KRAKEN

BROKERAGE AND MARKET PLATFORM
FOR PERSONAL DATA

D6.11 Third Advisory Board

www.krakenh2020.eu

This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 871473

D6.11 Project Advisory Board report

Grant agreement	871473
Work Package Leader	InfoCert
Author(s)	Silvio Di Virgilio (ICERT)
Contributors	Romualdo Carbone (ICERT), Davide Porro (ICERT), Giancarlo Degani (ICERT)
Reviewer(s)	Juan Carlos Pérez Baún (ATOS), Davide Zaccagnini (LYNKEUS)
Version	Final
Due Date	30/11/2022
Submission Date	30/11/2022
Dissemination Level	Public

Copyright

© KRAKEN Consortium. This document cannot be copied or reproduced, in whole or in part for any purpose without express attribution to the KRAKEN project.

Release History

Version	Date	Description	Released by
V0.1	08/11/2022	Initial version	Giancarlo Degani
V0.2	25/11/2022	Feedback from 1st review	Giancarlo Degani
V0.3	28/11/2022	Minor improvements	Giancarlo Degani
V0.4	29/11/2022	Feedback from 2nd review	Giancarlo Degani
V0.5	30/11/2022	Fixed back page	Giancarlo Degani
V1.0	30/11/2022	Submitted version	Atos

Table of Contents

List of Tables

List of Acronyms

Acronym	Description
APIs	Application Programming Interface
EBSI	European Blockchain Services Infrastructure
EC	European Commission
eIDAS	electronic IDentification Authentication and Signature)
ESSIF	European Self Sovereign Identity Framework
EU	European Union
FE	Functional Encryption
FHE	Fully Homomorphic Encryption
GDPR	General Data Protection Regulation
her	Electronic Health Records
HPRA	Homomorphic Proxy Re-Authenticator
HR	Human Resources
HTML	Hyper Text Markup Language
IoT	Internet of Things
JS	Java Script
KWCT	KRAKEN Web Company Tool
LSTS	Science, Technology and Society Studies
MPC	Multi-Party Computation
Mx	Month 1, Month 2…
PAB	Project Advisory Board
SMPC	Secure Multi-Party Computation
SP	Service Provider
SSI	Self-Sovereign Identity
Tx.x	Task 6.1, Task 6.2…
VC	Verifiable Credential
WP	Work Package
WPx	Work Package 1, Work Package 2…
ZKPS	Zero-Knowledge Proof Systems

Executive Summary

As part of the project, the KRAKEN consortium has involved external parties to share with them the approach, methodology, and results of the entire project. In this third and final Project Advisory Board meeting have been involved experts in different topics: from blockchain perspective to self-sovereign identity; from legal and ethical issues to business vision.

The previous Advisory Board, held in November 2021, aimed to collect feedback to address the final development steps and to discover possible areas of improvement.

The Third Advisory Board took place on November 10th and was focused on the future of the KRAKEN platform, aiming to collect feedback and suggestion from the advisors to improve the exploitation strategy.

During the meeting, we shared an overview of all the project's achievements. A particular emphasis has been put on the development of the last year with the demonstration of some project's use-cases.

We also shared KRAKEN exploitation plan which was the focus of the second part of the meeting.

A relevant part of the meeting has been devoted to the exploitation strategy. The advisors confirmed the choices made for the exploitation strategy and provided some relevant feedback about the definition of the price model.

1 Introduction

1.1 Purpose of the document

The present document has the purpose to report the feedback of the third Advisory Board meeting regarding KRAKEN's exploitation strategy. This D6.11 due by November 2022 is the last of three deliverables of the series, D6.9 submitted in November 2020, D6.10 submitted on November 2021, and.

1.2 Structure of the document

Chapter 2 presents the advisors and their expertise profile.

Chapter 3 describes the organization and agenda of the meeting. It also describes the topics addressed in the meeting: the project overview, the demo for the Health and Education Pilots, the market analysis, the price model, and the feedback provided by the advisors.

