Brokerage and market platform for personal data

KRAKEN project: Final delivery

Europe, 22/12/2022 – November 30th was the official last day of the **KRAKEN project**. When the 10 KRAKEN partners (Atos, AIT, FBK, ICERT, KUL, Lynkeus, SIC, TEX, TUG, XLAB) met in Madrid in December 2019, an exciting, promising and demanding journey was ahead of us. Then in March 2020 a pandemic transformed our lives and project meetings turn to be online instead of physical meetings. This additional challenge made us more resilient and with new energy for addressing the technical, privacy, security, ethical, legal and business challenges. During these three years a huge and hard work has been performed by the KRAKEN partners, for delivering the KRAKEN platform based on 3 main pillars, the Self-Sovereign Identity, Advanced Cryptographic Tools and the Marketplace. Legal and ethical recommendations were applied during the implementation process, and business and exploitation plans has been performed for the future of the KRAKEN outcomes.

The KRAKEN main achievement reached (as planned) is the implementation of a highly trusted and secure yet scalable and efficient personal data sharing and analysis platform through adaptation of state-of-the-art technologies. In this way the KRAKEN platform:

- Integrates a SMPC service for analytics
- Integrates a SSI solution for onboarding and login to the Marketplace and University using a mobile digital wallet
- Integrating also, privacy metrics on the published data, and applying usability principles.
- During the implementation process follows W3C standards and regulatory guidelines for being GDPR compliant.
- Has been demonstrated in 4 health and 3 education use cases, but the lessons learnt could be applied to other domains.
- Integrates blockchain for payment transactions, and the business model is based on pay per access to data and per computation, following a dynamic price structure.

It's time to highlight the main points and work made by the different KRAKEN dimensions helped to achieve this main goal.

SSI dimension

Regarding the Self-Sovereign Identity (SSI) paradigm, KRAKEN provides a decentralized user-centric approach on personal data sharing. The user has full control of data and able to **manage Verifiable Credentials** (VCs) and key material by using a **SSI mobile app**. The service providers (SPs), in this case the marketplace and the university leverage the SSI solution integrating the **Ledger uSelf broker**. The VCs issued by the SPs can have different level of assurance, namely the **Legal Identity**

Manager creates VCs from the eIDAS network, being able to sing pdf documents. An interesting aspect is the integration of a backup service which allows the use of several devices by the same user and recover the VCs and key material in the case of the mobile is lost or stolen. Finally, the KRAKEN platform is aligned with ESSIF/EBSI framework (created by EC) setting up a **trust framework**.

Cryptographic dimension

The the cryptographic tools have been integrated into the marketplace:

- **Secure Multy-Party Computation** (SMPC) for performing analytics on published products and nodes deployment
- **The homomorphic proxy re-authenticator** (HPRA) for key sharing
- **The Group Signatures** (GS) for signing data
- **The Zero-Knowledge Proof** (ZKP) data verification for authenticate data without revealing the data itself. ZKP is combined with MPC nodes to authenticate the shared data

The user's access to the crypto functionalities offered by the marketplace, such as the key sharing and the MPC data management, is possible by JS/webAssembly mechanisms. Also, the crypto team provided guidelines for a secure cryptographic implementation.

Marketplace dimension

Finally, these two technologies (SSI and advanced crypto tools) are used by the marketplace which developed a **backend** for handling operation requests made by the users through the **frontend**. The marketplace Includes a **catalogue database** for storing Data Product's metadata; the users' account and the VCs. Use of **Smart contracts** for publishing and purchasing Data Products on the **xDai blockchain**, and **xDai watcher** for registering events related to data products (publish/modify). Also, **Data Union** (DU) are engaged for aggregating data, generated by the DU members, in a single product to be monetised by using DU smart contracts which facilitates the one-to-many payment. The marketplace leverages a **P2P network** for publishing and subscribing to Data Union Data Product in real-time and a **Consortium Blockchain Network** for handling the catalogue, user data and policies for controlling the data access. A **marketplace mobile app** allowing users to manage basic functionalities has been developed. Also, the marketplace integrates **tools for managing natural persons acting on behalf of a company**.

Ethical dimension

During the life of the project the legal team has been assessing the design and implementation process for assuring that the final KRAKEN platform would be GDPR compliant. Providing support for simplifying the understanding of the users about their obligations and rights, and how to correctly share the data. The use of the platform revealed that most participants in the evaluation process found the information on data protection and privacy provided by KRAKEN as sufficiently clear and complete.

