prisma cloud

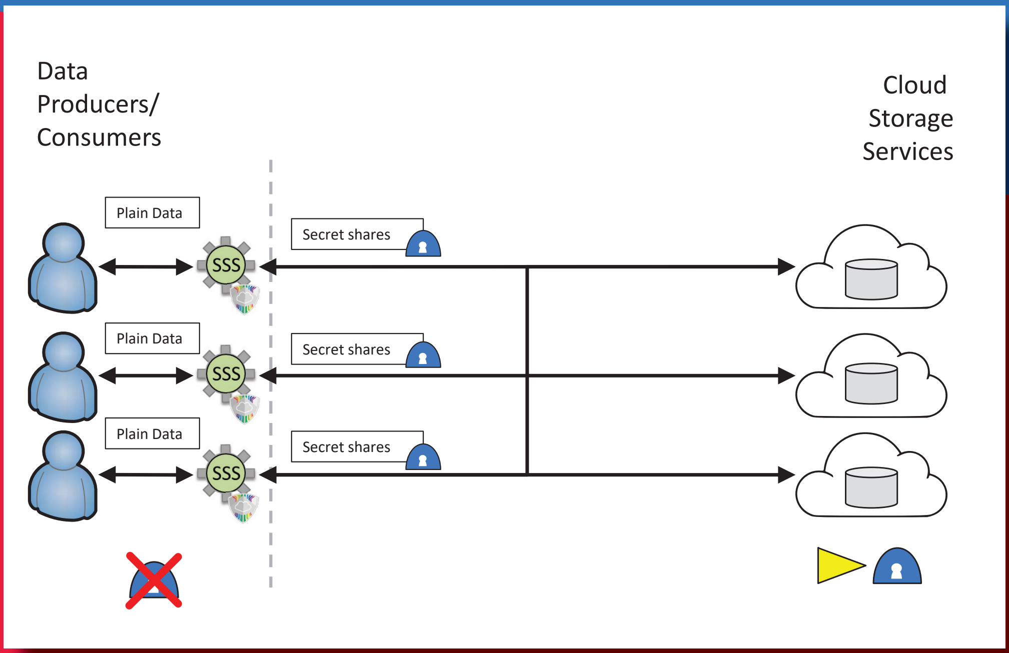
PRIvacy & Security MAintaining Services in the CLOUD

The EU Horizon 2020 PRISMACLOUD - PRIvacy and Security MAintaining services in the CLOUD - research project is dedicated to enabling secure and trustworthy cloud-based services by improving and adopting novel tools from cryptographic research. The project brings novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and make them usable for providers and users.

The main idea and ambition of PRISMACLOUD 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.

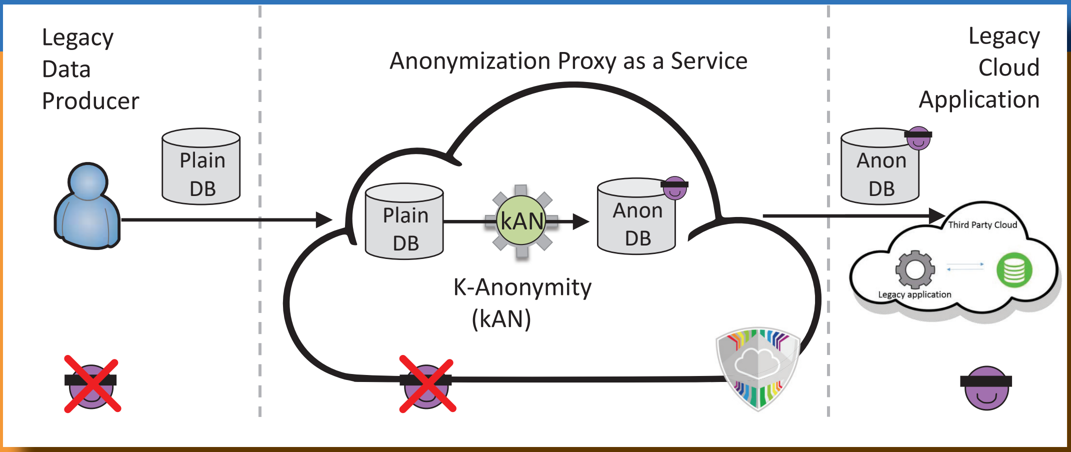
PRISMACLOUD Services

In PRISMACLOUD a portfolio of novel security and/or privacy enhanced services have been developed. Based on the PRISMACLOUD architecture a service can be seen as customization of one particular cryptographic tool (or several particular tools) from the PRISMACLOUD toolbox for one specific from the application scenario. It provides a set of features which has been identified as particularly useful for a broader class of applications scenarios the service is targeting.