2 The Role of Project Advisory Board

As mentioned within the grant agreement, the Project Advisory Board is an external body to the project, devoted to transmitting to the Consortium feedback and suggestions. Three official meetings with the Advisory Board have been scheduled as part of T6.5 – Project Advisory Board activities to achieve this goal. The reports of these meetings will be submitted as deliverables and the PAB recommendations considered as relevant input for the achievement of project goals and the technical management of the project. Of course, the collaboration with the Advisory Board will not be limited to these events, at the end of each year of the project, but involves a constant communication with KRAKEN WP leaders.

2.1 Members of PAB

Andrea Migliavacca (male), degree in Business Administration (1988), 26 - year experience in ICT projects. Since 2009 Senior consultant at Lombardia Informatica (Research, Innovation and Financed Projects Ar-ea). Andrea was team leader in LISPA for Palante and Salus Projects and he currently is the CEO of Think4Future.

Carlos Pastor (male), currently working for Inetum as Director of Blockchain Strategy. More than 25 years of working experience in national and multinational companies like Telefónica, or Sun Microsystems linked to then emerging technologies like Intelligent Buildings, Electronic Banking, e-Commerce, Internet Gaming, Social Networks, Voice over IP, SWIFT Communication, Federated Identity, Public Key Infrastructure, Electronic Signatures (advanced including biometric voice & voice recognition signature), Self-Sovereign Identity and Blockchain.

Melek Önen (female) is an assistant professor in the Digital Security Department at EURECOM. Her current research interests are the design of security and privacy protocols for cloud computing, Big Data and IoT. She was involved in many European and national French research projects. Melek Önen holds a PhD in Computer Science from ENST (2005).

J. Peter Burgess (male) is a philosopher and political scientist. He is Professor and Director of the Chair in Geopolitics of Risk at the Ecole Normale Supérieure, Paris; Professor at the Centre for Advanced Security Theory (CAST) at the University of Copenhagen; and Research Professor at the Centre for Law, Science, Technology and Society Studies (LSTS) of the Vrije Universiteit Brussel. His research and writing have focused mainly on the theory and ethics of security and insecurity, and more recently on questions of fundamental rights in relation to digitization, data protection and privacy. He is at present Chairman of the Ethics Advisory Group of the European Data Protection Supervisor and co-authored its recent report Toward a Digital Ethics.

Harald Zwingelberg (male) is head of the “Privacy Technology Projects” division at Unabhängiges Landeszentrum für Datenschutz (ULD), the office of the Data Protection Authority of Schleswig-Holstein. On behalf of ULD he participated in a series of EU-funded and national research projects with relation to data protection, privacy and identity management. His focus resides with legal aspects of data protection.

André Kudra (male) has more than 13 years of information security consulting experience. In his career he held various key positions in major information security projects of global enterprise organizations.

He studied business administration at the European Business School (EBS) in Oestrich-Winkel, Germany, and computer science at the James Madison University (JMU) in Harrisonburg, Virginia, USA. Since 2013 André is CIO of esatus AG, a consulting company specialized in information security matters, with its headquarter near Frankfurt in the Rhine-Main area and offices in Hamburg and Munich. André is a strong advocate of Self-Sovereign Identity and a Sovrin Technical Governance Board member.

3 Third Project Advisory Board Meeting

3.1 Meeting organization, agenda, and participants

The third and final Project Advisory Board has been organized as an online meeting. The meeting took place on Thursday, November 10th, from 9:00 am to 12:00 am and the platform used has been Teams, by Microsoft. The meeting has been recorded with the consent of all participants.

The agenda was designed to focus on the exploitation and sustainability of the project.

In order to have a more effective meeting, we shared in advance to the advisors not only the agenda but also some questions with topics we recognized as particularly relevant for the exploitation of the project.

After an initial review of the project objectives, the latest developments on both pilots have been demonstrated to the Advisors in order to provide an updated on the project progress and also stimulate the generation of more valuable feedback.

Then we addressed, from the perspective of both pilots, the business approach and the aspects related to the data valorisation and pricing.

