PRISMACLOUD
PRIvacy and Security MAintaining Services in the CLOUD

NEWSLETTER May 2017

This is the third 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 third issue contains a short description of the PRISMACLOUD Toolbox, and highlights recent scientific achievements. Furthermore, we present an overview of the e-Government pilot – one of our three project pilots - , the exploitation and standardization activities, and the future events which we will co-organize and participate.

PRISMACLOUD Toolkit

The PRISMACLOUD toolkit, one of the major results of the project, is a cryptographic toolbox for enhancing the security and privacy of cloud services. A tool can be regarded as an abstract concept which is composed of various cryptographic primitives that can be parametrized in various different ways.
But more importantly, the tools have also be implemented during the project and made accessible in form of software libraries, which will now be used to build the PRISAMCLOUD services and pilots.

The following tools are being developed in the PRISMACLOUD project:

A. Secure Object Storage Tool (SECOSTOR): This tool provides strong security guarantees in terms of confidentiality and availability to be applied to cloud storage and backup services. To achieve this properties, this tool leverages the concept of cloud federation and information dispersal, i.e. data is fragmented and distributed over different public cloud services to yield a secure and reliable virtual service on top of multiple less reliable services.

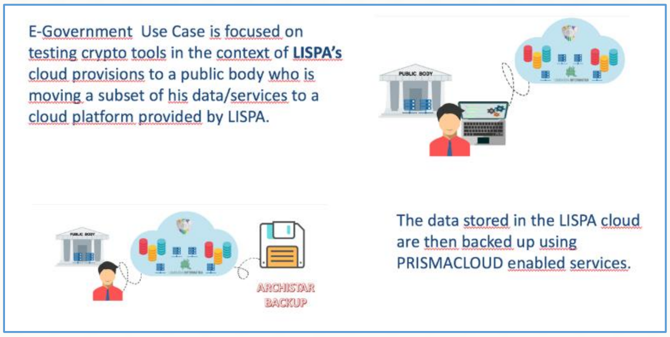
B. Flexible Authentication with Selective Disclosure (FLEXAUTH)*:* This tool supports the authentication of arbitrary messages (or documents) by means of digital signatures with selective disclosure features. This selective disclosure happens according to some well defined rules (called a policy) which can be determined by the originator of the data. A verifying party can then use the verification component to verify the authenticity of the partial information by means of the originator’s verification key.

C. Verifiable Data Processing (VERIDAP): This tool supports the delegation of processing authenticated data in a way that the result can be efficiently verified for correctness. The data processing component is given a set of input data and a description of the processing rules, and outputs the result of the computation, as well as a proof certifying the correctness of the delegated computation.

D. Topology Certification (TOPOCERT): The topology certification tool supports the application of graph signatures to certify and prove properties of topologies and realized as an interactive protocol framework between the roles of an issuer, a prover and a verifier.

E. Data Privacy (DATPRIV): This tool provides the means for processing structured data in different ways, supporting different purposes with different privacy requirements. This tool enables users of legacy applications to move their databases to a public cloud, while preserving data privacy and confidentiality. Moreover, the tool provides components for data generalization as means for anonymizing bulk data using k-anonymity techniques.

E-Government Pilot



E-Government Use Case is focused on testing crypto tools in the context of **LISPA's** cloud provisions to a public body who is moving a subset of his data/services to a cloud platform provided by LISPA.

The data stored in the LISPA cloud are then backed up using PRISMACLOUD enabled services.

Lombardy Region in Italy has set a strategy aimed at fostering a more effective use of IT resources, by rationalising IT infrastructures of public bodies and eliminating smaller ones. The PRISMACLOUD e-Government use case is framed within this context. Lombardia Informatica (LISPA), Lombardy Regions IT in-house company, is going to provide its customers the infrastructures to host datacenters when required.

The e-Government use case, more specifically, is focused on backup services exploiting the distributed secure storage services enabled by PRISMACLOUD.

