KRAKEN - Brokerage and Market Platform for Personal Data

By Andreas Abraham (Graz University of Technology), Juan Carlos Perez Braun (Atos Spain S.A.), and Sebastian Ramacher (AIT Austrian Institute of Technology

The EU Horizon 2020 KRAKEN project is dedicated to building a trusted and secure personal data platform enabling exchange and analytics of personal data

Data sharing platforms are facing several challenges in terms of security, privacy, trust, and regulatory compliance. In order to address these challenges, the KRAKEN (Brokerage and market platform for personal data) project [L1, L3] aims to develop a trusted and secure personal data platform with the state-of-the-art privacy aware analytics methods, guaranteeing metadata privacy and query privacy, empowering the citizens on the control of their own personal data, including sensitive data and motivate the user to share this kind of data.

KRAKEN provides a highly trusted, secure, scalable and efficient personal data sharing and analysis platform that is relying on Self-Sovereign Identity services and cryptographic tools for covering the security, privacy and user control on data. Also, investigating data processing mechanisms working in the encrypted domain with the aim to increase security, privacy, functionality and scalability for boosting trust.

KRAKEN is based in three main pillars:

- The Self-Sovereign Identity paradigm providing a decentralized user-centric approach on personal data sharing. KRAKEN is returning the control of personal data back into the hands of data subjects and data providers and its subsequent use, which includes the user consent management.
- A set of different analytics techniques that KRAKEN will develop are based on advanced cryptographic tools that will permit privacy-preserving data analysis, end-to-end secure data sharing and confidentiality of privacy-sensitive data.
- A data marketplace will allow the sharing of personal data in a preserving-privacy manner when Artificial Intelligence/Machine Learning analysis is performed. Additionally, to motivate the user to share their data, the developing of fair-trading protocols and incentive models is envisaged, establishing economic value and innovative business models for “personal data spaces”.

As personal and sensitive data are managed and shared, KRAKEN provides an ethical and legal framework for accomplishing the General Data Protection Regulation [L2] and eIDAS compliance, following standards for compatibility and interoperability, and promoting best practices.

The health and education domains were selected for demonstrating how SSI and cryptographic technologies can improve the security and privacy of personal data, including sensitive data when shared in a marketplace. The health scenario involves sensitive data such as biomedical and well-being data, which implies the use of powerful privacy-preserving techniques assuring the data are protected all times. The education scenario involves personal data such as grades, courses or diplomas, which can be provided to a third party in a privacy-preserving way. In both cases, the use of SSI and cryptographic technologies ease the shared use of these data assuring the data are protected and the owner has the control over the use of the data. Finally, the aim is to generalize the KRAKEN experience to other economic domains (Figure 1).