10/11/2022			
Time	**Description**	**Responsible**	**Duration**
9:00-9:05	Conference opening – partners & advisors join the conference		5’
9:05–9:15	Welcome, presentation of the agenda and meeting objective. Roundtable to present Advisors and Partners	ICERT	10’
09:15-09:40	Project Overview: Update on current status • Project Overview & organization (max 1 slide) • objectives (& achievements) • Project updates vs 2nd Advisory Board • Main Technical Achievements	ATOS	25’
9:40–10:05	DEMOS focused on User Experience	TEX LYN ATOS	25’
10:05–10 :15	Impressions & Feedback Session on DEMO	ICERT	10’

10:15–11:00	Market Updates & Exploitation of KRAKEN:
	• Whole Platform Go To Market Strategy
	• KRAKEN Experience on the Pilots and their Market
	• Healthcare Update: Pilot experience & KRAKEN business approach (hospital networks, consumer data)
	  ○ what’s the best Business approach in your opinion?
	• Education Update: Pilot experience & KRAKEN Business approach (HR company, students, universities etc)
	  ○ what’s the best Business approach in your opinion?
	• Data valorisation and pricing: KRAKEN idea (dynamic Price)
		ICERT –TEX Support the Discussion
		
		TUG & LYN Pilot Owner
			45’

10/11/2022			
Time	**Description**	**Responsible**	**Duration**
	• Computation as a service		
11:00–11:15	Break		15’
11:15–11.40	Round table for Feedback Session on Go To Market Strategy & Business Model	CERT – LIN - TEX	25’
11:40–11:45	Future of the Platform and its sustainability	ICERT	5’
11:45–12:00	Final feedback from Advisors	INFOCERT	15’
12:00	End of the meeting		

Table 1: PAB meeting agenda

Five out of the six project advisors participated in the meeting. One of them couldn’t attend.

Work Package leaders and representatives of the project partners attended the meeting.

3.2 Presentations and live feedback

This chapter describes the information shared with the Advisors and the feedback received.

To adapt to some advisors’ constraints and to let the discussion flow smoothly we adapted the agenda mixing the feedback about the demos with the broad discussions about exploitation and sustainability of the project.

3.2.1 Project overview: updates and current status

In the last year of the project, the Consortium has completed significant milestones releasing the following deliverables:

- Final KRAKEN Marketplace integrated architecture
- Final technical design
- Design for Marketplace integrated architecture
- Final release of the Self-Sovereign identity solution
- Final Data model and ledger for biomedical marketplace release
- Final research report on cryptographic protocols for privacy-preserving data markets and SSI systems
- Final implementation of cryptographic libraries
- Marketplace final release
- marketplace testing and validation final report

The main technical achievements can be grouped based on the technological pillar they belong to.

Self-Sovereign Identity

- SSI mobile app for managing VCs and key material
- Ledger USelf Broker for SP integration
- VCs with different levels of assurance for accessing the services the platform provides
- Legal Identity Manager creates VCs based on eIDAS identity and allows to sign documents with those VCs.
- KWCT, a tool for managing VCs

- Backup Service allows the use of several devices.

Cryptographic libraries

- Multi-Party Computation (MPC) to perform analytics on published products
- Homomorphic Proxy Re-Authenticator (HPRA) to perform key sharing
- Zero-Knowledge Proof to authenticate data and, combined with MPC nodes, to authenticate the share of data
- Marketplace JS/webAssembly library to share keys with HPRA and MPC data management

Marketplace

- Marketplace Backend with REST API
- Marketplace Frontend UI to allow the users to perform operations on the Marketplace
- Smart contracts to publish and purchase data products on the xDai blockchain
- xDai Watcher to receive events from the xDai blockchain and update the Marketplace
- Data Union to merge valuable data into a single Data Product and Data Union Smart Contract to manage the one-to-many payments for the Data Union
- Consortium Blockchain Network to run smart contracts handling the product catalogue and the data catalogue
- Depute Tool and Company Identification Tool to manage natural persons acting on behalf of a legal entity leveraging the SSI infrastructure

Leveraging these technical pillars, the final release of the KRAKEN Platform has introduced the following process improvements:

- Institutional user registration and login
- Publication and purchase of privacy-preserving analytical results
- Publication, purchase, and joining of a Data Union
- Computation of a data subject's Privacy Metrics
- Payment with fiat currencies

Feedback from advisors:

No feedbacks was provided by the advisors.

