Brokerage and market platform
for personal data

Understanding Maturity of Data Spaces: KRAKEN SSI and Crypto solutions to data spaces

Data Week 2022 31/05/2022

Juan Carlos Pérez Baún, Atos juan.perezb@atos.net
Sebastian Ramacher, AIT Sebastian.Ramacher@ait.ac.at

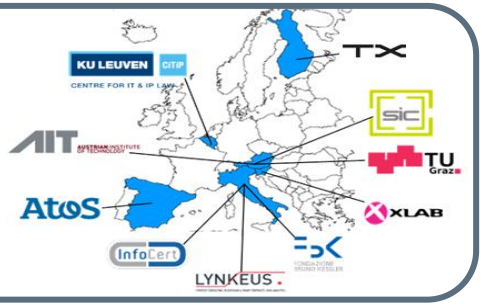
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871473

Online meeting

www.kraken-project.eu

KRAKEN Overview

- EU Horizon 2020 R & I programme under grant agreement No 871473
- Innovation Action
- From December 2019 to November 2022
- 10 Partners



BDV BIG DATA VALUE ASSOCIATION

GOAL

Removing obstacles which prevent citizen's controlling and widely sharing their personal data by implementing a highly trusted, secure, scalable and efficient personal data sharing and analysis platform adapting state-of-the-art technologies

KRAKEN SOLUTION

SSI: Provides user-centric access control to data. The data owner controls their data

Crypto: Enable a data-analytics-as-a-service platform integrated with the marketplace. Ensure end-to-end secure data sharing (confidentiality and authenticity)

Marketplace: Open and decentralised exchange system connecting data providers and data consumers, leveraging a blockchain network facilitating the business and legal logic on data transactions

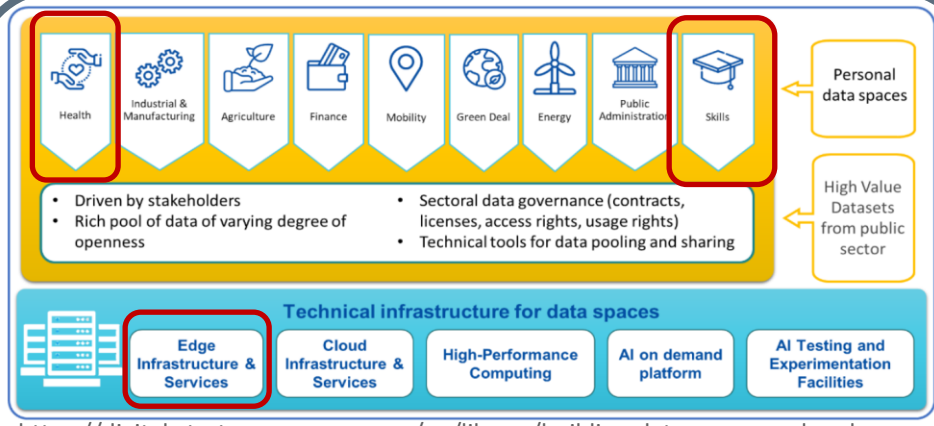
KRAKEN & Data Spaces

"Data spaces are central to the European strategy for data. The strategy envisages 'a European data space as a genuine single market for data where personal and non-personal data, including sensitive business data, are secure and businesses have easy access to high-quality industrial data, boosting growth and creating value'."

data.europa.eu and the European Common Data Spaces: A report on challenges and opportunities
https://data.europa.eu/sites/default/files/report/EN_data_europa_eu_and_the_European_common_data_spaces_0.pdf

CHALLENGES

- Data can flow within the EU and across sectors
- Privacy and data protection fully respected (EU rules)
- Rules for Access and use of data ser fair, practical and clear
- Build data economy



