D1.4 Annual Public Report III

Author: Alexandra Garatzogianni, Gerrit Rosam, Michael Fribus (LUH)

Contractual Due Date: 31 December 2022 (M36)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481

TRUSTS Trusted Secure Data Sharing Space

D1.4 Annual Public Report III

Document Summary Information

Grant Agreement No	871481	**Acronym**	TRUSTS
Full Title	TRUSTS Trusted Secure Data Sharing Space		
Start Date	01/01/2020	**Duration**	36 months
Project URL	https://trusts-data.eu/		
Deliverable	D1.4 Annual Public Report III		
Work Package	WP1		
Contractual due date	31/12/2022	**Actual submission date**	10/02/2023
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	LUH		
Responsible Author	Alexandra Garatzogianni (LUH), Gerrit Rosam (LUH), Michael Fribus (LUH)		
Contributions from	Alexandra Garatzogianni (LUH), Gerrit Rosam (LUH), Michael Fribus (LUH), Anna Beer (LUH/TIB), Gianna Avgousti (EBOS), Ioannis Markopoulos (NOVA), Benjamin Heitmann (FhG), Kim Frieda Fidomski (FhG), Ilan Goldberg (EMC), Yuliya Miadzvetskaya (KUL), Lidia Dutkiewicz (KUL), Andreas Huber (G1), Bert Utermark (G1), Nina Popanton (DIO), Hannah Engel (DIO), Petr Knoth (RSA), Manos Paschalakis (REL), Evangelos Kotsifakos, Rosa Araujo (LST), Silvia Castellvi (IDSA)		

Revision history (including peer-reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v0.1	03/05/2022	10%	Initial Deliverable Structure	Alexandra Garatzogianni (LUH), Gerrit Rosam (LUH), Michael Fribus (LUH)
v0.2	07/11/2022	80%	Content	Alexandra Garatzogianni (LUH), Gerrit Rosam (LUH), Michael Fribus (LUH), Anna Beer (LUH/TIB), Gianna Avgousti (EBOS), Ioannis Markopoulos (NOVA), Ioannis Routis (NOVA), Benjamin Heitmann (FhG), Kim Fidomski (FhG), Ahmad Hemid (FhG), Lorenzo Gugliotta (KUL), Ilan Golberg (EMC), Dominik Kowald (KNOW), Stefan Gindl (RSA), Nina Popanton (DIO), Hannah Engel (DIO), Bert Utermark (G1), Andreas Huber (G1), Manos Paschalakis (REL), Evangelos Kotsifakos, Rosa Araujo (LST), Silvia Castellvi (IDSA)
v0.3	19.12.2022	90%	First Review	Kim Fidomski (FhG), Ahmad Hemid (FhG)
v0.4	20.12.2022	95%	Second Review	Nina Popanton (DIO), Hannah Engel (DIO)
v1.0	10.02.2023	100%	Final Version	Alexandra Garatzogianni (LUH), Gerrit Rosam (LUH), Michael Fribus (LUH)

Disclaimer

caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
BV	Business Validation
CRM	Customer Relationship Management
DL	Deep Learning
DMP	Data Management Plan
DoA	Description of Action
DoW	Description of Work
DS	Data Stewardship
DSM	Digital Single Market
E2E	End-to-End
EDMI	Europeana Dataset Minimum Information
EOSC	European Open Science Cloud
ETL	Extract, Transfer, Load Process
FAIR	Findable, Accessible, Interoperable, and Reusable
FHE	Fully Homomorphic Encryption
FL	Federated Learning
FR	Functional Requirements
GAN	Generative Adversarial Network
GDPR	General Data Protection Regulation
GA	Grant Agreement
HE	Homomorphic Encryption
HFL	Horizontal Federated Learning
IDS	International Data Space
IM	Information Model

IPR	Intellectual Property Rights
KPI	Key Performance Indicator
LOSD	Linked Open Statistical Data
ML	Machine Learning
MPC	Multi-Party Computation
MVP	Minimum Viable Product
PET	Privacy-Enhancing Technologies
PoV	Point of View
RAM	Reference Architecture Model
RDF	Resource Description Framework
SAB	Stakeholder Advisory Board
SLA	Service-Level-Agreement
TL	Transfer Learning
TV	Technical Validation
UC	Use Case
VFL	Vertical Federated Learning
WP	Work Package

1 Executive Summary

The objective of this **Annual Report III** is to report the project's progress in the third and final year of the TRUSTS Project as well as the final achievements of the project. For each Work Package (WP) and for each specific Lead there are reports on overall objectives and achieved progress in the third project year[1].

During the third project year (M25 – M36) the TRUSTS Consortium has achieved all crucial goals in each WP. Some major highlights per WP include: In WP1, an all-encompassing, effective, forward-looking, and collaborative project management of the whole TRUSTS project was ensured while enabling regular communication between the EC and the project consortium and monitoring potential risks. The TRUSTS architecture was defined in WP2, and the analysis of the worldwide data marketplace ecosystem was finalised[2]. Key steps to realise the requirements and specifications of implementing the TRUSTS platform were realised in WP3. Moreover and among other achievements the next versions of the minimum viable product has been set, the TRUSTS platform was refined and a smart contract executor was integrated. In WP4, there was a focus on the development of risk analysis models and algorithms as well as on the implementation of corresponding modules for a ready-to-use application. The set-up of the test environment for the three use cases, as well as the planning and operation of the final execution phase of the use cases were undertaken in WP5. In WP6, an overview of the legal framework in order for TRUSTS to be compliant with the principles of research and ethics, and a set of legal and ethical requirements was set up with respect to potential legal and ethical obstacles. The results of the TRUSTS stakeholder landscape were transferred into suitable strategies for the TRUSTS stakeholder engagement plan in WP7. In WP8, the project's mission, vision, and achievements were actively communicated and disseminated to relevant TRUSTS stakeholder groups via various communication tools such as the website and social media channels. In WP9, Ethics deliverables have been resubmitted based on the requirements raised within the Ethics Check.

[1] For further info, please check the deliverables section of the TRUSTS website: https://www.trusts-data.eu/deliverables/

[2] Changes made in the third year are described in D3.11

2 Introduction

This Deliverable (D1.4) is the final report on the project's progress & outcome in the third year of the TRUSTS Project and consists of the following sections. Section 3 contains reports of the objectives, the achieved results and final outcomes as well as future outlooks of each of the nine TRUSTS Work Packages. In Section 4 the objectives, the achieved results and the future outlooks are specified for the Scientific Lead, Technical Lead, Innovation Lead, Security Lead, Legal and Ethical Lead, Communication and Community Building Lead, Business and Exploitation Lead. The project's Data Management Plan (DMP) (D1.6) lists all relevant information on realised data management activities. Section 5 contains a final update of the DMP. Conclusions of the TRUSTS project overall are outlined in Section 6.

Mapping Project's Outputs:

Purpose of this section is to map TRUSTS Grant Agreement (GA) commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to TRUSTS GA Deliverable & Tasks Descriptions

Task		Respective Document Chapter(s)	Justification
T1.1 Project Management	This task deals with all necessary project management tools, mechanisms and structures for the high quality, efficient and timely administrative coordination of the project. It incorporates Administration Management activities, including procedures and guidelines for activity planning and monitoring, cost and time management, submission of periodic progress reports and cost statements, preparation of annual review reports, review presentations, and timely submission of deliverables to the Commission. LUH will be responsible for the day-to-day coordination of project-related activities and tasks, as well as the administrative management of the project; contributions will be made by all the partners.	Section 3 – Section 5	Section 3: Progress within Work Packages Section 4: Progress within specific Leads Section 5: Data Management Plan
Deliverable			
D1.4 Annual Public Report III Report on the project's progress, targeting the general public. The report will focus on the impact of the conducted work.			

3 Progress within the Work Packages

3.1 WP1 Project Management

3.1.1 Objectives

The Project Management WP served the objective to ensure the timely and impactful delivery of the project's results in compliance with the EC regulations and the H2020 framework. This has been achieved via the hands-on and continuous monitoring of the implementation and completion of the project's tasks, activities, milestones, and deliverables, safeguarding thus their proper and timely development according to the Description of Action (DoA) and the project's work-plan, while ensuring a smooth and efficient collaboration among the consortium partners.

The activities of the project management WP focused on:

- Establishing tasks, providing thus guidance and direction to achieve the goals of the H2020 TRUSTS project
- Ensuring continuous, proactive communication with the EC
- Establishing efficient means of communication and document exchange between partners
- Ensuring transparency at all levels and in terms of reporting by establishing appropriate report structures and procedures
- Conducting quality assurance activities and performing risk analysis tasks
- Coordinating the organisation of project meetings and other possible participatory events where the project could be presented
- Ensuring that project objectives are realised within set time, quality and budget.

