handlers for integrity (gain end-to-end integrity).

Piloting Phase Started

We are piloting! To demonstrate the capabilities of methods and tools developed within PRISMACLOUD, they are being evaluated and validated in our three dedicated application scenarios (Smart City, e-Government, and e-Health), which integrate selected components and tools in different combinations to gain in security for representative tasks within the respective domain.

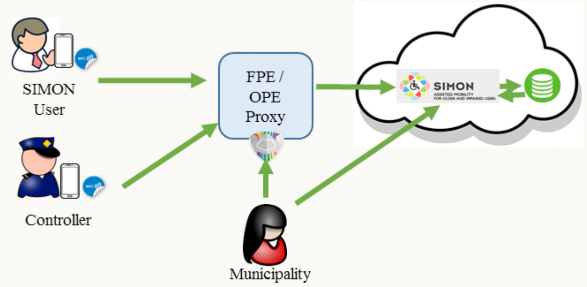
The PRISMCLOUD tools have been integrated in cloud test-beds at multiple sites identical to real-life service scenarios and their performance is being validated under realistic assumptions. This approach demonstrates to service providers how they can migrate parts of their systems to cloud environments with increased security. It thus also enables the deployment of hybrid scenarios or provides novel trustworthy services for third parties in their own private cloud, which have not been possible without the results of PRISMACLOUD.

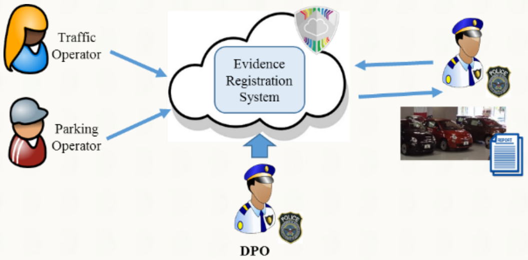
Each pilot will be developed and improved until March 2018 and will be validated until July 2018, following a two iterations approach: the services will be in the cloud by the end of the first iteration and a preliminary validation will be finished. In the second iteration, and based on the results of the first one, a refinement of services and applications will take place for each pilot. New tests and validations will aim at finalizing the collection of data that will be analysed to prepare the set of recommendations and lessons learnt.

Smart City Pilot

The SIMON system (http://simon-project.eu) is a platform aimed at managing mobility of disabled citizens, and it is one of the smart city use cases in which PRISMACLOUD services are being validated. In a first step, we carry out the *cloudification* of SIMON, that is, to move the current application to the cloud. This implies to encrypt sensitive data, through the **Encryption Proxy service**.
The second step is the anonymization of SIMON. The user will not be identified by the system in any way to guarantee his/her privacy, so the identifier of the user is replaced by a proof of belonging to a group. This change include the use of **Privacy Enhancing Identifier Management service**.

The objective of the Evidence Registration Platform use case is to use secure ICT technologies to implement a solution for the exchange of information to enhance current practices mostly based on recording and delivery of physical media. This cloud-based sharing system is developed allowing traffic system operators, parking operators and law enforcement units to exchange sensitive data (pictures of license plates, video of incidents, and all the meta-data linked to them) in an easy, reliable and secure way. The **Data Sharing service** is used to divide files in parts and ensure that this data can only be accessed by the proper actors, and can be securely stored in the cloud.





Standardization and ISO Meeting

PRISMACLOUD has continued its standardization efforts at the meeting of the **ISO/IEC JTC1/SC27 "Security techniques" in Berlin, Oct 30 – Nov 3, 2017**. A team of three researchers from Universities Lausanne and Passau, and from the coordinator AIT attended the week-long work group meetings of **WG2 "Cryptography and Security Mechanisms"** and **WG4 "Security Controls and Services"**. We have two active liaisons (liaisons category "C") with these groups, and in order to maximize our impact, we are also accredited by the national standardization bodies of Austria (ASI) and by the German DIN.