https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure

INITIATIVES

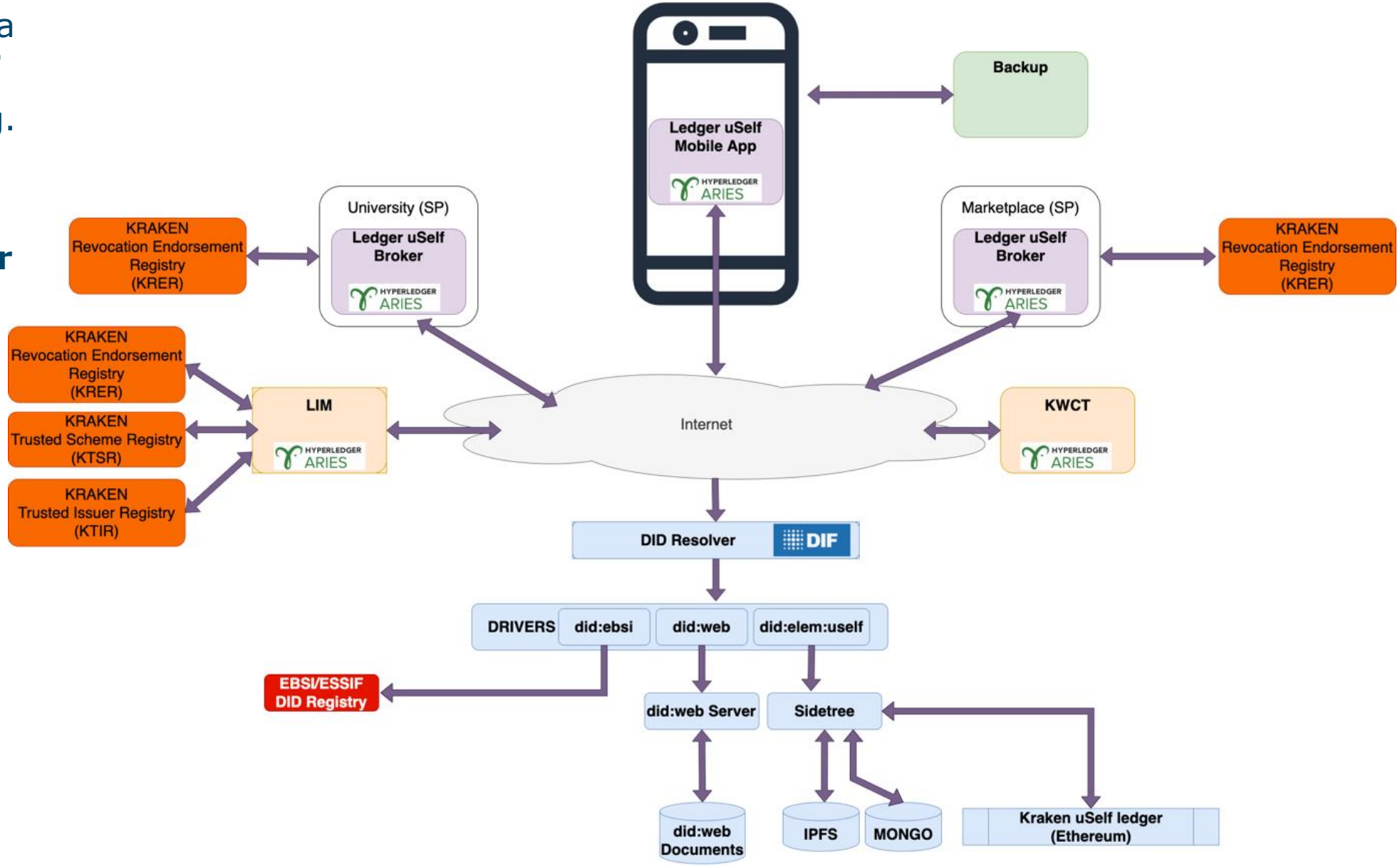
- IDSA
- Gaia-X
- Open DEI

- **Provide decentralized SSI solutions and user centric access control.**
- **Cryptographic tools for:**
  - **Secure end-to-end data sharing**
  - **Authenticity and confidentiality of data analytics**

- **Privacy metrics and usable interfaces.**
- **Ethical and legal framework**
- **Economic value and innovative business models for personal data spaces**
- **Piloting two domains: Health and Education**