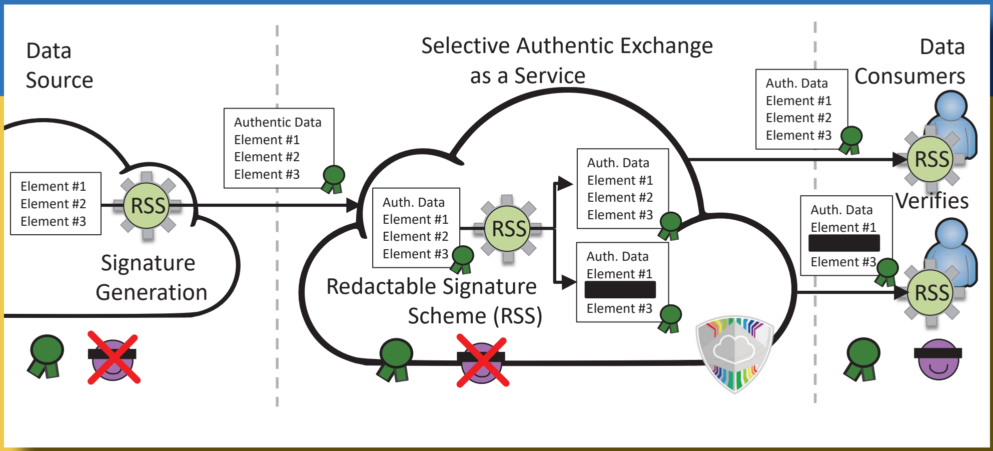
Secure Archiving

- Files selected for archiving get split and then distributed to multiple cloud service providers
- The user no longer has to trust the cloud service provider w.r.t. confidentiality
- The availability of the data can be increased if not all parts of the data are needed for reconstruction
- The proxy nature of the service allows legacy applications to use SAaaS



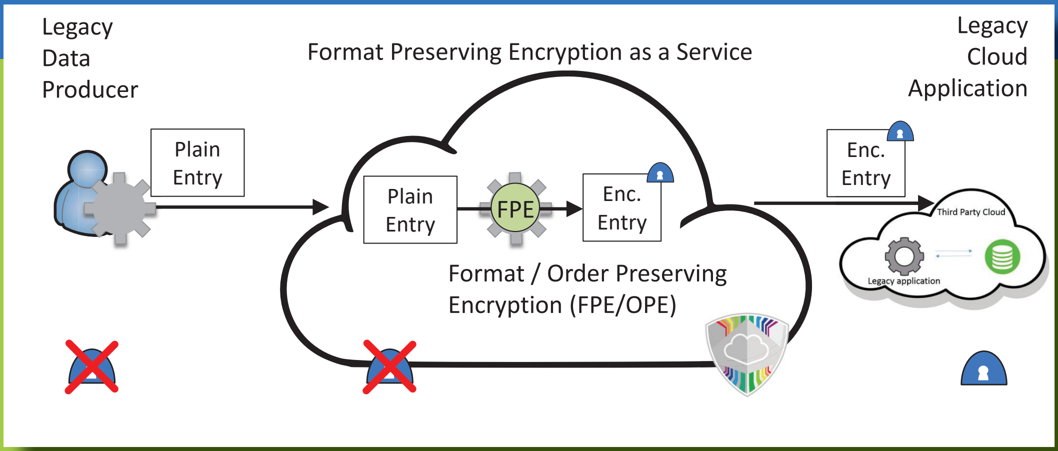
Anonymization

- Plain data stored in a legacy database is analyzed and is obscured enough so no connections between the datasets and the user can be made
- The user's privacy is protected while the cloud service consumer can still make calculations on the obscured data.