3.1.2 Results achieved

Between M25 and M36 the status on deliverables is as follows:

T1.1 Project Management

Table 2: Deliverable Status Overview (M25-M36)

Del.	Title	Lead	Due	Status
D5.2	Pilot planning and operational management reports II	eBOS	M25	**SUBMITTED**
D4.2	Report on the implementation of deep learning algorithms on distributed frameworks	EMC	M30	**SUBMITTED**
D3.6	Data Marketplaces with Interoperability Solution III	RSA	M33	**SUBMITTED**
D3.8	Data Governance, TRUSTS Knowledge Graph II	SWC	M30	**SUBMITTED**

D5.9	Actual field trials of use case 3 v.2	REL	M34	**SUBMITTED**
D5.7	Actual field trials of use case 2 v.2	NOVA	M34	**SUBMITTED**
D5.5	Actual field trials of use case 1 v.2	eBOS	M34	**SUBMITTED**
D6.3	Legal and Ethical Assessment	KUL	M33	**SUBMITTED**
D5.3	Pilot planning and operational management reports III	eBOS	M35	**SUBMITTED**
D5.11	Performance evaluation and lessons learned report II	NOVA	M35	**SUBMITTED**
D7.6	Report on standardisation activities	IDSA	M36	**SUBMITTED**
D7.8	Business plan and Implementation action plan II	LST	M36	**SUBMITTED**
D3.3	Smart Contracts	FhG	M36	**SUBMITTED**
D6.4	Legal and Policy Recommendations	KUL	M36	**SUBMITTED**
D3.13	Profiles and Brokerage II	KNOW	M36	**SUBMITTED**
D8.5	Final Dissemination Report	DIO	M36	**SUBMITTED**
D3.11	Platform Status Report III	FhG	M36	**FIRST VERSION SUBMITTED**
D8.7	Accomplished training and capacity building programme	REL	M36	**SUBMITTED**
D1.4	Annual Public Report III	LUH	M36	**SUBMITTED**
D7.2	Sustainable business model for TRUSTS data marketplace II	TUD	M36	**SUBMITTED**
D7.5	Supporting mechanisms for Intellectual Property Rights Protection and Data Stewardship II	G1	M36	**SUBMITTED**
D7.10	Innovation Impact Assurance II	G1	M36	**SUBMITTED**

In terms of an amendment it was agreed that for D3.11 an initial version will be submitted highlighting the most important updates of the current status quo of the platform. An updated version of D3.11 will be submitted in M38 in order to capture and include important insights and inputs from WP5.

T1.2 Technical & Quality Assurance and Risk Management

For this task, appropriate **mechanisms and processes** have been established **to maintain overall quality** in all WPs of TRUSTS. In particular, WP1 oversees an extensive quality management of all TRUSTS deliverables. Thus, for the reporting of deliverables and for managing the overall quality of the deliverables, LUH set up a dedicated **review process for the deliverables** which can be seen below.

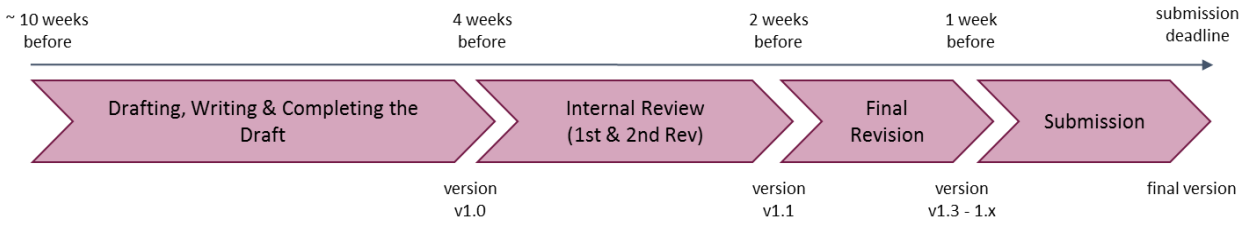


Figure 1: Deliverable Drafting, Review and Submission Process

The content of the deliverables of each TRUSTS WP is checked against 'Deliverable Quality Indicators' such as format, readability and consistency (e.g. contains right information, avoids redundant information, consistent with previous deliverables, etc.). Also, two Consortium partners were assigned to act as peer reviewers for each deliverable.

LUH has **identified and monitored potential PM Risks** and has successfully developed respective **mitigation plans** and established a **Risk Impact Assessment** for Risks from TRUSTS' DoA, which was discussed regularly in terms of Project Management Board (PMB) Telcos and updated when needed.

T1.3 Project Reporting & Communication

LUH ensured the implementation of regular reportings, milestone reviews and the Mid-Term Review (M18) as stated in the DoW. Thus, the Project Management Report as well as the Financial Report were finalised and timely submitted in M18. Moreover, a setup of various, regular PM calls were organised by LUH in the period M25-M36. This includes one WP1 PM Executive Board Telco, eight Project Management Board (PMB) Telcos, one online plenary (M26) as well as one live plenary (M30) organised in collaboration with DIO in Vienna. Beyond this, the coordination team regularly communicated results on various events online and onsite, including the European Big Data Value Forum 2022 (Prague), European Research & Innovation Days, European Sustainable Energy Week, Data Week, Media Data Space Workshop, Sweden Innovation Days, EU Industry Days and more. As the Coordinator of TRUSTS, LUH functioned as a contact point between the EC and the TRUSTS Consortium. In this role any potential deviations in terms of the project have been communicated and jointly, with the guidance of the EC, implemented. Thus, LUH ensured proper communication within the consortium, to external stakeholders, as well as between the EC and the consortium.

An overview of the Project Reporting & Communication activities can be seen in this table:

Table 3: Project Communication Formats

Project Reporting and Communication activities		
Types of Telcos	**Frequency**	**Purpose**
Executive Board PM WP1 Telcos	monthly	A call that provides oversight and an update of WP1, as well as the other WPs in TRUSTS. It gives participants the opportunity to learn about the progress, status quo and challenges of each WP.
Plenary	bi-annual	A deep dive into the project in which partners discuss the progress and proactively work on solutions for current challenges.

EC Review	after 18 months	A periodic conference with the purpose to report the progress and achievements of TRUSTS and its WPs to the EC. In total, there are two EC Reviews that take place during the TRUSTS project.
Project Management Board Telcos (PMBs)	bi-/ tri-monthly	A high-level conference to discuss the strategic development of TRUSTS with focus on specific tech / business-related / organisational tasks and challenges.

3.1.3 Future Outlook

Looking back at the last three project years, it can be concluded that the project management planning methods as well as monitoring of actual and target statuses turned out to be both effective and efficient. It was possible to react quickly and flexibly to unexpected problems, so that a suitable project management solution could always be found. As in any successful H2020 project, a transparent and clear communication between all involved partners as well as the EC is of highest importance. Since TRUSTS is a very technology-focused project it was of highest importance to maintain the communication between all technological partners, especially the Technical Coordinator, in order to consider the technological restrictions and nuances before developing project management solutions to any challenges that occurred during the lifetime of the project. As an outlook for future H2020 projects, it is highly recommended for the Coordinator and Project Management team to maintain a mediator role in a given project in order to help partners with different specialisations (business companies, institutions with focus on certain technologies, public institutions, legal entities, among others) to understand all angles and aspects of the project overall, and to respect all angles and aspects in finding the optimal solution. Furthermore, a clear timeline which should be constantly adhered to, is effective in implementing the milestones that were indicated in the Grant Agreement of a H2020 project.

3.2 WP2 Requirements Elicitation & Specification

3.2.1 Objectives

The overall objectives of WP2 as defined in the DoA were:

- to analyse the EU and worldwide challenges and trends and to define the requirements for the provision of a multi, concurrent and cross-domain, secure and scalable end-to-end (E2E) data marketplace service.
- to define detailed and functional industry specifications appropriate for a data marketplace linked to specific target Key Performance Indicators (KPIs) considering and bridging the vertical user point of view (PoV) with the analytics/solution provider PoV and the data marketplace platform provider PoV.
- to produce a set of KPIs and methodologies to enable:

  (a) the technological and Business Validation (BV) of the E2E data marketplace service and associated control and management within and across verticals;

  (b) the definition of the test reports format, parameters, test points, and benchmarking of the results for a unified and reliable outcome.

3.2.2 Results achieved

WP2 has concluded at the end of the second year and the results achieved have been reported on the previous version of this deliverable, D1.3 "Annual Public Report II".

During the third year, regarding the activities of WP2 that were not finalised, the majority of them were finalised under WP5 effort including a) the second Technological Validation (TV) and the third Business Validation (BV) and b) the finalisation of the update and evolution of the trials evaluation testing methodology, while the finalisation of the definition of the final version of the TRUSTS platform architecture was done under WP3.

3.3 WP3 TRUSTS Platform implementation

3.3.1 Objectives

This WP implemented the relevant requirements (identified by WP2 and prioritised by the whole project consortium) and specifications for the TRUSTS platform. This was achieved by dividing WP3 into supportive, innovative and integrative tasks.

In the third and final year of the project (M25-M36), WP3's overall focus was on finalising the implementation of all prioritised requirements and on bringing together all the components implemented as part of the different tasks into one platform.

Therefore, the following sub-objectives have been completed:

- Testing and setting the next versions of the minimum viable product for the TRUSTS platform in close collaboration with WP5.
- Refinement of the TRUSTS platform by continuously incorporating given feedback from the use case trials in WP5.
- Integration of the Smart Contract Executor.
- Implementation and validation of the components related to the metadata and semantic layer.
- Implementation of an interoperability solution to enable the interconnection between the TRUSTS platform and external data markets.
- Continuous improvement of the TRUSTS user interface based on feedback from the use case trials.
- Finalisation of the implementation of services for the TRUSTS recommender system as well as integration and evaluation of the recommender system in the TRUSTS infrastructure.

Continuous development and testing led to continuous improvements of the platform in the project's final year. Through close collaboration between the WP3 participants and with other WPs, the objectives were achieved.

3.3.2 Results achieved

Task 3.1 Infrastructure set-up and technical operations

The aim of this task was to provide and support the environment for the development of the TRUSTS platform components. The platform provides a set of capabilities that enable operators to develop applications with a high degree of privacy-by-design features. The cloud-based environment for the

development infrastructure set-up is using Google Cloud, which is compliant with the European laws and offers robust servers with tools to ensure data security with backup, monitoring, and encryption. All the resources used in the project are located in Google's EU servers.

