SECURITY IN DATASCAPES

- Juan Carlos Pérez Baún (Atos)
  juan.perezb@atos.net
Security in data spaces Overview

Use Case in KRAKEN project
Security in data spaces Overview

Use Case in KRAKEN project
Security in data spaces Overview

“The term ‘data space’ refers to a type of data relationship between trusted partners who adhere to the same high-level standards and guidelines in relation to **data storage and sharing** within one or many Vertical Ecosystems.” (Gaia-X)

- **“Security-by-design**, i.e., security of data space assets and support of non-repudiable and unambiguous agreements.”
- **“Assurance-by-design**, i.e., integration of security and privacy assurance requirements in the development of data platforms and data-sharing applications.” (OPENDEI)
- Common framework for the **federation of security management** (OPENDEI)

**European Commission** promotes initiatives for the development of secure and sustainable digital infrastructures, such as Gaia-X, for developing an open, federated and interoperable data infrastructure in the cloud, and the International Data Spaces Association (IDSA), among others.

Data spaces must be secured and controlled environments. The **data exchange** must carry out in a safe and secure way, adopting **security schemas** to protect data.
Data Spaces building blocks

**Soft infrastructure**

How do participants interact in and between spaces (solution neutral). General building blocks that are harmonised for each data space. Not all services are obligatory to each case.
Security in data spaces Overview

Use Case in KRAKEN project
Use Cases in KRAKEN project

**KRAKEN goal**
Provide a decentralized SSI solution and user centric access control.

- **SSI mobile app** for managing VCs and key material
- **Ledger uSelf broker** for SP integration
- **Backup service** allowing the use of several devices
KRAKEN Use Case 1: The data owner sells data

Use case 1 Health
THE DATA OWNER (INDIVIDUAL/ORGANIZATION) SELLS HIS/HER DATA

Citizens, institutions, and organizations are enabled to offer protected personal and sensitive data (biomedical data and well-being records).

The Data Providers are able to sell their data setting the user consent, the price of download and defining the conditions of access and use of their data.

The marketplace shows a catalogue with the available datasets and the Health marketplace. Before the dataset price, the marketplace through the use of smart contracts stores the user consent for sharing data and the access criteria.

Data Providers can register and access to the marketplace by using SSI solutions, a SSI mobile app stores Verifiable Credentials (VC) and key material for accessing the marketplace.

The user can execute their right to be forgotten in accordance with the GDPR.

Through the Marketplace App, the Data Providers are able to control their account and track who is accessing the data.

The data can be used by food product manufacturers, health insurance companies or biomedicine product companies interested in certain lifestyle and demographics for monitoring or product development purposes.
THANK YOU!!

juan.perezb@atos.net