These services, leveraging on advanced encoding techniques, allow customers to spread their data across several storage units with premium advantages:

- data are spread across several storage units and the customer may rebuild its original archive using only a limited number of shares generated;
- should someone violate any of the archive it would be impossible for him to destroy the entire archive;
- thanks to PRISMACLOUD technology the use of disk space is optimized;
- backup integrity can be checked without the need of performing a full restoration of the DB (which is a big issue when talking about big data).

Advantages

The storage of data and backups is a key issue for LISPA. In real life, we are often talking about big data so back-ups are not easy to handle. Restore testing may be difficult because of the additional storage capacity needed to test a restore procedure and, to maintain a high level of security, using encryption, you should manage keys which is a demanding procedure when applied to many customers. The storage efficiency brought up by Archistar and the possibility to test backups, without the need of handling keys, will be object to thorough test during the use case pilot.

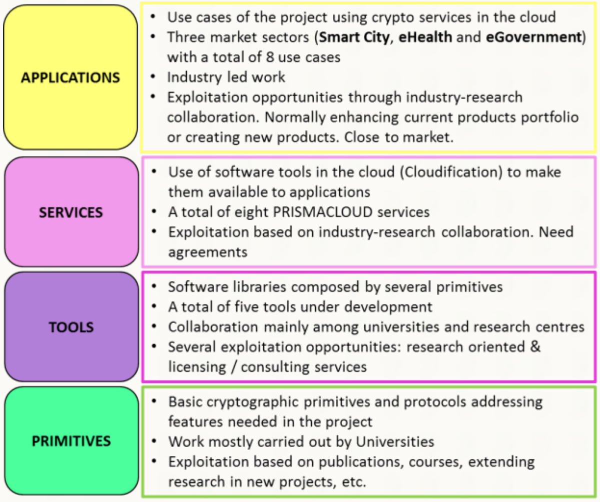
Even more interesting, distributing backup shares across several locations with the possibility to know which shares are required for archive restoring is a premium feature; it potentially opens the doors to the implementation of hybrid cloud environments. Currently, Lombardia Informatica, delivers its services using a proprietary infrastructure, located in two different data centers in Milan, Italy. Being able to upload single shares to untrusted locations, being sure that those shares do not allow archives to be restored, gives the opportunity to use private providers increasing infrastructure scalability and making it possible to also use cheaper providers, potentially having more cost flexibility for service delivery. This, potentially, would innovate the company's business model and is currently under study.

PRISMACLOUD

PRIvacy and Security MAintaining Services in the CLOUD

Exploitation Activities

Exploitation opportunities in PRISMACLOUD have been defined around the different results and the profiles of the partners involved, as follows:



APPLICATIONS	• Use cases of the project using crypto services in the cloud • Three market sectors (**Smart City**, **eHealth** and **eGovernment**) with a total of 8 use cases • Industry led work • Exploitation opportunities through industry-research collaboration. Normally enhancing current products portfolio or creating new products. Close to market.
SERVICES	• Use of software tools in the cloud (Cloudification) to make them available to applications • A total of eight PRISMACLOUD services • Exploitation based on industry-research collaboration. Need agreements
TOOLS	• Software libraries composed by several primitives • A total of five tools under development • Collaboration mainly among universities and research centres • Several exploitation opportunities: research oriented & licensing / consulting services
PRIMITIVES	• Basic cryptographic primitives and protocols addressing features needed in the project • Work mostly carried out by Universities • Exploitation based on publications, courses, extending research in new projects, etc.