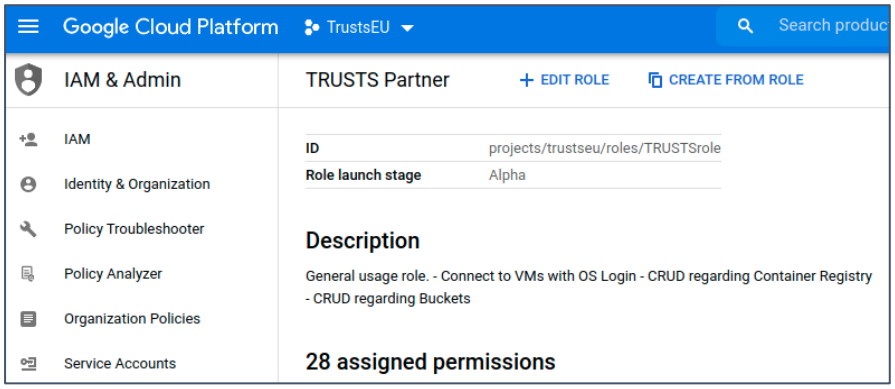


Figure 2: Screenshot of the GCP management system

LSTech employed DevOps and all the state-of-the-art mechanisms to support the architecture and specifications defined in T2.4 "Architecture design and technical specifications" and further developed in the project's third and final year, simulating a decentralised environment. The Docker environment allowed easy implementation, extensibility, scalability, portability, and security, allowing the different containers to run quickly from one computing environment to another.

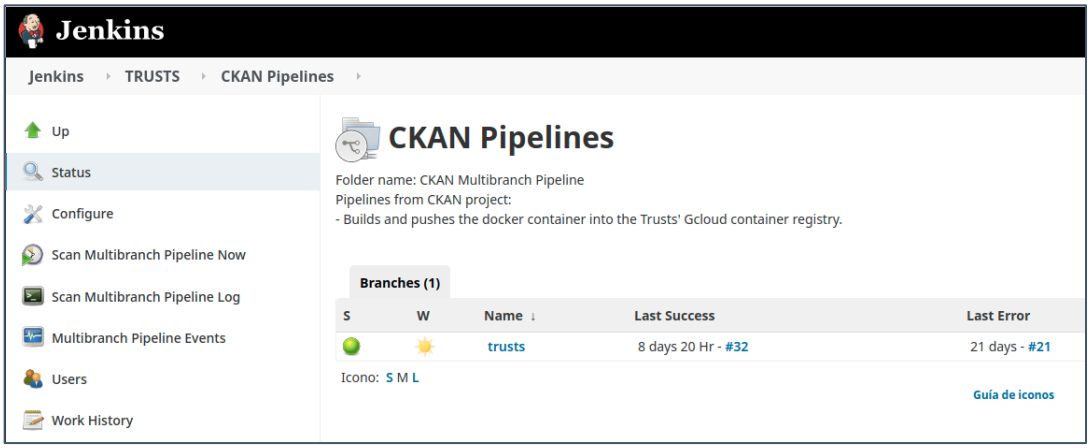


Figure 3: Screenshot of the Jenkins software

As it was in the second year, in the final year of the project, T3.1 continuously seeked feedback from the project partners with a technical perspective on the platform, in order to improve and iterate on the provision of infrastructure. Apart from the deliverable D3.2 "TRUSTS Infrastructure II" submitted in M24 which describes the infrastructure, T3.1 keeps a live technical document that was updated when needed, describing the necessary actions, instructions, procedures, and parameters required in order for the partners to connect to the available infrastructure and tools and in a secure way, through limited/controlled access, role management, versioning, and backup and restore procedures.

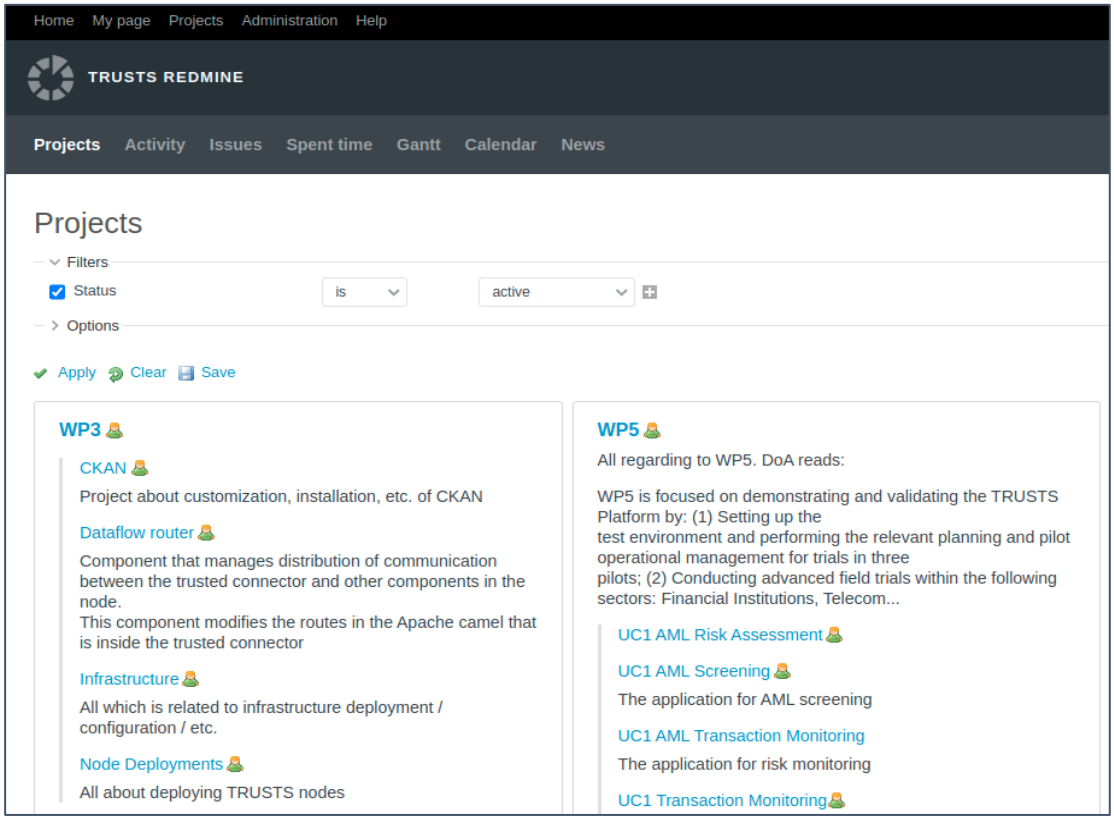


Figure 4: Screenshot of the Redmine project/issue management software

Apart from the main development infrastructure, LST setup, provided and supported the following tools:

- Gitlab repository for code and versioning
- Slack communication server for facilitating the day-to-day communication of the developers teams
- Redmine project/issue tracking platform

In summary, the actions and tasks that were performed during the final year include:

- Setup and manage the development environment.
- Support the needs of the partners in terms of resources, roles, access, deployment instructions, and documentation.
- Hands on day to day support, using CI/CD pipelines (using Jenkins) and the GitLab repository to ease the development.
- Setup, support, and maintenance of the GitLab repository, the Slack server, and the Redmine platform.

Task 3.2 Smart Contracts

The focus was primarily on the further development and completion of deliverable D3.3, which was divided into three main sections: Smart Contract Conceptualization, Legal Challenges in Applying Contract Law to Smart Contracts, and Extensions to the Description of the Smart Contract Demonstrator.

Smart Contract Conceptualization

Smart contract conceptualization includes establishing requirements for a blockchain and deriving recommendations for a blockchain that is most suitable for use in TRUSTS.

The requirements are divided into functional and technical requirements. The functional requirements are derived from deliverables D2.2 and D2.3. The technical requirements were then derived from the functional requirements, in addition to the technical characteristics of a blockchain: Blockchain, Permission, Smart Contract, Type, and Node. Blockchain describes the general requirement for a blockchain technology, because smart contracts need it in order to be executed. Permission can be used to decide whether the blockchain is private or public. The Smart Contract requirement specifies that smart contracts must be defined in advance among all participants before they can be transferred into the chaincode. Figure 5 illustrates the process. Furthermore, there are two types of smart contracts: On-Chain and Off-Chain.

Figure 5: Smart Contract Lifecycle

The last requirement deals with the consensus mechanism, which is essential for the integrity of transactions within a blockchain network. The flow of the consensus mechanism is shown in Figure 6.