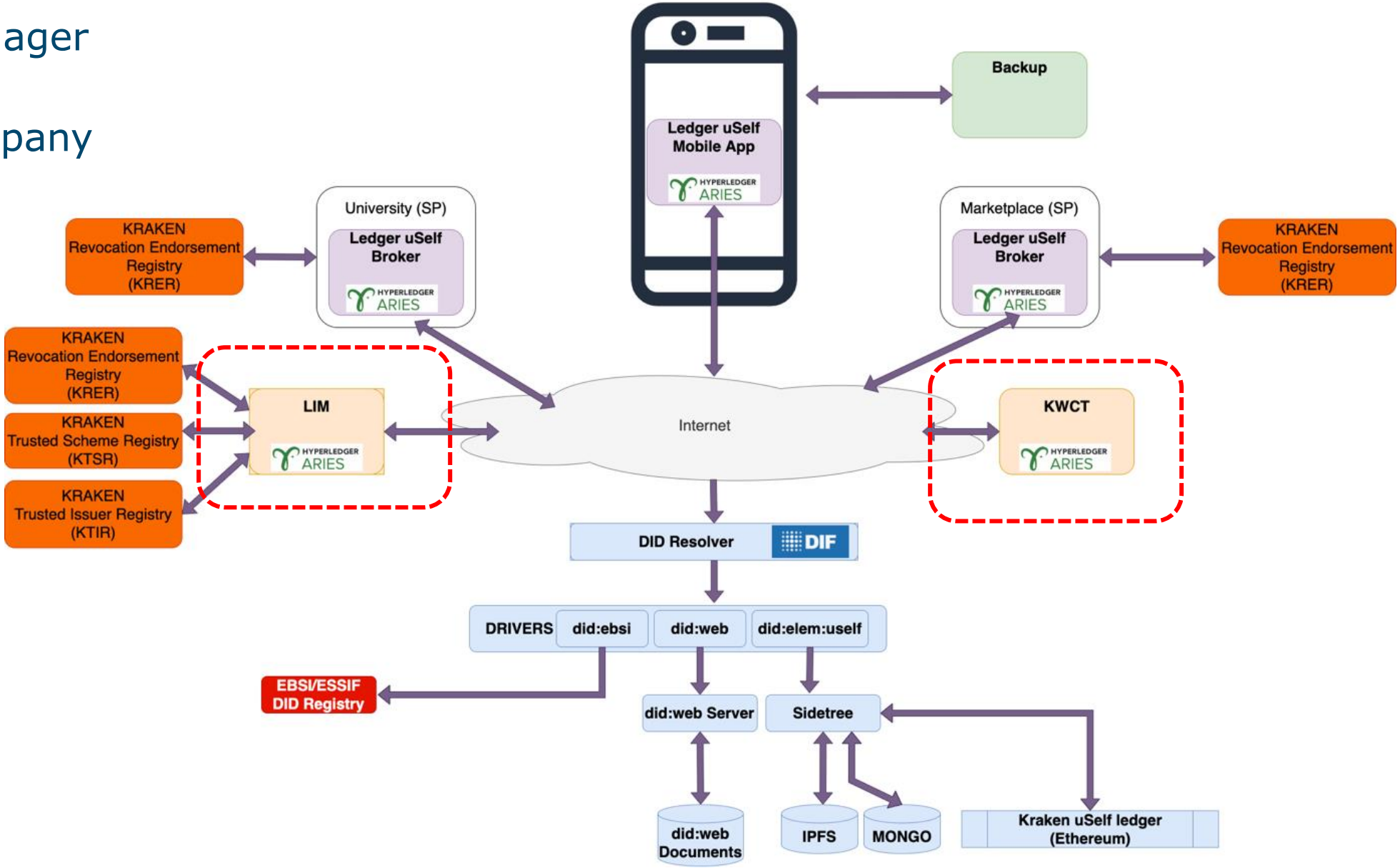
SSI solution

- Use of SSI providing a **decentralized user-centric** approach on personal data sharing.
- **SSI mobile app** for managing VCs and key material.
- **Ledger USelf broker** for SP integration.
- VCs with different **level of assurance** for accessing the services the platform provides.
- LIM creates VCs based on eIDAS network identity info.
- **Backup service** allowing the use of several devices. Device lost or stolen.
- Trust framework to **ESSIF/EBSI alignment**.



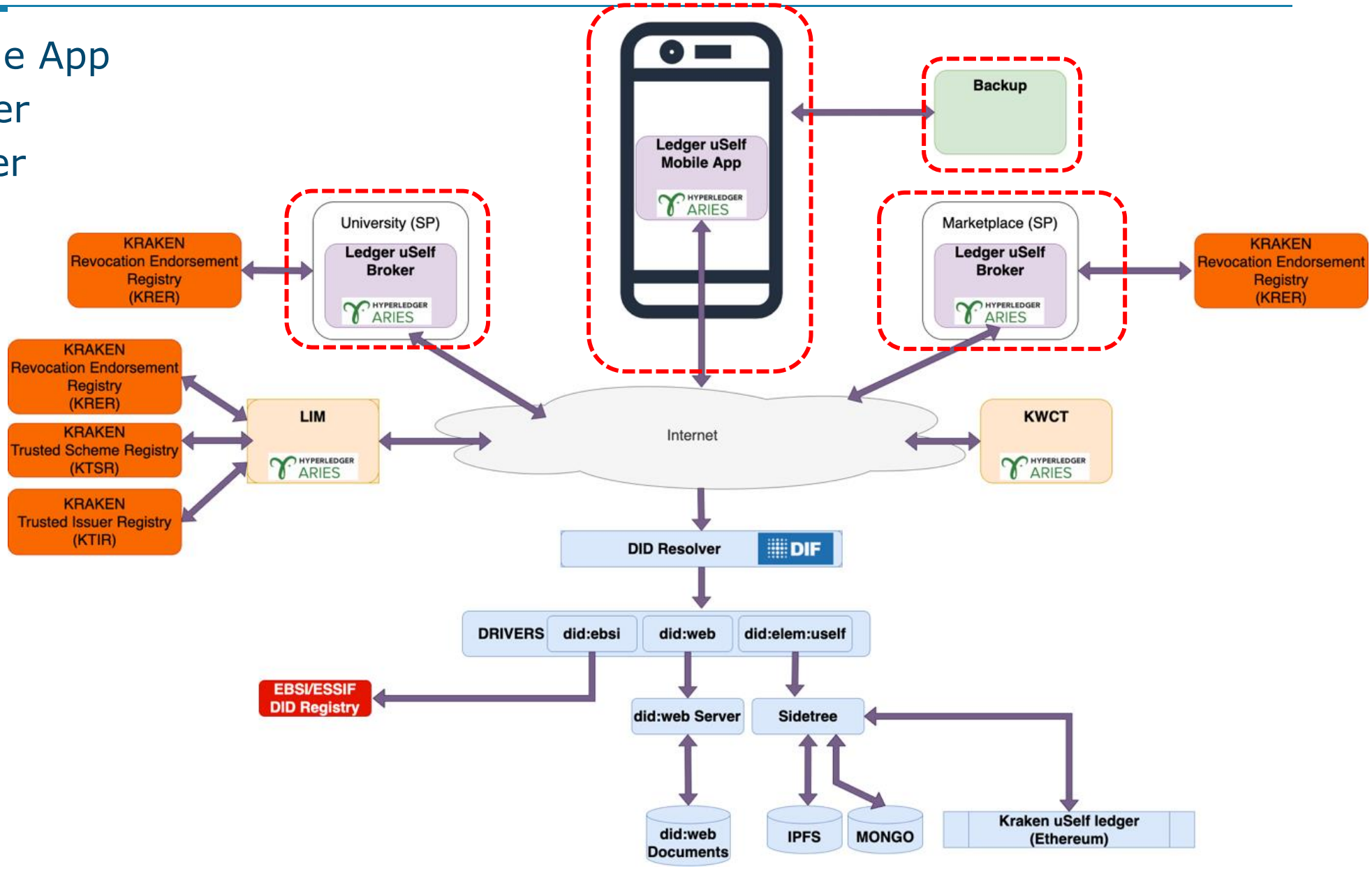
SSI Verifiable credential management tools

- Legal Identity Manager (LIM)
- KRAKEN Web Company Tool (KWCT)