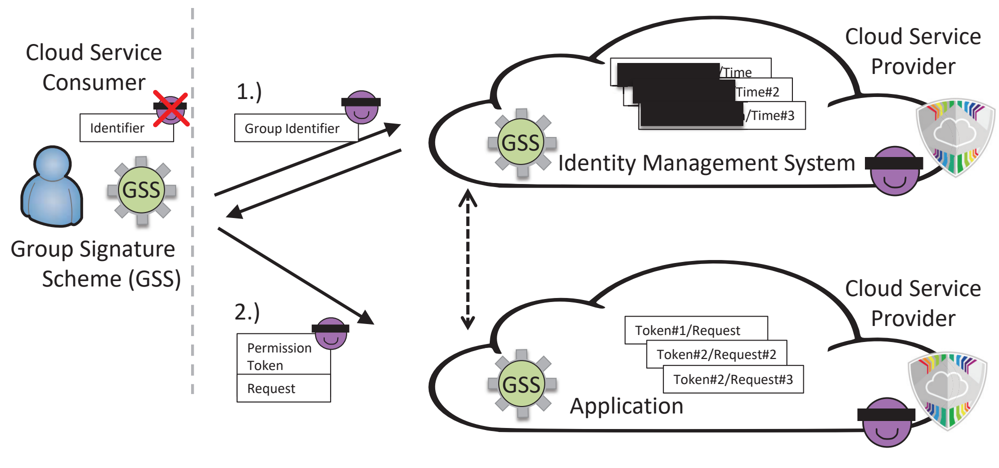
Selective Authentic Exchange

- Documents which were uploaded to the service can be redacted without invalidating the original signature of the document
- Allowing the user to redact signed documents allows them to only share necessary information without sharing too much
- On the flipside, the data consumer can be sure that the data they received were based on a signed document.



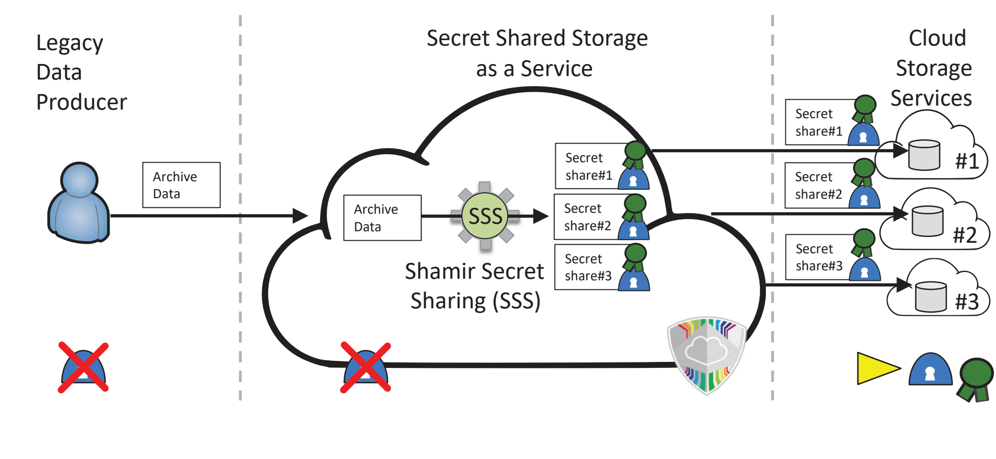
Encryption Proxy

- The data producer sends unencrypted data to the encryption service, which encrypts the data in either an order or format preserving manner and then sends it to the cloud service provider
- When requesting data from the proxy, the request is modified by the proxy to work on the encrypted data, retrieves the requested data from the server and then sends the decrypted data to the cloud service consumer



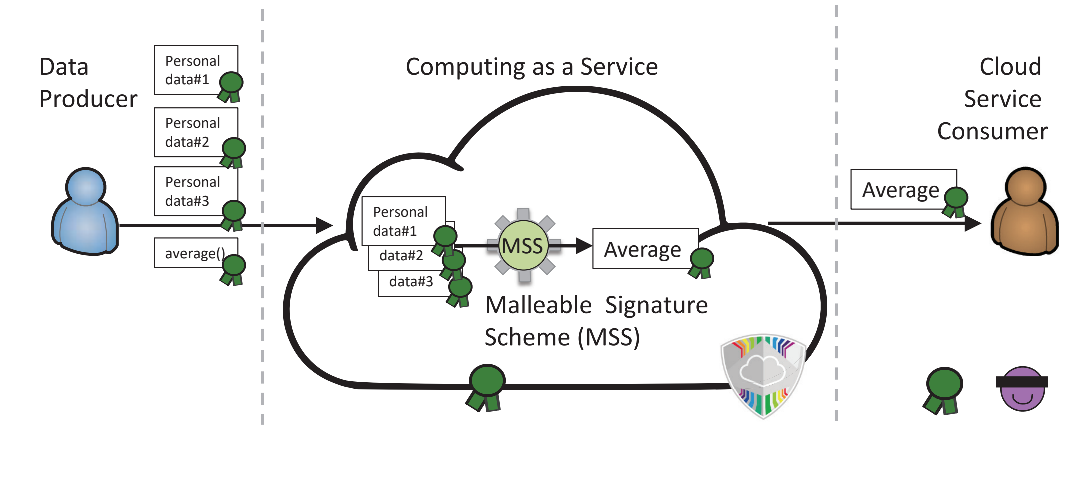
Privacy Enhancing IDM

- Users are granted certain rights depending on the group they belong to
- The service provider does not need to identify the users by ID to be sure they have the rights for certain actions
- Increases trust of the user in privacy protection without impeding the service