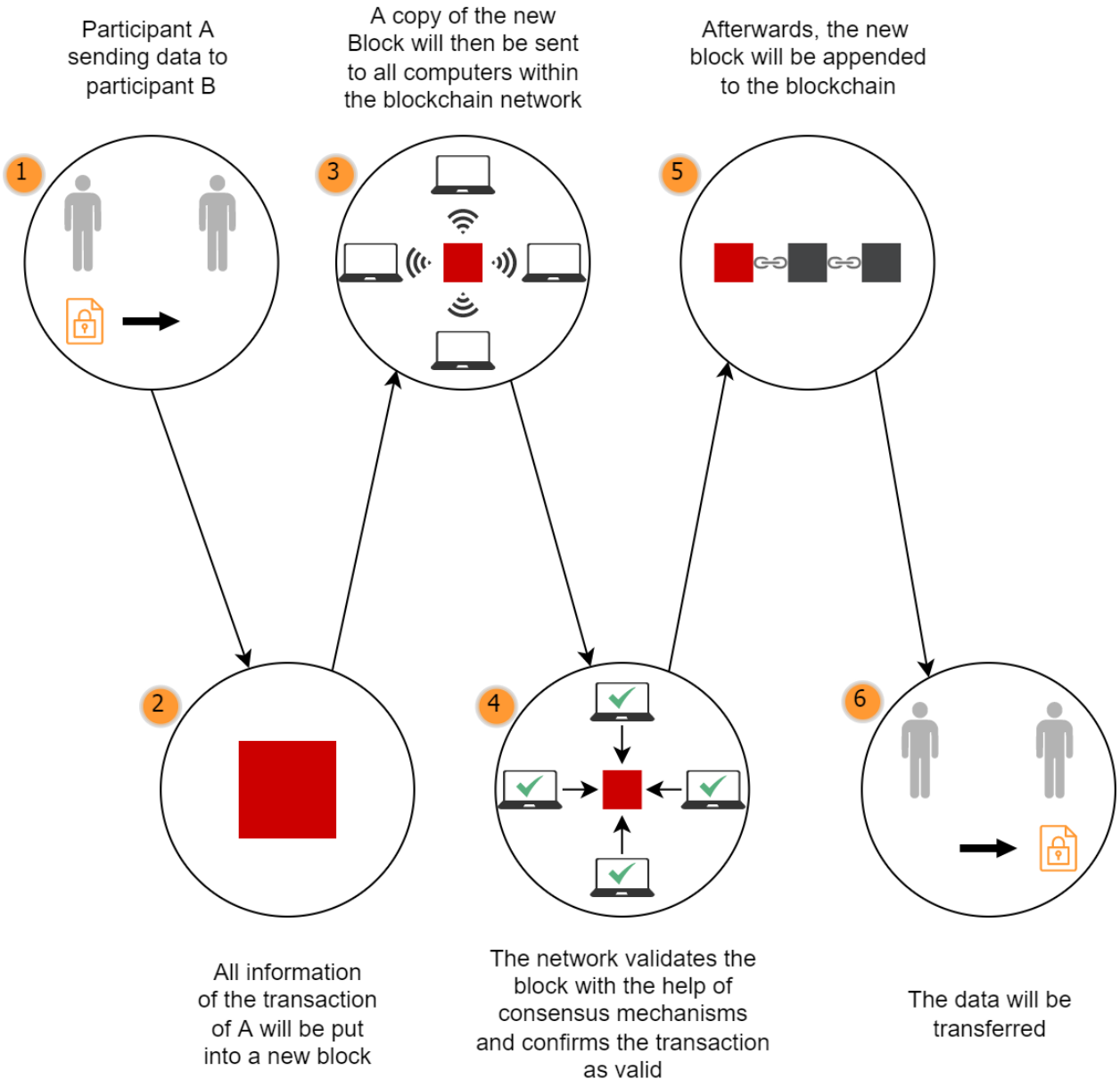


Figure 6: Adding a new block to the blockchain while an asset shall be transferred

Argumentative recommendations were then derived from the requirements, which are explained in a possible technical implementation.

In addition to all the advantages explained in D3.3, the use of a blockchain with smart contracts can also have disadvantages, which must be taken into account in any case. These include, for example, lower performance: Compared to a properly configured solution with a database, a blockchain solution performs lower due to higher response times and lower throughput when transactions are processed. Another risk is privacy: Although a participant is e.g. in a private chain, each of the participants can see what is happening on the blockchain. Through analysis and pattern recognition, conclusions can then be drawn about individual participants. These risks must be considered in any case when operating a blockchain.

Legal Challenges in Applying Contract Law to Smart Contracts

Task 3.2 also involved investigating the main legal challenges stemming from using smart contracts to regulate data exchanges. An analysis was first made of the relationship between the concept of 'smart contract' in computer science and traditional contract law, in which smart contracts would need to find their standing. The discussion concluded that the computer science concept of 'smart contract' may or may not have legal standing depending on the circumstances. An analysis of the key requirements for formation of contracts showed that smart contracts are, at least in principle, capable of satisfying such requirements and therefore be regarded as binding contracts. It was indeed observed that, despite the automatic nature of smart contract execution, there can still be an exchange of wills between two or more human parties in the pre-contractual phase, that can culminate with the acceptance by one party of the offer made by another one. The analysis then found that the validity of smart contracts that have legal standing can be put into question by traditional causes of invalidity, but it may be more difficult to ascertain them than in traditional contracts. The assessment then turned to the language challenge, i.e., how to make legally binding smart contracts 'in tune' with traditional contract law whereby smart contracts are written in code, which is a fundamentally different language than languages used by humans. It was observed in this regard that this fundamental difference can prove to be an inhibitor of legal certainty insofar as smart contract drafters try to incorporate nuanced and complex concepts (such as 'good faith', 'reasonable efforts', etc.) that sit at odds with the conditional and binary ('if this occurs, then that is the effect) nature of smart contracts. The simpler the code, the more effective and predictable the smart contract: this would then lead to maximising the legal certainty-enhancing effect of smart contracts compared to traditional contracts. The automated execution of smart contracts and their immutability, however, was also regarded as a challenge when it comes to ensuring continuous compliance of smart contracts with applicable law. The analysis showed that, while some technical solutions are being studied, there is not yet a consensus-based approach that is set to be endorsed by the industry. Finally, it was observed that the underlying blockchain is also key to the legal implications of smart contracts, in particular with a view to ensuring legal certainty and avoiding breaches of data protection and data security law.

Extensions to the Description of the Smart Contract Demonstrator

Four major extensions were made to the Smart Contract demonstrator in this period. To recap what the demonstrator consisted of up until these extensions: it was a blockchain accessible via commands on the local machine, a graphical user interface to showcase data from the blockchain, rudimentary blockchain query mechanisms, as well as basic and secured asset transfer smart contracts. The first extension was a remote API to use the blockchain over a network connection. The development of this was done using Hyperledger SDK, and Javascript NodeJS. The main task was mapping blockchain properties to the API application which then exposed these to the network in a request / response REST-style system. The second extension was an additional smart contract for scoring, rating and reviewing assets. This contract was developed using an existing hyperledger "create asset" function which was modified to create a specialised data object of type "review", which was stored on the blockchain in a similar fashion to an asset. Details such as the username of the reviewer, the identity of the asset being reviewed and the score were stored in this review data object as properties. The third extension was the implementation of a more robust search mechanism in the API application, which supports granular searching of assets on the blockchain through layers of filters. The search functionality was bolstered by additional properties to allow for the returning of specific IDs related to transactions, that can be used to formulate URLs capable of linking straight to an asset entry on the Explorer UI. A payment compatibility demonstrator sits on top of the improved blockchain search, in the form of a web UI application linked to external payment systems. Assets can be searched by ID and when a selection is returned it populates the web form with the corresponding asset properties retrieved from the blockchain. Radial buttons allow the user to choose between one of three popular

payment systems included in this demonstrator, and upon clicking to purchase the asset the user is then moved to the relevant payment system to complete the payment out-of-band. The above is featured in D3.3 in far greater detail but the following figure 7, taken from that deliverable, offers a view of the payment compatibility demonstrator.

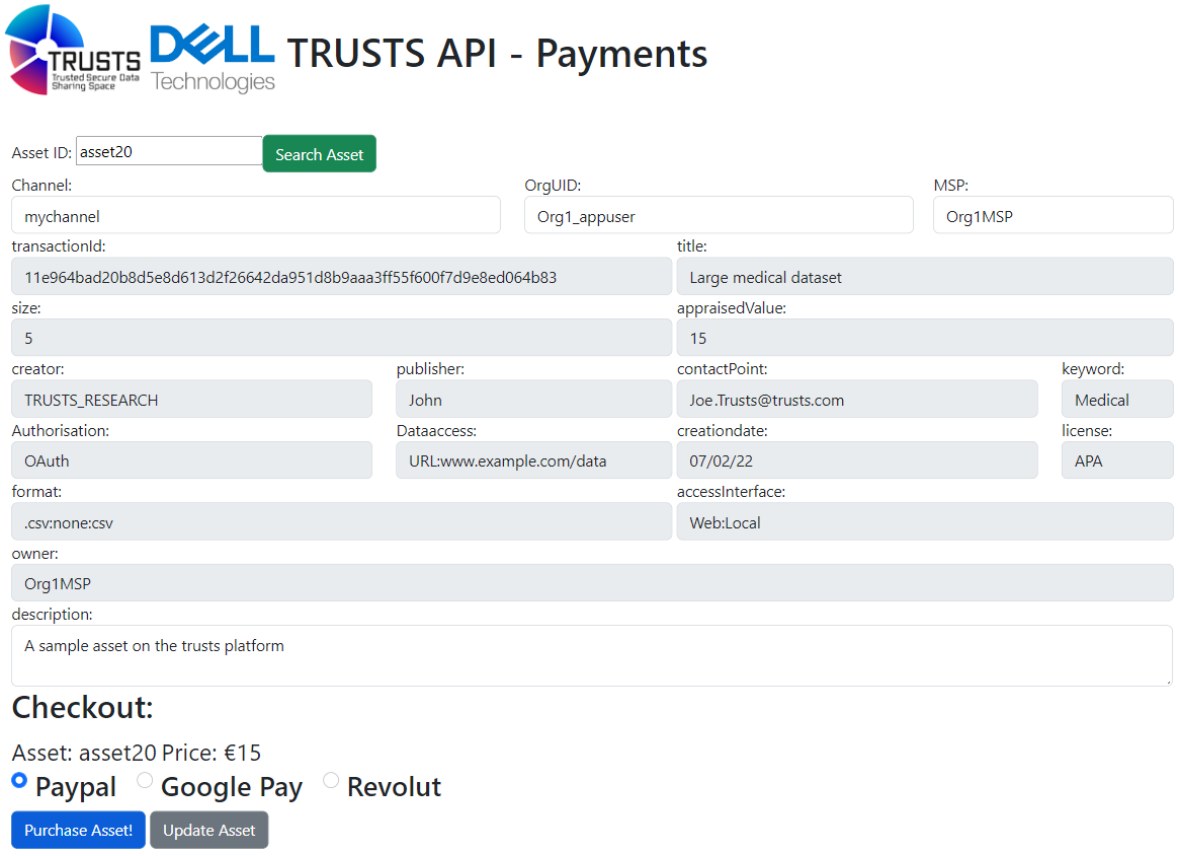


Figure 7: Payment Compatibility Demonstrator

Task 3.3 Data marketplace interoperability solutions

Task 3.3 continued interoperability research along the four layers **technical**, **semantic**, **organizational**, and **legal** interoperability. In the **technical layer**, two connectors for the EOSC initiatives OpenAIRE and Europeana were developed as well as another component to programmatically load metadata of datasets into TRUSTS. The latter solution helps to map data catalogs from external sources, e.g., third-party datamarkets. The functionality was demonstrated in an experiment, where an additional TRUSTS instance functioned as an external marketplace and uploaded metadata using this component. The software solutions all relied on the established ETL process (Extract, Transfer, Load), which is used in the area of data warehouses to load data from external sources into an internal data storage (see Figure 8).

