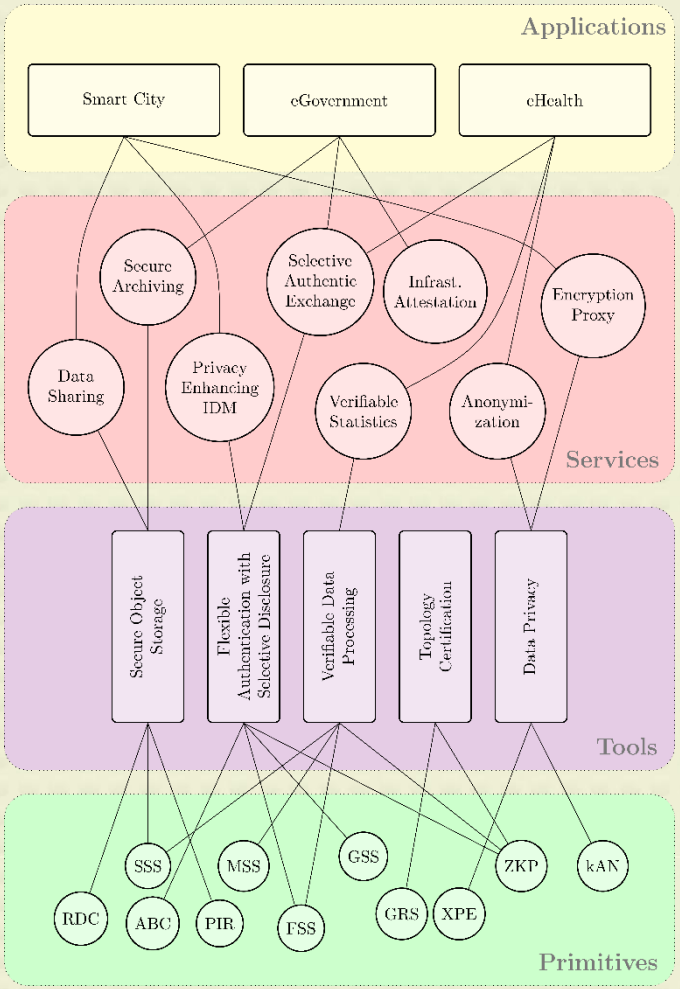
ARCHITECTURE

The PRISMACLOUD project is a huge undertaking and produces outcome in many different disciplines and layers. To structure and categorize the technical outcomes, we introduced the PRISMACLOUD architecture, which is organized in 4 tiers.



SOCIAL MEDIA

PRISMACLOUD Project @prismacloud

PRISMACLOUD Project H2020

PRISMACLOUD Project

https://prismacloud.eu

admin@prismacloud.eu

PARTNERS

PRISMACLOUD

Privacy and Security Maintaining Services in the Cloud

We are developing the next generation of cloud security technologies. We bring novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services for providers and users.
***Our main idea and ambition** 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**.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644962.

OBJECTIVES

Development of cryptographic tools to protect the security of data during its lifecycle in the cloud. Development of cryptography to protect confidentiality, integrity, and authenticity of data at rest beyond standard content encryption and message authentication.

Development of cryptographic tools and methods to protect privacy of users. Development of cryptography to preserve privacy of users interacting with cloud services by anonymous authentication and to preserve privacy of user related data using anonymization techniques.

Creation of enabling technologies for cloud infrastructures. Provision of software and implementations of relevant cryptographic mechanisms for fast dissemination of results.

Development of a methodology for secure service composition. Development of security and usability models and their integration in development life-cycles according to security and privacy by design methods.

Experimental evaluation and validation of project results. Validation of the developed methods and tools in three pilots from three different domains: healthcare, smart city and e-government.

PRISMACLOUD Framework

PRISMACLOUD Toolkit comprising **5 cryptographic tools** to solve typical problems in cloud computing.

8 PRISMACLOUD Services with increased security and privacy features based on cryptography.

Design methodology and security models for cryptographically enhanced cloud services covering the full life-cycle.

Guidelines and recommendations for application design based on PRISMACLOUD services and tools.

TOOLKIT

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. This tool leverages the concept of cloud federation and information dispersal to achieve this properties, 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.

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. They provide selective disclosure according to 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.

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.

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

Data Privacy (DATPRIV). This tool provides the means for processing structured data in different ways, supporting different purposes with different privacy requirements. It 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.

USE CASES

Smart Cities. Two areas related to mobility and security are investigated and tested within our project: firstly, a more privacy friendly version of ICT implementation of the European Disabled Badge for public parking areas based on FLEXAUTH; secondly, a secure cloud based evidence sharing platform for public agents (emergency services, law enforcement units, traffic control centres, etc.) based on SECOSTOR.

E-Government. Public bodies will be enabled to set up their back-up policies more flexibly. Thanks to PRISMACLOUD services based on SECOSTOR, they will take advantage of a secure distributed storage system allowing them to use resources more efficiently and periodically check backup integrity, including configuration checks based on TOPOCERT.

E-Health. The e-Health use case proposed in the PRISMACLOUD project aims to support secure and privacy friendly interaction between patients and healthcare providers or between different hospital services and the clinicians. The main objective of this use case is to add several privacy and security features based on PRISMACLOUD primitives to the FCSR's Trusted Healthcare Platform (THP).