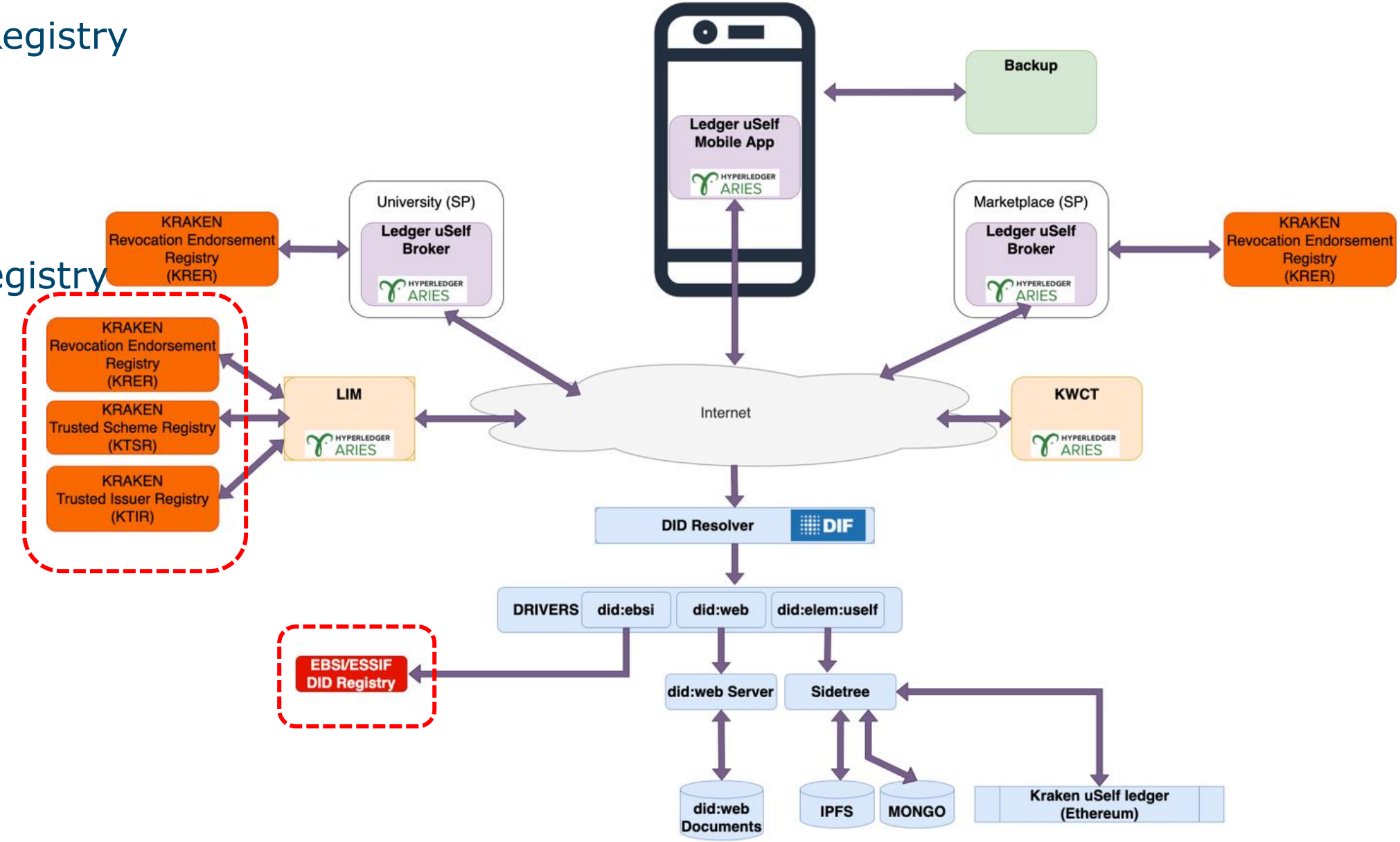
SSI Edge Tools for the Decentralised Identity Solution