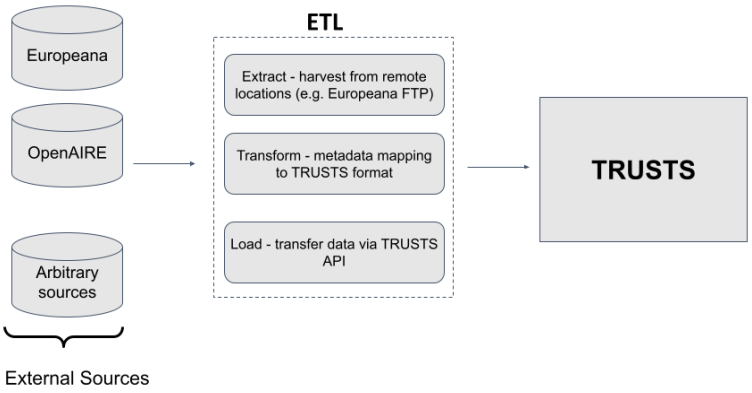


Figure 8: The ETL process used to load data from external sources into TRUSTS

Semantic interoperability encompasses the adaptation of the TRUSTS-IM with EDMI, the Europeana Dataset Minimum Information. EDMI has proven a valuable additional resource for the already very comprehensive TRUSTS-IM and was thus selected for incorporation. We also developed a metadata mapper which converts the metadata schema of OpenAIRE and Europeana into the format TRUSTS requires.

The **organisational layer** covered two aspects, firstly the experiment described earlier. In this experiment, an additional TRUSTS deployment served as an exemplary external datamarket. This TRUSTS deployment was completely independent from the main TRUSTS platform. We conducted this experiment to demonstrate the functionality of a component for the programmatic transfer of metadata from this external source into the main TRUSTS platform.

In this layer we also implemented the smart contract client, a component to connect CKAN, the data management system serving as the basis for TRUSTS, with the smart contract demonstrator, a component for the handling of smart contracts, which is based on Hyperledger Fabric and was developed by T3.2.

Finally, the **legal layer** covers issues and challenges connected to interoperability with external sources. Such issues can arise through the existence of differing legal frameworks, especially when entities from different nations interact with each other. In the respective part in D3.6, the final deliverable of T3.3, we discuss legal interoperability aspects, especially with regards to intellectual property law, as well as privacy and data protection law.

Task 3.4 Data Governance: Metadata, Lineage and Semantic Layer

The third and final year of the TRUSTS project has seen the metadata and semantic layer of the TRUSTS platform move into the implementation and validation phase. Development of new software components included the IDS extension for CKAN, the TRUSTS client library, and the Vocabulary Extension for CKAN. During these deployments, the adaptation of the TRUSTS-IM (as specified in D3.7 and D3.8) was undertaken, and its operationalization using the IDS Dataspace Connector API and data model was achieved.

The result of this, as schematized in Figure 9, is a series of flows that transform metadata as input from users or harvesting mechanisms, into the CKAN and then DSC's data models. These are then transformed into the TRUSTS-IM itself, as expressed in RDF, and propagated into the central node. The TRUSTS-IM serves as the lingua, the common description that all nodes in the TRUSTS platform understand and can translate from and into. This standardised description is then leveraged both by existing IDS infrastructure, as well as by the platform client and interoperability solutions.

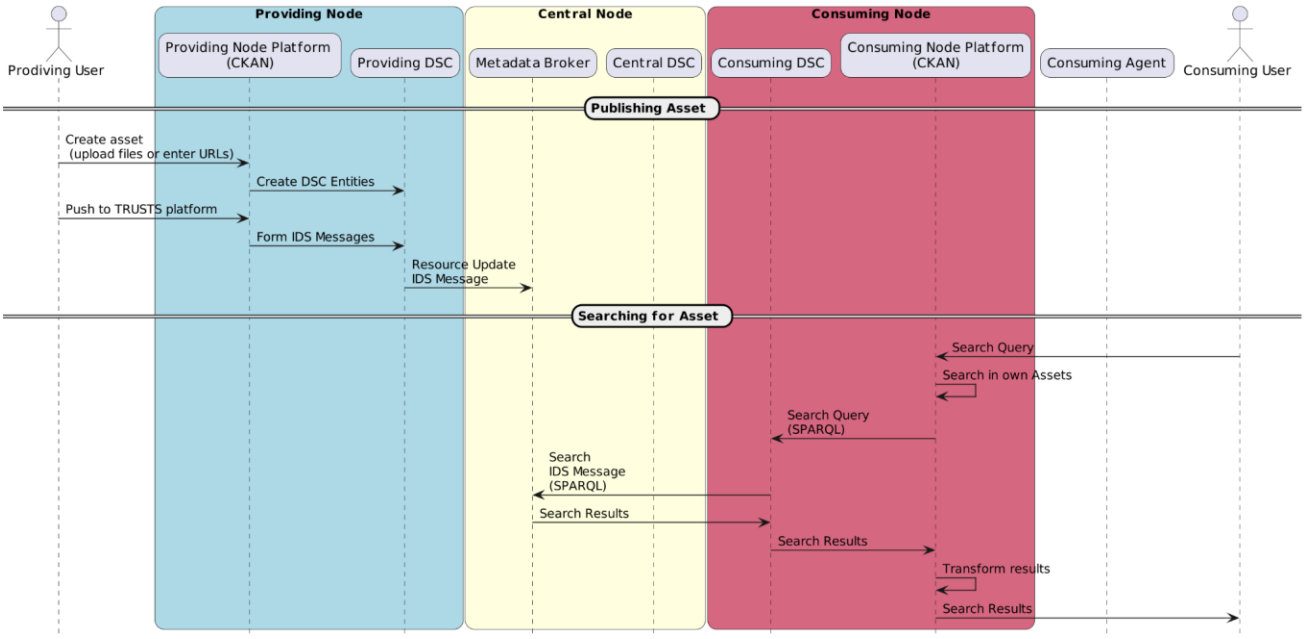


Figure 9: Flows of Metadata in the TRUSTS Platform (From Deliverable D3.8)

For the metadata flowing in the TRUSTS platform to be correctly understood by the different components, and acted upon in a previsible and consistent manner, explicit semantics are needed. For this, the TRUSTS-IM serves as scaffolding, as it defines what the different properties and attributes of entities mean. Based on the IDS-IM, the TRUSTS-IM is expressed as a collection of ontologies and controlled vocabularies. The management and exploitation of these vocabularies in the TRUSTS platform is based on the PoolParty Thesaurus Manager and the newly-developed Vocabulary Extension from CKAN. In brief, the vocabularies are accessible to, and automatically synchronised between different nodes as they are being edited and updated in a centralised fashion. The vocabularies themselves have been collected in the frame of this task, with a first version already online and serving the platform's prototypes, and a governance model described in D3.8 from where further updates and maintenance will follow.

Task 3.5 Platform Development & Integration

During the third and last year of the TRUSTS project, Task 3.5 continued the development and integration of the TRUSTS platform delivering new Minimum Viable Products (MVP.v2, MVP.v3, and MVP.v4). The final year of the project was very productive and major changes were made to the platform. We continued the adoption of new versions of the IDS Dataspace Connecter and IDS Metadata Broker, focusing on functionality (datasets, services, and applications offered, contract creation and access control) and secure communication between nodes. We have decided to use an open source IDS DAPS component as an authentication service. The notification service was developed and integrated and especially thanks to the contribution of all WP3 partners the end of project version of the platform was created according to functional requirements.