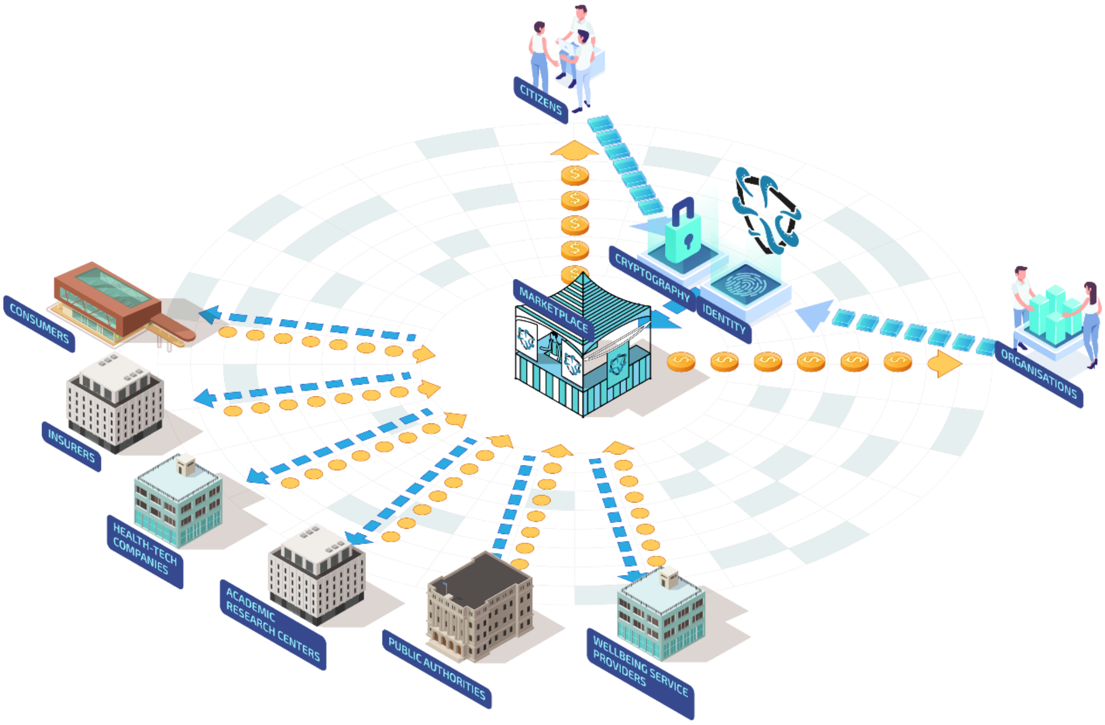

Figure 1: The KRAKEN data marketplace provides opportunities for various data owners and stakeholders to exchange data and analytics for monetary compensation

Computation Platform. The core primitive leveraged by the platform is secure multi-party computation [1] which allows nodes to jointly perform a computation without each node learning the input data of the other nodes. Data providers can decompose their data into fragments such that no single fragment contains any information about the original data. For each data item, each node is then granted access to one of the shares, and the nodes can jointly perform analytics, compute statistics, or answer queries from consumers, without learning the individual data provider's data as long as a single node behaves honestly. In addition to secure multi-party computation, KRAKEN deploys further privacy-enhancing technologies such as group signatures and zero-knowledge proofs to ensure that data consumers receive strong and undeniable cryptographic evidence about the correctness of the received results.

KRAKEN's design also allows data providers to apply fine-grained policies to their data that specify which computations may and may not be performed on their data. These policies are checked by the nodes before participating in any further computation, thereby avoiding potential misuse through unauthorized consumer requests. The result is a cryptographically secured and feature-rich market platform that achieves an unprecedented level of privacy for personal input data.

Self-Sovereign Identity. KRAKEN further utilizes the recent Self-Sovereign Identity technology addressing the digital identity aspect in the project. Digital identities are required for users to identify and authenticate towards service providers. Digital identities are often based on central authorities where users are not in full control over their data. Self-Sovereign Identity systems tackle these issues by utilizing technologies such as the distributed ledger technology to address the central authority.

KRAKEN will enhance the state-of-the-art of the SSI technology for different aspects. One of these aspects is that KRAKEN will enable the privacy-preserving identity attribute showing [2]. This is especially interesting in case a user wants to reveal only a subset of their identity attributes to service providers. Additionally, SSI systems lack identity data with legal background, i.e., qualified identity data issued by trust service providers operating in traditional identity systems which do not support SSI paradigms. Thus, KRAKEN will develop an efficient and privacy-preserving way to derive existing identity data into an SSI-based identity system. Zero-knowledge proofs are utilized to achieve this objective and further elevate the level-of-assurance in the identity data used within the SSI system.

The KRAKEN project has been running since December 2019 and is a 36-month project that receives funding from the European Union’s Horizon 2020 Research and Innovation programme under grant agreement No 871473. The project is coordinated by Atos and its consortium consists of ten partners from academia and industry from six different countries.

Links:

[L1]: https://krakenh2020.eu/

[L2]: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[L3]: https://cordis.europa.eu/project/id/871473

References:

[1]: Karl Koch, Stephan Krenn, Donato Pellegrino, Sebastian Ramacher: Privacy-preserving Analytics for Data Markets using MPC. In: Privacy and Identity Management 2020, Springer IFIP AICT 619. (to appear)

[2]: Andreas Abraham, Felix Hörandner, Olamide Omolola, Sebastian Ramacher: Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems. ICICS 2019

Please contact:

Sebastian Ramacher
AIT Austrian Institute of Technology,
Vienna, Austria
sebastian.ramacher@ait.ac.at