3.2.2 Demo and feedback session

We shared with the advisors the latest improvement in the KRAKEN platform showing five different workflows involving both the Health Pilot and the Edu Pilot.

Recorded videos of these workflows are publicly accessible on KRAKEN's website for both pilots:

- Health Pilot: https://krakenh2020.eu/pilots/health
- Edu Pilot: https://krakenh2020.eu/pilots/education

3.2.2.1 The seller publishes the dataset in the marketplace catalog

This workflow demonstrates the publishing of a new data product on the Marketplace, and it consists of the following steps:

- Choice of the catalog category
- Select the create product function
- Insert the product name and details
    - Insert tags selected from the medical terminology
    - Define the legal permissions and the access preferences
    - Define the companies allowed to access the data

    - Define if the data can be shared outside EU
- Encrypt the file and upload it to a publicly accessible storage
- Select the price and connect a crypto wallet
- Sign the transaction to pay the gas fee and publish the product on the catalog

3.2.2.2 Buyer purchases access to the data product

The workflow demonstrates how a buyer can purchase access to the data product. It consists of the following steps:

- Browse the catalog and select the data product
- Check the product details
- Fill in a form defining how the data product will be used
- Confirm the purchase and pay
- Download and decrypt the data set

3.2.2.3 Data made available for privacy-preserving analytics

This workflow demonstrates how a publisher can create a new dataset and make it available for privacy-preserving analytics:

- Select the analytics section of the product catalog
- Create a new data product defining name, tags, and other parameters
- Choose the file to be shared and define the column names for the dataset
- Encrypt and upload the encrypted file to a public storage
- Sign the transaction and publish the data product

3.2.2.4 Buyer purchases access to a privacy-preserving computation

This workflow demonstrates how a buyer can select many datasets from the catalog and then buy a privacy-preserving computation to obtain analytics from the dataset. It consists of the following steps:

- Search the data products and add them to the computation basket
- Open the computation basket to check the selected datasets and chose the desired analytics
- Buy the computation paying with the browser crypto wallet
- Then the computation is started and, eventually, the user can download the computed analytics.

3.2.2.5 Recruitment service and academic data

This workflow demonstrates how a student can obtain academic data as Verifiable Credentials and share them with a recruitment service. The workflow consists of the following steps:

- Log in to the Education Credential Exporter
- Connect the mobile wallet
- Select the academic data (grades or diploma)
- Export the academic data to the mobile wallet
- Accept the VC issued by the Credential Exporter
- Open the recruitment service and select a job proposal
- Scan the QR code to connect the mobile wallet
- Fill in the application form and submit it
- On the mobile wallet accept the VC request and fill in it

3.2.2.6 Feedback from advisors

The feedback from the advisors highlights the relevance of assuring the trustworthiness of the technological platform.

Regarding the marketplace, the advisors appreciated the look and feel and the smooth processes.

They advised providing some more information to the users in order to sensitize them about the aspects related to the possible transfer of data across European borders.

The advisors suggested highlighting that no data are actually stored in the blockchain.

3.2.3 Market Analysis, Exploitation, and Go-To Market Strategy

During this section, we showed to the Advisors how the pilots are proceeding from a market and business point of view highlighting takeaways from the recent surveys and from the KRAKEN partners that worked directly on the pilots. Those takeaways lead to further discussion and ideas on business model approach for the whole platform. In particular, the presentation showed the following flow:

- Recap of what was said regarding the healthcare pilot for the 2 areas of action:
  - **Hospitals** with privacy-preserving analytics using SMPC for Hospital networks
  - **People** with consumer data streams from mobile apps
- Recap of what said for the education pilot in terms of user groups that should benefit from the KRAKEN solution (students, recruiters / HR companies, and statistical agency
- KRAKEN experience and update from both Pilots, particularly:
  - Healthcare:
    - 80% of the participants of a survey we performed in the pilot said that the security and privacy features would be the most important factors in deciding whether to share their health data with another entity
    - European data residency can be an issue for several stakeholders
    - Compared to 3 years ago, crypto remuneration is now more accepted (70% vs 20%)
  - Education:
    - 80% of the evaluation users are interested to use the privacy-preserving analytics of KRAKEN
    - HR Companies seem to be less interested in the data market than expected
    - Using MPC technology to perform analytics on data from different sources is interesting for data buyers to stay compliant
- **Strategical consideration on Education Updates**: the takeaway regarding the low interest of the HR companies in a data market brought us to further considerations. An action could be to highlight the analytical potential of the KRAKEN platform service as a tool that enables the analysis of a vast privacy-preserved database. A renewed message on the suggested value proposition can be beneficial for that kind of potential customer.
- **Idea for business model**: **The Freemium approach:** considering the experiences and feedback received during the pilot phase, the KRAKEN platform could benefit from a Freemium approach to bypass the difficulties of certain markets and to embed a «free trial-like» logic to better penetrate a market. especially in the initial phase of life
- **Potential effects of a Freemium approach**:
  - **Attract more customers,** especially for markets and categories where the service is yes not well perceived (i.e., HR companies in the education market)
  - **Efficient exploitation** of data hard to valorise (i.e., old or common health data)
- **Dynamic price, Pay-per-use Model, and Computing as a service:** regarding the data monetization approach we decided to pursue the Pay-per-use model. In fact, this model allows us an approach able to manage the difficulties in giving a price to a non-rival good. KRAKEN approach is to use parameters such as the number of data access requests, type of use of data, different kinds of computations, and other business-type variables to adjust data asset price given a time window. With this approach KRAKEN hopes:
  - To maximize the value of a data set through constant “market inputs adjustment”

- To create an incentive for the Data providers to supply better and better “quality of data”

While this payment approach seemed in line with Advisors perception of the value model, the question of how to actually price data assets remains a complex and still unanswered one. Market-based pricing, i.e. how much a give actual is simply willing to pay, seems at this stage the only viable framework. More complex model such as dynamic pricing are seen as viable as the market place reaches maturity and large numbers of data providers engage in it.

3.2.4 Feedback Session

Peter Burgess:

- the Freemium approach is in line with the actual global strategy in application purchasing.
- Medical data should be considered always “special” data. With this in mind, it’s important to approach different geography (Europe vs America) with different approaches. You might have to have political sensitivity in different markets about buying and selling medical data.

Andrea Migliavacca:

- The quality of data that the supplier delivers is a very relevant element for the KRAKEN business model. A dynamic price approach, in which the data quality is an important factor to the calculation of this price is an incentive for the supplier to supply high-quality of data.
- If I have to choose the most important factor as a supplier to enter in a partnership with a marketplace of data like KRAKEN, I could choose the integration costs. Those costs are the main factor to analyse and understand to evaluate those kinds of project.

Harald Zwingelber**g**:

- To implement a feature to let the customer express their preferences regarding the use of the data could be important for certain markets and types of data.
- The Freemium approach really makes sense for this kind of service

4 Conclusions

As in the previous meetings, the Third Advisory Board meeting was also fruitful thanks to the expertise and constructive collaboration demonstrated by the advisors.

The meeting has been an opportunity to review the overall project and the most recent improvement.

From the advisors there has been a particular emphasis on the aspect related to the GDPR compliance, the security of the data exchange, and the possible transfer of data across national borders.

The advisors appreciated the progress made in the last year of the project and the smoothness of the use cases that have been demonstrated.

Furthermore, the discussion about the sustainability of the KRAKEN platform generated some insightful consideration about the price model that will be very useful to design the global strategy for the KRAKEN platform exploitation and for the definition of the price model itself.

The general feedback about the project and its achievement have been positive. The advisors appreciated the smoothness of the workflows developed to implement the use cases.

KRAKEN

@KrakenH2020

Kraken H2020

www.krakenh2020.eu

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