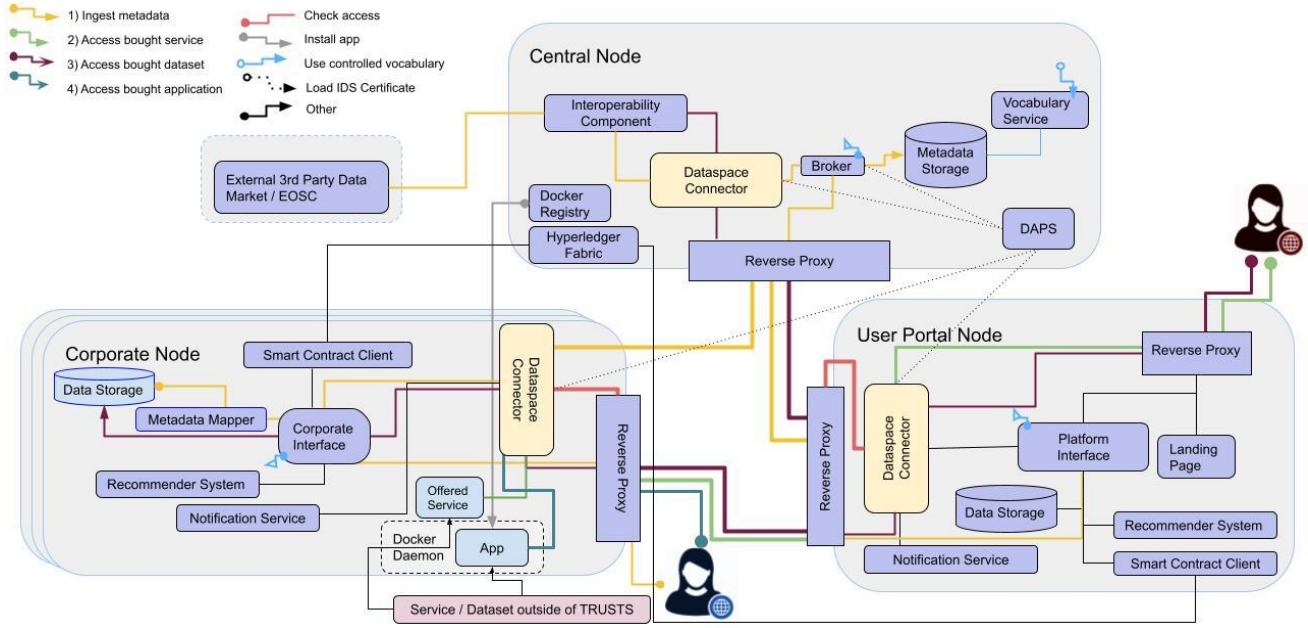


Figure 10: Platform Architecture

The end of project version of the platform architecture has great changes compared to the previous one. We continue to use CKAN as the main UI interface that was enriched with new functionalities and brand new designs from our partners. During this period new components, like contracting (new UI interfaces), recommender, smart contract, landing page, notification service, metadata mapper, were added to the platform. Our partners from WP5 were trained each time when a new version of the platform was deployed to gcloud and the WP5 trials were conducted with active participation of the WP3 team.

Below we have listed a direct comparison of a few pages, to help the reader understand the extent of the redesigning of the default CKAN UIs:

- Figure 11 displays the user dashboard before (on the left) and after the redesigning (on the right)

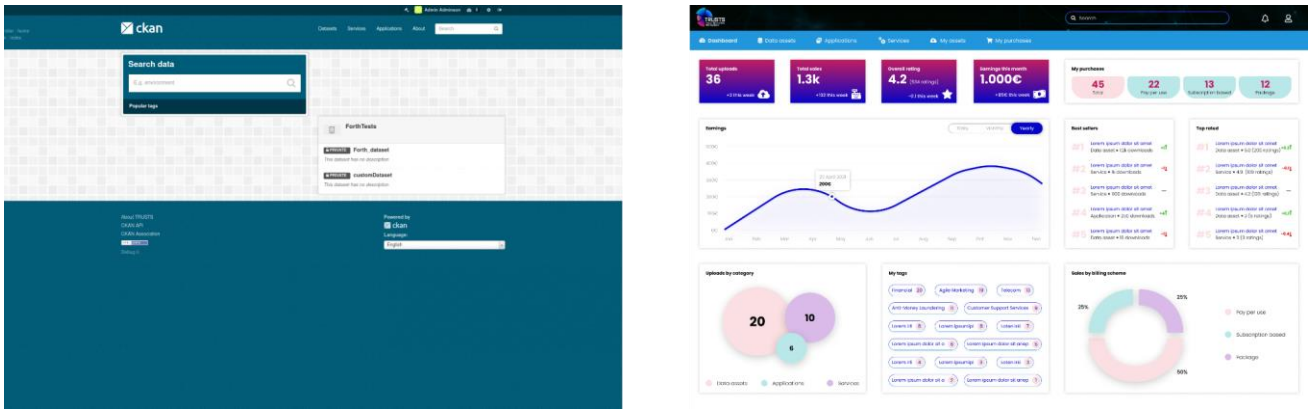


Figure 11: CKAN user dashboard before (left) and after (right) the UI revamp

- Figure 12 displays the search page before (on the left) and after the redesigning (on the right)

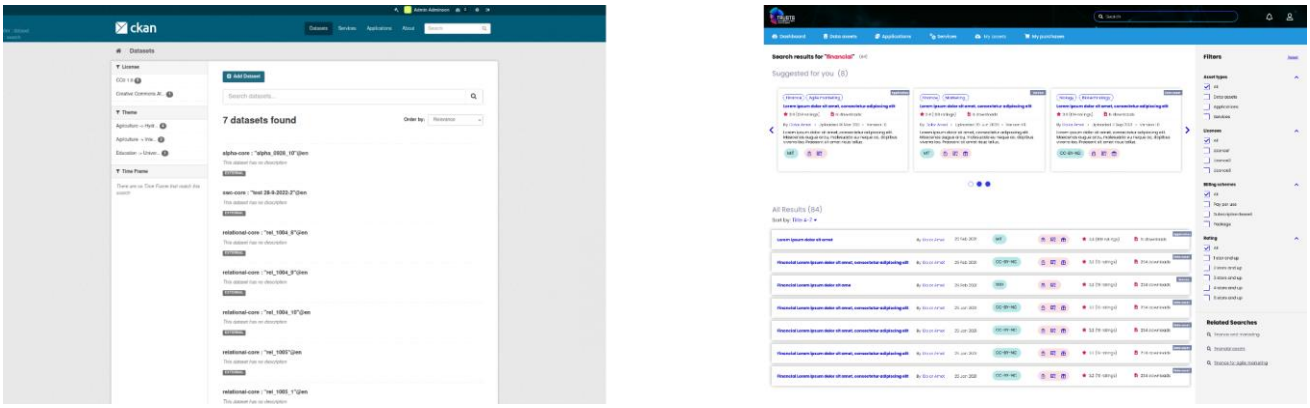


Figure 12: CKAN search results page before (left) and after (right) the UI revamp

- Figure 13 displays the user profile page before (on the left) and after the redesigning (on the right)

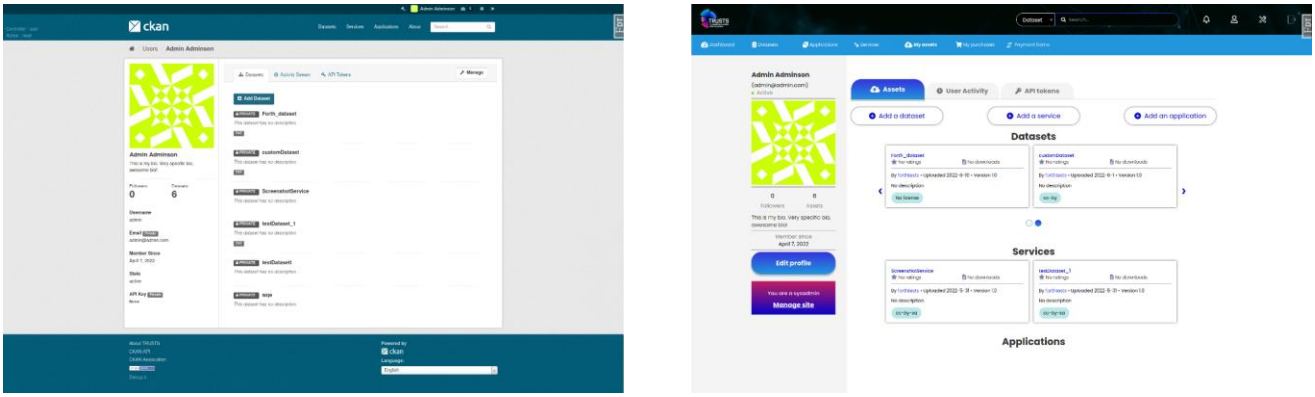


Figure 13: CKAN user profile page before (left) and after (right) the UI revamp

The partners tried to preserve as much as possible of the original CKAN functionality, but also give a breath of fresh air into the platform, as well as try to add some extra functionality that may prove useful in the TRUSTS platform context. We have to mention that the screenshots of both old and new versions, are indicative of what should be available by the time version TRUSTS 1.0 is released in January 2023.

Task 3.6 User and corporate profiles and brokerage

In the third and final year of TRUSTS, we provided an updated and final description of the functional requirements and the service interfaces of the TRUSTS recommender system. We also worked on the full integration of the recommender system in the TRUSTS platform. Additionally, we worked on the offline evaluation based on interaction data we gathered from the dataset and service sharing platform OpenML. Our offline evaluation results showed that collaborative-based recommendations (i.e., Collaborative Filtering) are the most accurate ones. However, we also find that content-based recommendations (i.e., Content-based Filtering) are the least popularity-based ones that also provide the highest dataset and algorithm coverage. This is in line with the fundamental accuracy-popularity bias trade-off present in recommender systems.

Taken together, the results achieved in T3.6 are three-fold:

1) From an evaluation perspective, T3.6 used publicly available data from the OpenML data and service sharing platform to evaluate the TRUSTS recommender system. This also allowed us to fine-tune the recommendation algorithms, and we shared our created OpenML dataset with the research community.

2) From a research perspective, T3.6 contributed five scientific publications. This includes a paper presented at ECIR'2021 conference on privacy aspects of recommender systems, as well as two papers presented at ECIR'2022 conference on popularity bias in recommender systems. In a third paper at ECIR'2023, we will present the ScaR recommender framework, which was also used to implement the TRUSTS recommender system. Additionally, we will present a paper in the DataEconomy workshop in 2023 on our offline recommender evaluation using OpenML data.

