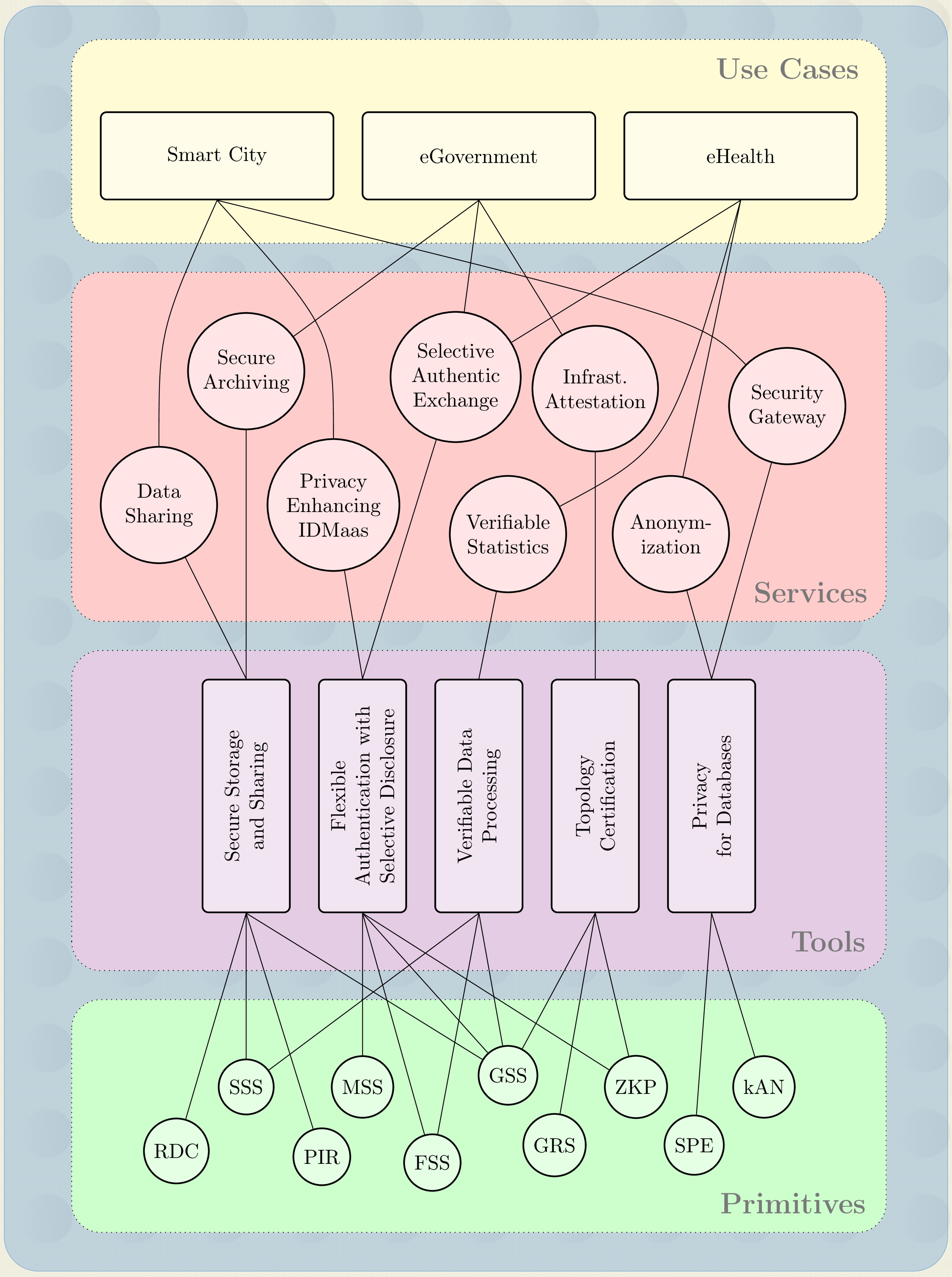
# PRISMACLOUD Outcome



## SERVICES

**S.1 Data Sharing:** Facilitates file storage and sharing with increased data privacy and availability as well as secure deletion.

**S.2 Secure Archiving:** A data backup service with long-term security option and means for efficient and privacy preserving remote auditing.

**S.3 Security Gateway:** An Encryption service for outsourcing databases within legacy applications to untrusted cloud infrastructures.

**S.4 Privacy Enhancing IDM:** An identity management service that enables users to delegate privacy-preserving identity management to a cloud service.

**S.5 Anonymization:** This services enables anonymization of large amounts of data in a way that sharing data with other stakeholders provably protects the anonymity of data subjects.

**S.6 Selective Authentic Data Exchange:** This service enables users to move their authentic documents to a cloud service and then delegate the selective but authentic sharing of parts of these documents.

**S.7 Verifiable Statistics:** This service enables the collection of authentic data series over time and calculation of statistics such that the results can be efficiently checked for validity.

**S.8 Infrastructure Attestation:** This service enables a cloud provider to leverage auditing results and to prove security properties to customers in a privacy friendly way.

## TOOLS

**T.1 Secure Storage and Sharing of Data:** This tool builds a virtual storage services out of multiple individual storage services, i.e., a cloud of clouds, which better protects the confidentiality and availability of stored data than the individual does. It applies the concept of secure information dispersal to encode stored data such that no individual provider cloud read stored data or tamper with them.

**T.2 Privacy for Databases:** This tool supports the encryption and anonymization of structured data and thus enables the “cloudification” of applications containing potentially sensitive data. Privately hosted security gateways could be built out of this tools, which operate in a transparent way.

**T.3 Flexible Authentication with Selective Disclosure:** This tool supports the authentication of arbitrary messages (documents) by means of digital signatures with selective disclosure features. This allows a cloud service to pass authentic parts of documents to verifiers and thereby provide privacy features as well as end-to-end authenticity.

**T.4 Topology Certification:** This tool is intended to increase transparency of cloud infrastructure without the provider needing to reveal inner workings of the infrastructure. An auditor component certifies snapshots of infrastructure configurations by means of so called graph signatures. On the basis of such a signature, the provider can then proof certain properties, e.g. isolation, to different customers without revealing internals of the infrastructure.

**T.4 Verifiable Data Processing:** This tool supports the processing of (authenticated) data in way that the result of the processing can be efficiently verified for correctness. Thereby, a cloud component given a set of input data and a description of the processing rule, can output the result of a computation as well as a proof certifying its correctness to a verifier who can check the correctness without requiring all the input data.

*This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 644962.*

Web: http://prismacloud.eu
LinkedIn: https://in.linkedin.com/in/prismacloud
Twitter: https://twitter.com/prismacloud (@prismacloud)
Coordinator Contact: Thomas Lorünser, AIT Austrian Institute of Technology, E-Mail: Thomas.Loruenser@ait.ac.at