On February 23rd, 2017 the PRISMACLOUD Consortium organized an Exploitation Strategy Seminar aimed at better identify the Key Exploitable Results. Initialy, a total of 17 KERs were characterized and a risk assessment was carried out for each of them. Based on this preliminary analysis, the KER list of the project was reduced to 6 results, and for those a complete characterisation was completed, including also the external factors affecting them and their development. A variety of different aspects connected to the KER have led us to discover opportunities, risks, problems etc., that were not so visible before doing this exercise:

- *The "Characterization of KER" provides a basic description*
- *The "Internal & External Players" to describe partners, customers and competitors*
- *The "KER Risk Assessment Map" to define the risks connected to bringing the KER to market.*

Standardisation

The PRISMACLOUD project can proudly present a first influx of project developed content into an actual standards document. It happened at the recent 24th meeting of **ISO/IEC JTC1 SC27 "IT Security Techniques"** at Waikato University in Hamilton, New Zealand (18-22 April, 2017), where the project was represented by standardisation task leader University of Lausanne (UNIL).

After having successfully applied for a **Liaison Category C with SC27 Working Group WG4** "Security Controls and Services" at the penultimate SC27 meeting in Abu Dhabi (23 – 26 Oct, 2016), the PRISMACLOUD team responsible for standardisation developed and submitted 73 comments for an upcoming cloud SLA (Service Level Agreement) standard: **ISO/IEC 19086-4 "Information technology – Cloud computing – Service Level Agreement (SLA) framework – Part 4: Security and privacy"** will provide security and privacy components of cloud SLAs that can be used by organisations and individuals to create, modify, or understand a cloud SLA.

Among the contributions which were accepted during extensive comments resolution meetings are Cloud Service Qualitative Objectives (SQOs) for **integrity protection of data in motion, for anonymous and pseudonymous authentication support and for data minimisation cryptographic controls.** We intend to continue our effort for the 19086-4 standard (which is currently in "Committee Draft" status) in the upcoming two SC27 meetings that will still fall in the duration of the project (in Berlin and Wuhan).

Additionally, we also applied **for another liaison with SC27 WG2 "Cryptography and Security Mechanisms"**, and within WG2 for a **study period for a new standard for redactable signatures**, which is one of the PRISMACLOUD core technologies. Both applications were unanimously accepted.

PRISMACLOUD

PRIvacy and Security MAintaining Services in the CLOUD

Scientific Publications Highlights

* Michael Till Beck, Jan Camenisch, David Derler, Stephan Krenn, Henrich C. Pöhls, Kai Samelin and Daniel Slamanig. Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures. 22nd Australasian Conference on Information Security and Privacy. Auckland, New Zealand, 3-5 July 2017.

* Johannes Braun, Johannes Buchmann, Denise Demirel, Matthias Geihs, Mikio Fujiwara, Shiho Moriai, Masahide Sasaki, Atsushi Waseda. LINCOS - A Storage System Providing Long-Term Integrity, Authenticity, and Confidentiality. ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017. Abu Dhabi, UAE, April 2-6, 2017 (to appear).

Upcoming Workshops and Events – Find us there!

International Workshop on Security, Privacy, and Identity Management in the Cloud – SECPID 2017
August 29 – September 2, 2017, Reggio Calabria, Italy

SECPID 2017
prisma cloud
Workshop on Security, Privacy, and Identity Management in the Cloud
Reggio Calabria, Italy
August 29 – September 2, 2017

PRISMACLOUD and our liaison project CREDENTIAL are organising the second SECPID workshop at ARES conference. This year's workshop is supported by the DPSP Cluster, which gives the opportunity for funding sunergies and establish better collaboration between EU research projects, and discuss innovative ideas related to security, privacy and identity management in the Cloud. https://www.ares-conference.eu/workshops/secpid-2017/

12th International IFIP Summer School on Privacy and Identity Management – the Smart World Revolution
September 3 – 8, 2017, Ispra, Italy

We are happy to support the IFIP Summer School for a third year, where we will have the opportinity to hold a workshop together with our liaison projects CREDENTIAL and WITDOM which will give us the opportunity to present the PRISMACLOUD output and discuss about demonstrators. http://www.ifip-summerschool.org/

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