3) From a technical point of view, T3.6 fully integrated the recommender system into the IDS-based infrastructure of the TRUSTS platform. Specifically, this led to the implementation of the 15 services shown in the following figure:

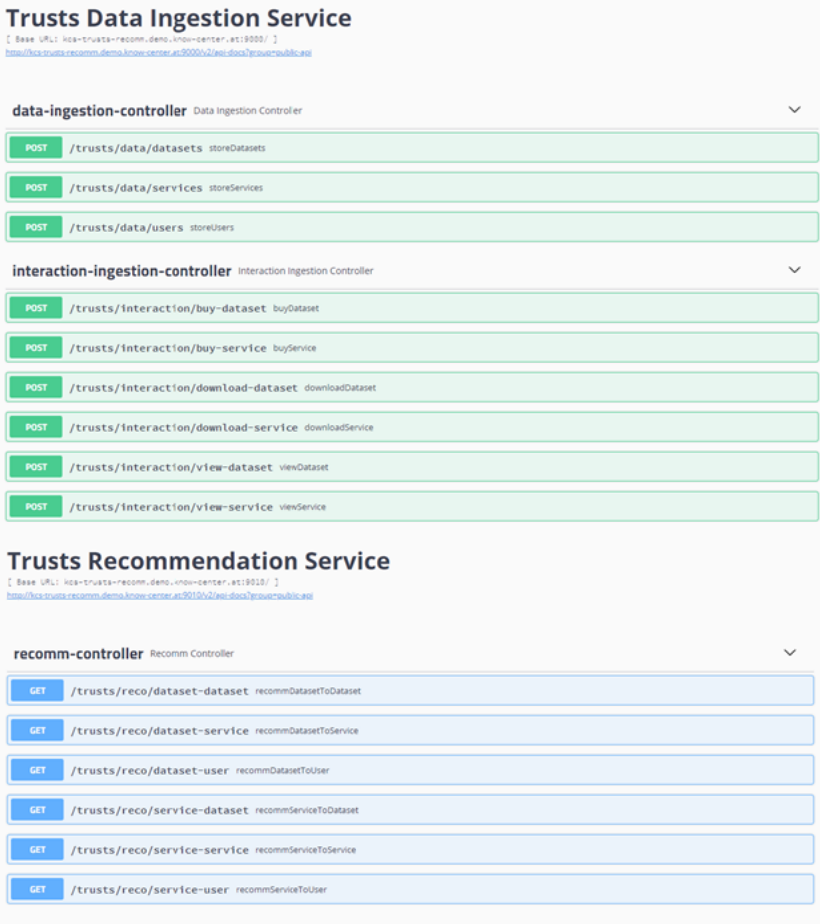


Figure 14: Services implemented by the recommender system

3.3.3 Future Outlook

Task 3.1 Infrastructure set-up and technical operations

The infrastructure that has been setup for the TRUSTS project, to support the development and to simulate a marketplace environment has been designed as a development/ test environment. It will be available for two months after the end of the project in order to support the period until the project review. After that period, it will be offline, although if any partner would like to use it, an agreement related to the availability and the costs can be made.

Furthermore, all the documentation and the information related to setting up such an infrastructure is already available through the project deliverables, in order for any interested party to be able to set up such an infrastructure. Special consideration should be made though, if a production grade infrastructure needs to be set up.

Task 3.2 Smart Contracts

Task 3.2 provides conceptual and technical foundations relating to setting up a smart contract infrastructure for a data sharing platform. One could leverage the results of this task in a variety of ways, for example taking the privacy and security outputs to develop a smart contract system which accounts for some of the more prominent attacks on these kinds of systems. Dell EMC intends to utilise the smart contract demonstrator work as a basis for further investigation of blockchain and smart contract security issues post-project, specifically the issue of illegal content being placed on blockchain platforms via exploiting freely-editable input fields is of particular interest. The payment compatibility demonstrator showcases how one can utilise more conventional payment systems in conjunction with smart contracts while still leveraging the blockchain's integrity guarantees, as opposed to using tokens or cryptocurrencies in tandem with the blockchain and Dell EMC is also interested in further exploration of this approach. Both the security research and payment system research will see the work of task 3.2 furthered after project-end.

Task 3.3 Data marketplace interoperability solutions

Task 3.3 had the research of interoperability methods as its focus. The goal was to create interoperability solutions to exchange data with potential external datamarkets on the one hand, and with EOSC initiatives on the other hand. The research showed the complexity involved in the creation of interoperability solutions, which results from the diversity and heterogeneity of different technological systems.

For the aspect of EOSC, two connectors were created, which are solutions to access data from the two initiatives OpenAIRE and Europeana. The connectors use an ETL process to acquire the data from the respective two initiatives, transform their metadata into a format understood by the TRUSTS platform, and to ultimately map the external metadata catalogues into TRUSTS. Consequently, the offerings of these two initiatives can be made visible from within TRUSTS. RSA aims to utilise these two connectors in the context of future work and research in the area of data spaces, especially in the domains of green technologies and cultural heritage. The connectors help to make the data from those two initiatives available in respective data spaces, which allows for the future creation of innovative data-driven applications. Furthermore, this path is in line with the goals of GAIA-X, which aims at the creation of a data-driven economy within Europe.

Task 3.4 Data Governance: Metadata, Lineage and Semantic Layer

- Refinement and publishing of the TRUSTS-IM.
- Test of the TRUSTS-IM in a real world use case where monetary transactions are involved.
- Extend the list of vocabularies used, to synchronise with what is used in other initiatives like EOSC, which are not done yet with implementation.

The TRUSTS information model has been successfully used so far for the use cases tested in the project. Minor adjustments have been made to it, namely the inclusion of more provenance related predicates and the expansion of some vocabularies. With these refinements in place, the TRUSTS-IM can now be published in the form of Linked Data, along with textual documentation detailing the enhancements over the IDS-IM. Afterwards, testing the TRUSTS-IM in a real case scenario where monetary transactions are involved shall be pursued. In particular, processing-of-payment and order-fulfilment predicates are not included so far, so requirements for them must be further elicited.

The list of vocabularies shall be continuously updated to keep up to date to what is used in other similar initiatives. In particular, as Gaia-X and EOSC take off, it would be advantageous to allow for semantic interoperability with them by means of vocabulary adoption or, in case of need, alignment. Future initiatives will, for sure, further refine the European vocabulary landscape, including in the legal and regulatory sense (e.g. Data Governance Act). The TRUSTS-IM must keep up to date with these if the outcomes of the project is to remain valid in years to come.

Task 3.5 Platform Development & Integration

Process of development and integration of the TRUSTS platform showed the complexity of creating a Secured Federation of Data Marketplaces. Using existing open source components has some types of difficulties, but nevertheless we have integrated a lot of components to the viable platform that has features of Federation of Data Marketplaces. Providers can offer datasets, applications and services to all participants of the data market. Consumers can search, select and buy all data assets through secured channels using mutual authentication on both contracting sides. It is very important that as based components were used IDS software like Dataspace Connector, Metadata Broker and DAPS server, that helps us to move to some sort of standardisation of data markets. IDS Information Model is the main part of data exchange in the built communication infrastructure.

During the process of platform building a lot of open source components were evaluated and intensive work was done on their adoption.New components were also developed by the whole team of WP3, this granted all participants very valuable experience in creating, supporting, and improving data marketplaces. The final product covers all aspects and features that any data marketplace should have, such as secured communication, selling, buying, immutable transaction logging, friendly user interface, recommendation system, and easy way of onboarding.

Important to say that the TRUSTS platform was intensively tested from the WP5 team that is indication of readincy to use.

Task 3.6 User and corporate profiles and brokerage

The work done in T3.6 on recommender systems for dataset and service sharing platform will be beneficial for future projects in the field of data markets and data economies. Our research has shown (i) how to implement recommender systems in such a setting, and (ii) how to evaluate recommender systems with

respect to different trade-offs (e.g., accuracy-popularity bias). However, future work also needs to take the monetization factor into account, which we have neglected so far.

Additionally, our research on privacy aspects in recommender systems addresses a very timely topic in light of the GDPR. Here, we have shown that machine learning techniques such as meta learning can help to reduce the personal data needed to generate accurate recommendations. Here, future work should focus on combining privacy-preserving technologies such as differential privacy with recommender systems to add privacy guarantees and to increase the trust in recommender systems.

Finally, our evaluation of the TRUSTS recommender system was conducted solely in an offline-based manner. This enabled us to test the applicability of the recommender algorithms before integrating them into the TRUSTS platform. However, offline evaluation results do not necessarily need to correlate with online evaluation results. Thus, future work should also focus on evaluating the user acceptance of the recommendations in the running TRUSTS platform after project end.

3.4 WP4 Privacy preserving technologies

3.4.1 Objectives

Data privacy is a global concern due to threats and risks that can harm individual security, reputation, and lead to negative social exposure. In recent years, many countries have been ruling on the activities related to data collection, transfer, storage, management, and deletion, to mitigate privacy risks and assure civil rights on personal data, especially in the European Union with the General Data Protection Regulation (GDPR). The terms of such regulations play an important role in the development of Machine Learning (ML) and Deep Learning (DL) models that exploit personal data. Therefore, privacy-enhancing technologies (PETs) that eliminate or limit the amount of private information in datasets have been developed and integrated into ML/DL models. PETs like differential privacy, homomorphic encryption (HE), Federated Learning (FL), secure components, multi-party computation (MPC), and adversarial training have been successfully applied to real-world systems. Furthermore, tools for measuring data de-anonymization and/or mitigating its anonymizability have been proposed to tackle the problem.

Advanced decision-making capabilities are required for broad areas and arise from the improvements of data science along with the technical ability to draw advanced conclusions based on big data. These capabilities have been proven when it comes to public data. However, for private or personal data, there still exists the requirement to develop a technology platform that will allow the execution of advanced techniques for data analytics alongside the complete prevention of data breaches that may endanger privacy. Furthermore, regulatory constraints and the desire to preserve individuals' privacy uphold the accomplishment of this requirement, which is the main objective of this work package.