- Ledger uSelf Mobile App
- Ledger uSelf Broker
- SSI Wallet Manager



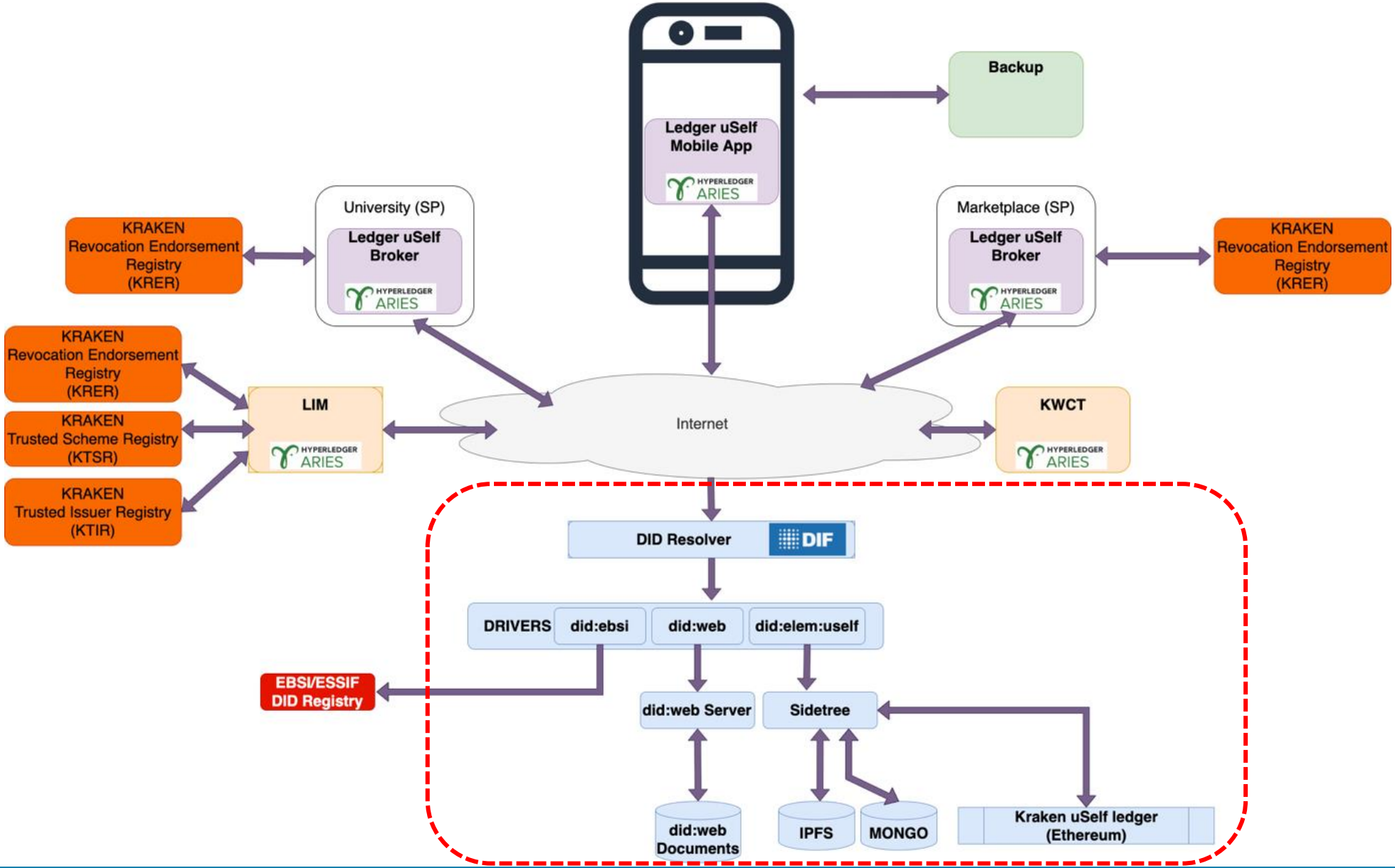
SSI Trust Framework

- Trusted Issuer Registry (KTIR)
- Trusted Scheme Registry (KTSR)
- Revocation & Endorsement Registry (KRER)
- DID Registry



SSI DID Infrastructure

- DID Universal Resolver
- DID Web server
- Sidetree server



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

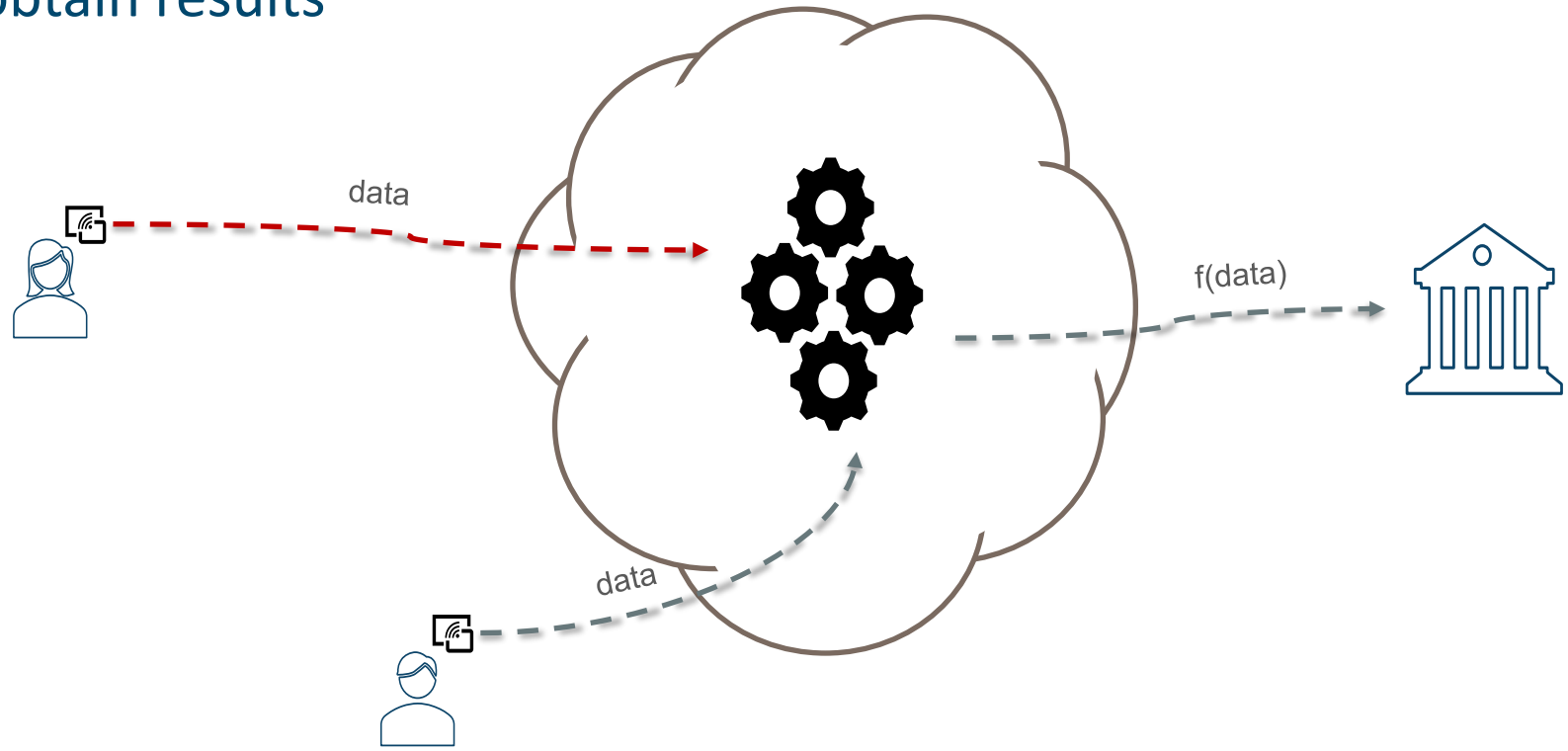
CRYPTOGRAPHIC ARCHITECTURE FOR DATA MARKETPLACES