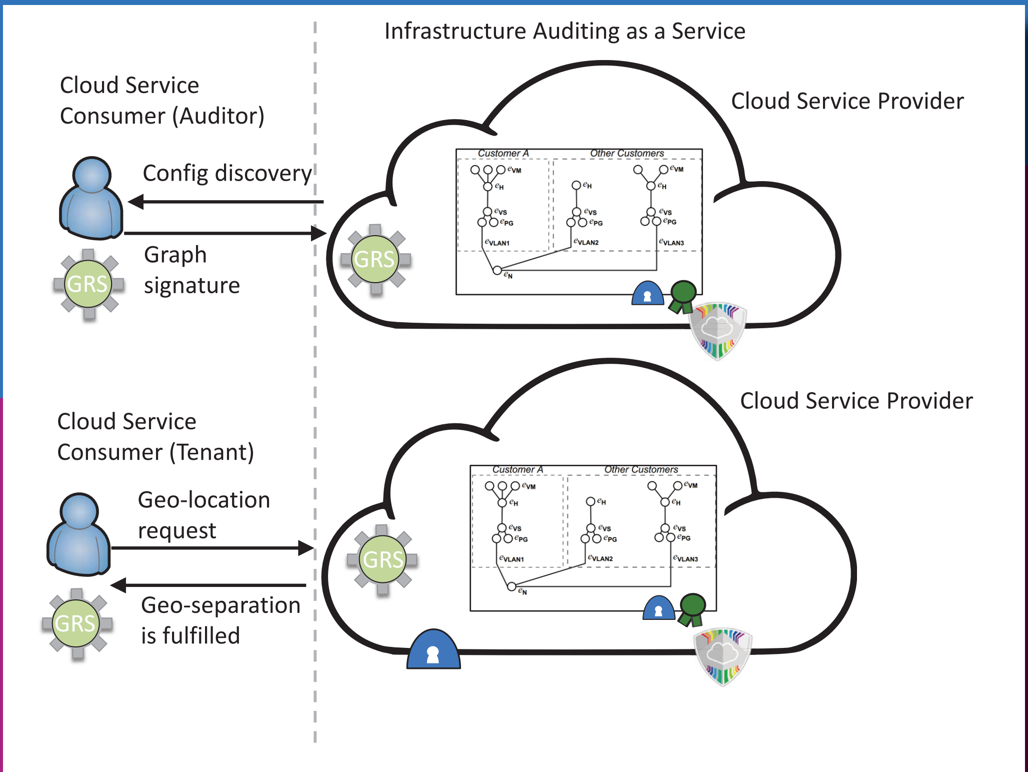
Data Sharing

- Files get split into multiple parts on the users' device
- The parts get sent to multiple cloud service providers
- As with SAaaS, the availability can be increased if not all parts of the data are needed for reconstruction and the cloud service provider no longer has to be trusted w.r.t. confidentiality



Verifiable Statistics

- The data producer sends signed data to the cloud
- The cloud service consumer is then able to retrieve the result of a computation on the original data, which will still have a valid signature, thus proving the result was calculated using the input data.
- The cloud service consumer can validate their results without breaching the privacy of the data producer


Infrastructure Auditing as a Service
Cloud Service Consumer (Auditor)
Config discovery
Graph signature
GRS
Cloud Service Provider
Customer A
Other Customers
Cloud Service Consumer (Tenant)
Geo-location request
Geo-separation is fulfilled
Cloud Service Provider

Infratructure Auditing

- An auditor creates a certificate based on a graph representation of the infrastructure of a cloud service provider.
- The cloud service consumer can then send a challenge request to the cloud service, which can only be fullfilled if the cloud service upholds the requirement
-The cloud service provider no longer needs to grant access to their infrastructure in order to prove that they uphold the requirements

For more information you can find us here:
https://prismacloud.eu/

Partners

IAIK TU Graz
UNIVERSITÄT PASSAU
MIKROPLAN
TECHNISCHE UNIVERSITÄT DARMSTADT
XITRUST SECURE TECHNOLOGIES
LOMBARDIA INFORMATICA
Newcastle University
KARLSTADS UNIVERSITET
interoute from the ground to the cloud
FCSR Fondazione Centro San Raffaele
cea leti
Atos
Unil UNIL | Université de Lausanne
IBM
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
etra I+D
European Commission

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