In WG2, at the recent SC27 meeting in Hamilton, NZ (April 2017), we proposed a **study period for a new standard on redactable signature schemes**, being one of the core technologies implemented in the project. This study period yielded positive feedback and hence we could launch a **new work item proposal** for a respective standard, now named **„Information Technology – Security Techniques – Redaction of Authentic Data – Part 1: General"**, which is now to be voted upon by the national ISO member bodies. We expect that the work item proposal will be accepted and expect the work on that new standard to begin at the upcoming **ISO/IEC JTC1/SC27 meeting in Wuhan/China, April 16 -20, 2018**. The study period was also prolongated to assess the possibilities of further parts of the standard, dealing with the cryptographic detail of suitable primitives and protocols.

In WG4, it was the second time that we were able to contribute to the standard **ISO/IEC 19086-4 Cloud computing Service Level Agreement (SLA) framework - Part 4: Security and privacy'**. At the recent ISO meeting in Hamilton, PRISMACLOUD contributed 81 comments and could manage to get **several Cloud Service Qualitative Objectives (SQOs)** for our newly developed tools and services into that standard: for integrity protection of data in motion, for anonymous and pseudonymous authentication support and for data minimization cryptographic controls. For Berlin, we prepared a complete overhaul of the "Cryptography Component", being a central part of that standard. Our proposal was accepted with only minor modification, so that the standard now covers the **cryptographic protection of data wrt. confidentiality and integrity** not only **"in motion"**, but also **"at rest"** and **"in use"**. ISO 19086-4 is to be propagated to level **"Draft International Standard"** (currently under ballot) so that it is entirely possible, that our essential contributions may become part of an **International Stand** at the upcoming Wuhan meeting, i.e. even before the end of the project!

Scientific Publications Highlights

- David Derler, Stephan Krenn, Thomas Lorünser, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks. Revisiting Proxy Re-Encryption: Forward Secrecy, Improved Security, and Applications. Public Key Cryptography (PKC), Rio De Janeiro, Brazil, March 25-28, 2018
- David Derler, Sebastian Ramacher, Daniel Slamanig. Short Double- and N-Times-Authentication-Preventing Signatures from ECDSA and More. 3rd IEEE European Symposium on Security and Privacy (EuroS&P 2018). April 24-26, 2018, London, United Kingdom.
- Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Greg Zaverucha. Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. 24th ACM Conference on Computer and Communications Security (ACM CCS 2017). Dallas, Texas, USA. October 30 – November 3, 2017.

PRISMACLOUD
PRIvacy and Security MAintaining Services in the CLOUD

SECPID 2018 at ARES Conference 2018

SECPID 2018
3rd Workshop on Security, Privacy, and Identity Management in the Cloud
August 27-30, 2018
Hamburg, Germany
DPSP
prisma cloud

PRISMACLOUD, its partner project CREDENTIAL and the DPSP Cluster are organizing a **Workshop on Security, Privacy, and Identity Management in the Cloud** at this year's ARES conference, the 13th International Conference on Availability, Reliability and Security

Date: August 27 - August 30, 2018
Place: Hamburg, Germany

The aim of this symposium is to provide a platform to discuss innovative ideas related to the following questions: How can cloud services be made more trustworthy? How can we build distributed systems without single point of failure or trust? How to design end-to-end secure services in an untrusted environment? Which methodologies and technologies are required to integrate security and privacy by design? Is it possible to give back users full control over which data they want to reveal when and to whom?

We are looking forward to your submissions, and interesting and fruitful discussions during the workshop sessions! The **call for papers** as well as the submission guidelines can be found >> here <<.

Additional News in Short

- PRISMACLOUD successfully passed the 2nd European Commission intermediate review
- All public deliverables accepted so far from the European Commission are availbale at: https://prismacloud.eu/project-deliverables/
- We published two new videos on the PRISMACLOUD videos series „Data, Thieves & Cloud“.
  Check our YouTube channel:
  - Data, Thieves & Cloud Part 1 - How to store and share your data safely.
  - Data, Thieves & Cloud Part 2: How to reliably process your data.
  - Data, Thieves & Cloud Part 3: How to selectively share authentic data.

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