Privacy and Authenticity

MOTIVATION

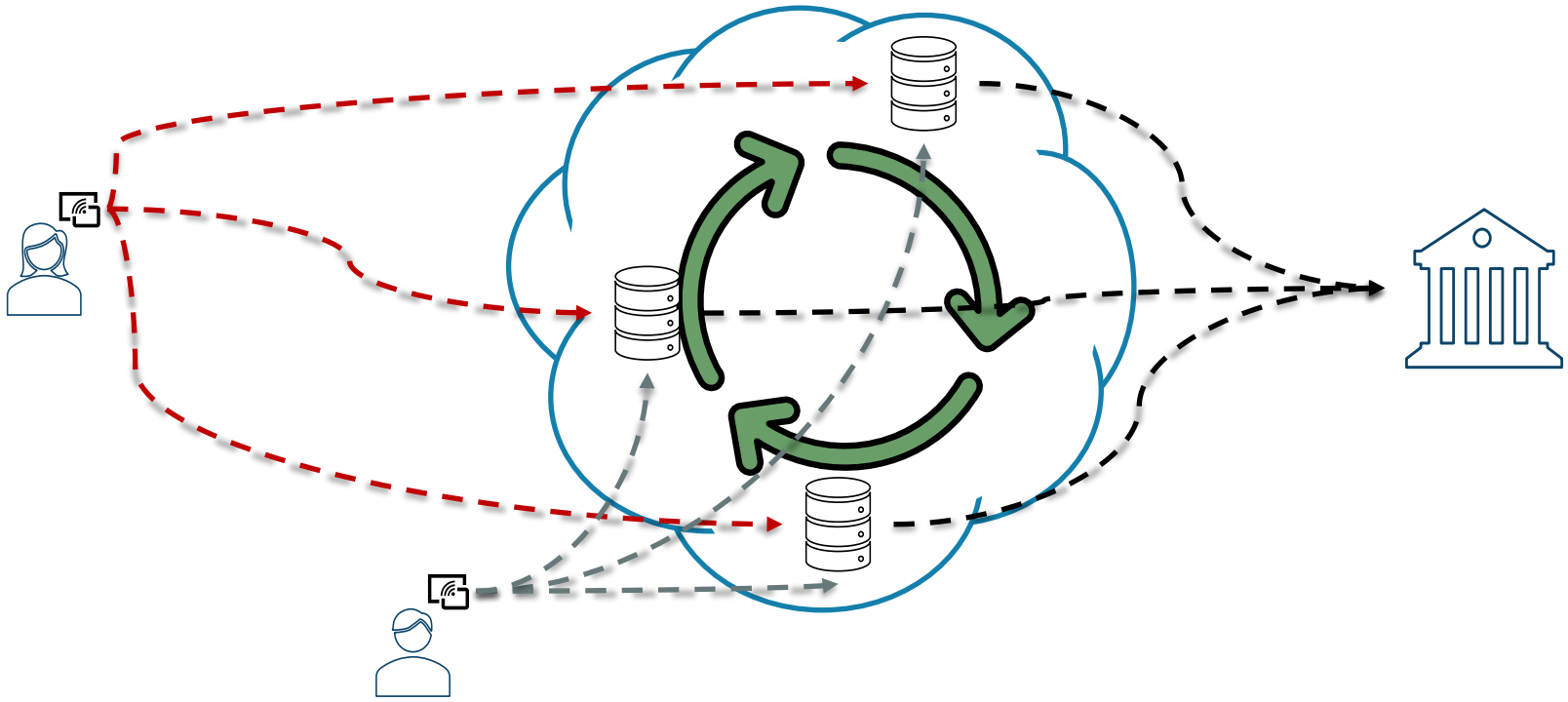
- Data sets available from multiple producers
- Combine these data sets and sell combined statistics
- Consumers should only obtain results