Business and exploitation dimension

During the 3rd year of the project KRAKEN team has been working on the preparation of the final market analysis including the most important trends, solutions how the actual players addressing the needs. The analysis focused on Healthcare and Educational market, provides interesting information on target, value proposition and monetization model. The analysis shows KRAKEN platform in a good position.

Additionally, the exploitation plan for the KRAKEN platform and its components is provided. Also, be able to monetize access to highly valuable data assets, enhance security in data sharing, provide an easy way to guarantee GDPR compliance, and empower data providers to connect directly with data consumers without intermediaries.

Communication, dissemination and standardization dimension

The communication and dissemination activities exceed the initial expectations. Namely KRAKEN achieved the following figures:

- More than 600 followers in Twitter and LinkedIn, with more than 77,464 impressions per month.
- KRAKEN web site received more than 7,000 visitors.
- Delivering 5 newsletters and 3 press releases and 7 infographics as communication and promotional material.
- Delivering 12 non-scientific technical publications.
- Publishing more than 20 publications in conferences and 2 articles in journals.
- Collaborating with 22 R&D initiatives for contributing to building blocks of data spaces.
- Producing 27 scientific publications and carry out 2 theses.
- Following standardization bodies relevant to KRAKEN, such as ISO/IEC, ETSI, ITU-T, IETF, W3C, ZKProof.
- Contributing to standardization bodies: ISO/IEC JTC1-SC27-WG2 and ZKProof WG Sigma protocols.

Validation dimension

During the last months has been conducted the second round of evaluation involving key target user groups in both domains health and education. The main findings indicate that the KRAKEN platform usability is OK/Fair and reaches a marginal level of acceptance. Most of them expressed interest and trust in using the data sharing solution, both as providers and consumers of data products. Testers consider the service provided by KRAKEN platform for sharing data analytics products (by SMPC) as an added value of KRAKEN, as it ensures security and privacy of the shared data.

EC acknowledge

The following innovative assets delivered by the KRAKEN partners, contributing to secure and privacy data sharing, have been analysed by the European Commission's Innovation Radar and selected as innovations.

- *Ledger uSelf, tool for the integration of SSI with the Service Providers*[1] innovator by Atos.
- *Cryptographic Service Provider for Group Signatures*[2] innovator by SIC.
- *Identity credential derivation from eIDAS identity*[3] innovator by ICERT.
- *Privacy-Preserving Analytics (PPA)*[4] innovator by XLAB.
- *Backup-and-Synchronization Service in SSI leveraging Proxy Re-Encryption*[5] by TUG.
- *(Qualified) Digital signature based on personal identity wallet. Market maturity: Exploring*[6] innovator by ICERT.
- *HPRA Key Sharing Process for asynchronous Key Sharing*[7] innovator developed by 3 KRAKEN partners AIT, SIC and XLAB.
- *Responsible data marketplaces using SMPC for privacy-preserving analytics*[8] by TEX.

The acceptance by the EC of this high number of innovators produced during the KRAKEN project means a great recognition of the work done by the KRAKEN consortium.

I would like to highlight a final achievement made during these last days, KRAKEN provides a public stand-alone MPC component[9], which allows deploying a multi-party computation service. This service needs minimal effort to be deployed (not only locally, but also over WAN), since it is fully dockerized. It means that outcomes from the KRAKEN platform can be used by others contributing to extend the KRAKEN life.

As can be seen the work performed by the KRAKEN project is recognized by the users and the EC. As KRAKEN coordinator I'm very proud of leading this amazing team and I appreciate the work and effort dedicated by all the KRAKEN team members for reaching these successful achievements along these 3 years.

THANK YOU.

---

[1] https://www.innoradar.eu/innovation/44378

[2] https://www.innoradar.eu/innovation/44379

[3] https://www.innoradar.eu/innovation/44380

[4] https://www.innoradar.eu/innovation/44381

[5] https://www.innoradar.eu/innovation/44382

[6] https://www.innoradar.eu/innovation/44383

[7] https://www.innoradar.eu/innovation/44384

[8] https://www.innoradar.eu/innovation/44387

[9] https://www.krakenh2020.eu/news/stand-alone-mpc-component