- **Privacy?**
- **Authenticity?**

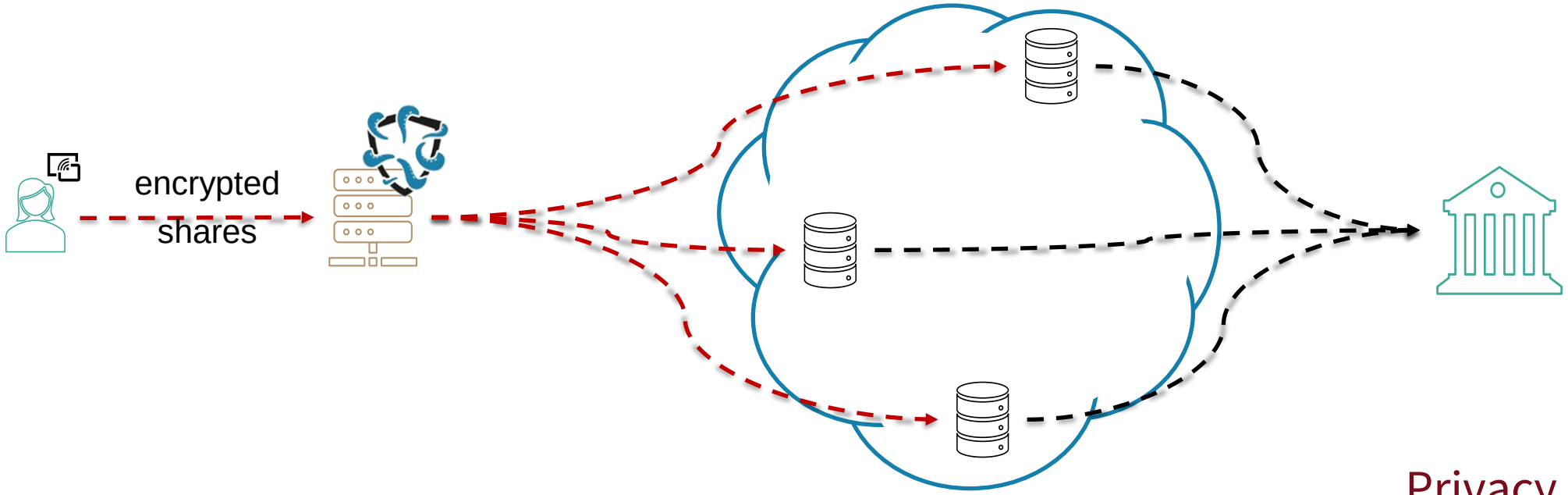


Secure Multi-Party Computation (SMPC)

- Protocols for jointly computing on data
- Parties keep their input data private



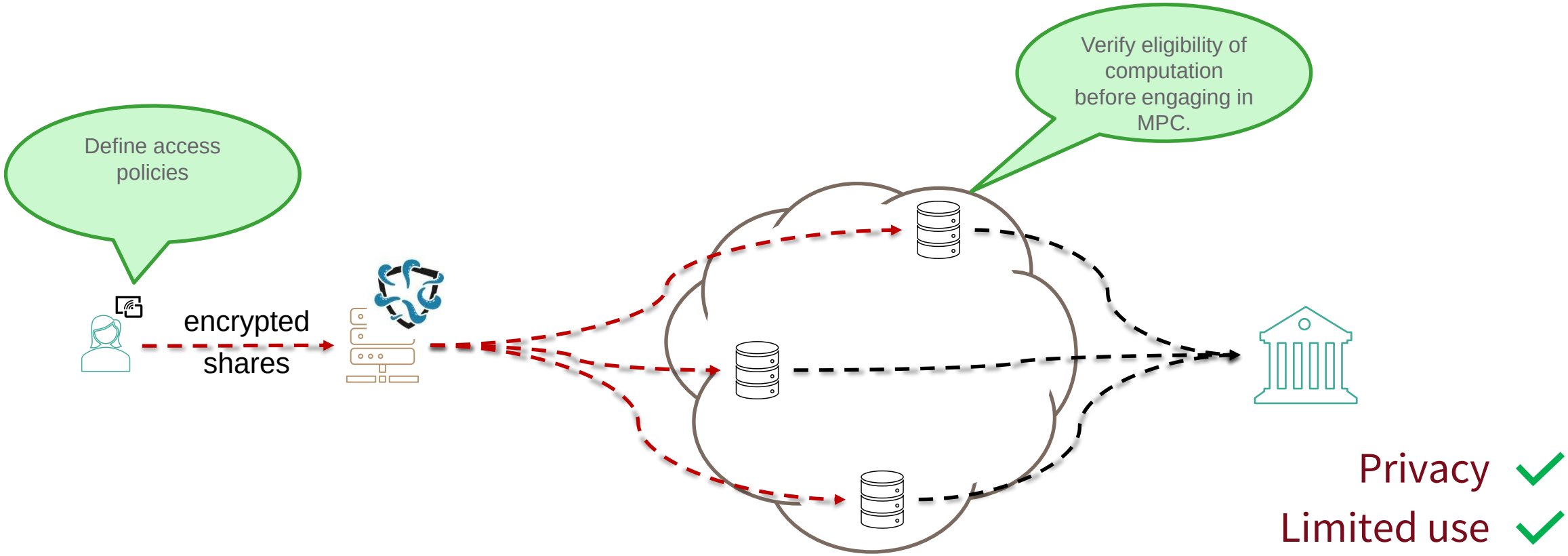
A MARKETPLACE ARCHITECTURE



Privacy ✓

But… I want to restrict the computations my data is used for!

A MARKETPLACE ARCHITECTURE



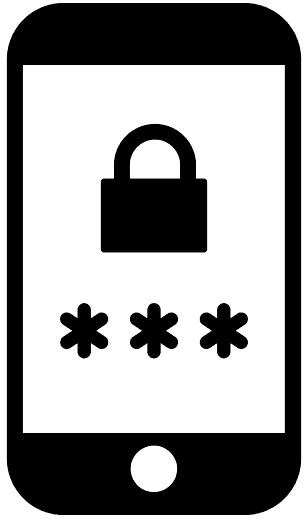
Privacy ✓

Limited use ✓

But… are there any authenticity guarantees?

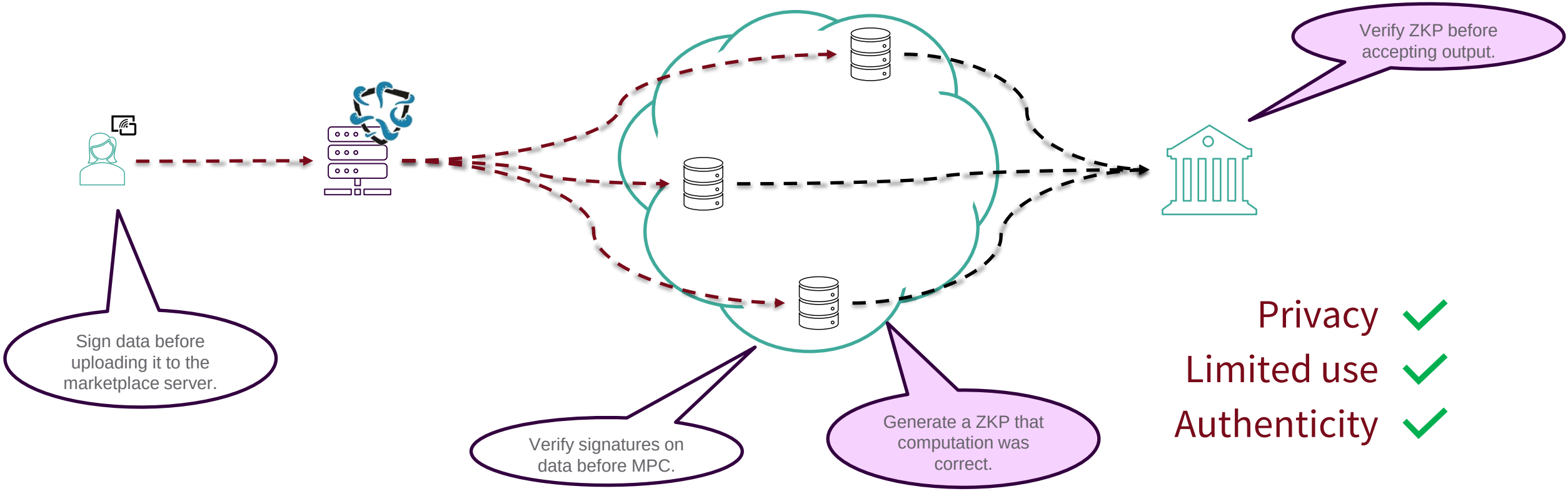
ZERO-KNOWLEDGE PROOFS

- Allows to prove knowledge of a certain piece of information without revealing it.



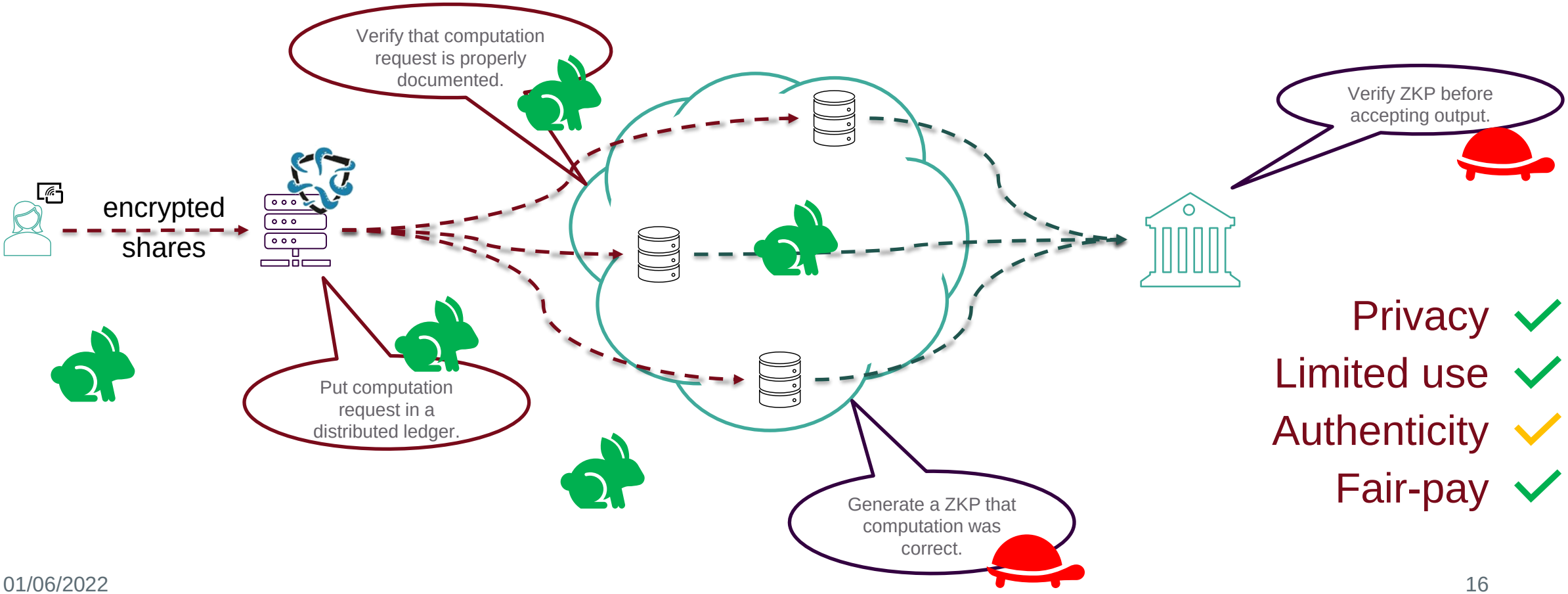
- Also: ensures correctness of computation

A MARKETPLACE ARCHITECTURE



Privacy ✓
Limited use ✓
Authenticity ✓

A MARKETPLACE ARCHITECTURE



KRAKEN

Thank you for your attention !

<< Juan Carlos Pérez Baún >>

<< juan.perezb@atos.net>>

<< Sebastian Ramacher>>

<< Sebastian.Ramacher@ait.ac.at>>

@KrakenProject

Kraken Project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871473

www.kraken-project.eu