This WP has the objective of integrating privacy-preserving mechanisms to TRUSTS in order to safeguard the UCs in the financial domain from privacy threats. In addition, data trading and sharing activities will also be protected. Furthermore, WP4 has the objective to provide tools for anonymization and de-anonymization.

Because personal private data trading is not possible in the ordinary sense of the word, WP4 is required to develop the ability to support data processing without compromising data privacy. Throughout the project WP4 works in full collaboration with the UC leaders and the WPs leaders in order to adapt the research perfectly to the system requirements and the UCs requirements.

T4.3 Anonymization and de-anonymization

The objective of task 4.3 is to develop a tool that combines risk analysis and anonymisation to provide an integrated solution for the secure processing of personal information. The specific aims of this task are supporting to:

1. *Raising awareness* for de-anonymisation risks and providing appropriate anonymization methods.
2. Helping to be *compliant with GDPR* and help the data controller to become aware of potential de-anonymization risks.
3. Design appropriate *anonymisation methods* based on the risk analysis methods developed.

T4.4 Federated Deep Learning methodologies [M18-36]

This task constitutes a horizontal layer of the TRUSTS architecture facilitating the federated training and utilisation of the envisaged DL algorithms, which will be incorporated in the platform, by distributed devices, running on the edge of the system's cloud. A cloud based framework will be deployed enabling the distribution, training, inference, monitoring and update of existing AI models to selected distributed clients, which will be able to utilise local isolated content repositories. To this end, each federated deployment is enabled to use private or sensitive datasets for the generation of the necessary feedback to the TRUSTS platform, without endangering their unauthorised access or exposing the data source.

T4.5 Transformation of algorithms to privacy-preserving certified [M18-36]

This task will strive to convert risky algorithms that compromise privacy into safe and privacy-preserving without harming their functionality. Various algorithms ought to use external sources and run computation to execute certain functions. The development of most algorithms is driven by outcome and performance, leaving privacy and security issues on the least of requirements. The challenge is in retrofitting and enabling working algorithms to perform under the desired set of privacy regulations without the need of redevelopment.

3.4.2 Results achieved

T4.1 and T4.2 were fully finalised and the outcomes of it were reported in D4.1. [M18]

T4.1 Privacy Preserving Data Analytics

Cryptographic primitives involved in building collaborative trust systems were investigated.
Fully homomorphic encryption (FHE) – Setting up an FHE framework will allow you to do outsource computation without giving up any privacy and without having to trust the service provider, since they are not able to access the actual content of your data.
Secure multi-party computation – Secure MPC provides similar confidentiality and privacy in the real-world, where one cannot fully trust third parties. Therefore, what can be achieved in the ideal-world, can also be done by applying secure MPC.
Private Set Intersection (PSI) – Private set intersection is a special-purpose secure MPC. It allows two participants to compute the intersection of their data sets.
A PSI application was developed.
Homomorphic Encryption versus Multi-Party Computation – FHE is a good choice in the classical client-server setting, whereas MPC prevails whenever at least two parties actively perform a computation. The nature of FHE fits an infrastructure that can be widely found on the internet. On the one side, we have a weak client device, like an edge device, a smartphone, or a laptop with input data. On the other side, there is a powerful server (computationally or application-wise). Usually, the client provides input data to the server because it offers a useful application to the client (which the client cannot do on his own). In this scenario, the server performs all the computation. The client only provides input data and could go offline during the computation. This perfectly matches the FHE design. In FHE, the client encrypts its data, sends it to the server, which does all the computations, and then sends back the result to the client.

In contrast, MPC is a technology that allows computations with two or more input parties. This much greater flexibility comes with the cost that each party has to take part in the computation actively.
To sum up, for a client-server, setting FHE is a proper choice. In all other cases, one would use MPC-protocols, sometimes also combining them with FHE.

T4.2 Privacy Preserving Transfer Learning and Classification

Task 4.2 Privacy Preserving Transfer Learning and Classification, which has run from M1 to M18, presented the challenge of bridging the gap between Transfer Learning (TL) and privacy-preserving methods of HE and DP for privacy-sensitive datasets. As a result, a private, efficient, and secure TL method, namely CryptoTL, was proposed and had its efficiency tested over publicly available benchmarks datasets for the natural language processing task of text classification. Therefore, CryptoTL allows for the first time to efficiently train deep learning networks even though all involved datasets are protected by HE. Furthermore, due to the usage of TL the resulting model achieves high accuracy for tasks where only a very small training dataset is present. The CryptoTL architecture can be seen in Figure 15.

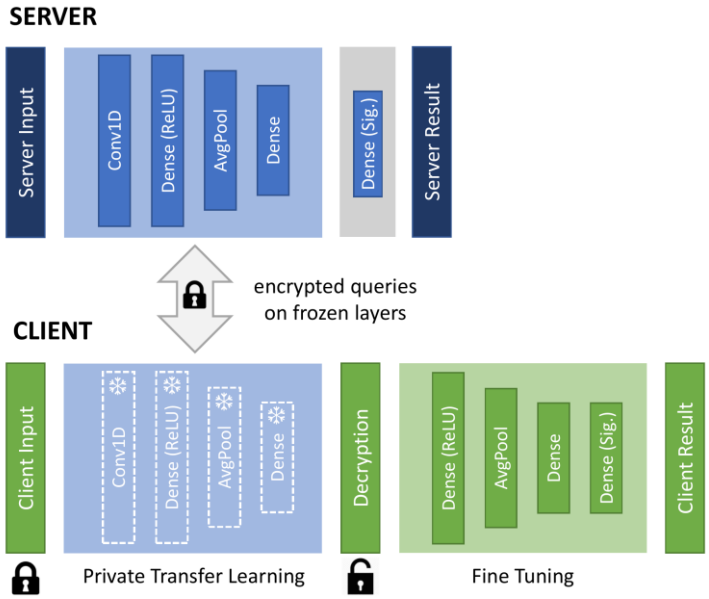


Figure 15: CryptoTL architecture scheme[3]

The main advantages of the CryptoTL can be summarised as follows:

- Due to using TL, an accurate network is trained for a task where only a small dataset is available.
- Due to the usage of HE and DP all datasets are protected.
- Since HE is only applied to classifications in the forward direction, CryptoTL allows for the first time to efficiently train a network on HE-protected data.
- HE is only applied to a small network, achieving very fast runtimes of just 1s (on a notebook CPU) for one forward pass through the network.

To emphasise the functionality of CryptoTL for scenarios featuring scarce data, we reduced the available target training dataset in multiple steps down to 1% of its original size and trained a CryptoTL model with high accuracy. The resulting accuracies for training a model for a dataset from Twitter posts based on a dataset from IMDB movie reviews can be seen in Figure 16, which also shows the result for a CNN purely trained on the target dataset. This figure clearly shows the high accuracy gains when employing CryptoTL for very small datasets.

[3] The lower CNN layers on the server are frozen after training and a client can query homomorphically encrypted input on these layers. The private source domain data can be additionally secured by DP. After the query new top layers are added at the client to fine tune the pre-trained CNN to the target domain data. The fine tuning does not have to be encrypted anymore since it is performed locally at the client.

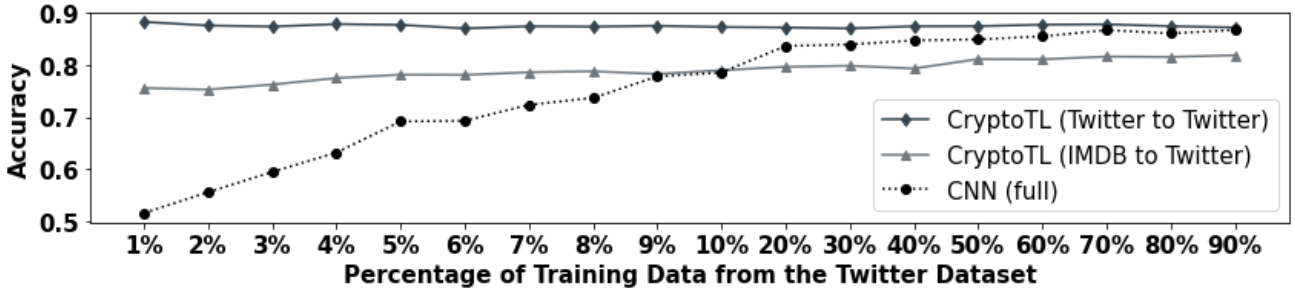


Figure 16: CryptoTL results against the full CNN (without TL) baseline varying the percentage of data sampled from the training set of the target data (Twitter) for fine-tuning

Beyond coming up with novelty regarding the combination of TL with HE and DP, this framework has potential to be applied to many other real-world use cases. As future works, CryptoTL is expected to be extended to data types other than textual data, e.g., financial data, in order to preserve data privacy in a larger number of applications. Finally, the research outputs of Task 4.2 were submitted as a research paper for the *Financial Cryptography and Data Security 2023* conference.

The protection of privacy is not always accompanied by the mitigation of downstream privacy-related issues, such as the prevalence of human-discriminatory biases on DL models or in their decision-making outcomes. Some PETs may worsen this drawback of privacy protection, especially DP, which has been found to discriminate against social groups by reducing model accuracy for them more drastically than others. DP-based optimizers, such as DP-SGD, are particularly sensitive to fairness issues. Since CryptoTL uses such optimizers, we intend to extend its experimental evaluation to datasets including features that may trigger discriminatory outputs by the model. In Figure 17, we depict an example of a classification task involving TL on data from different social groups. Developing strategies for enabling fairness for DP in such settings is also a research direction for our work, whose findings are to be submitted as a full research paper soon. The research paper is currently in its final phase.

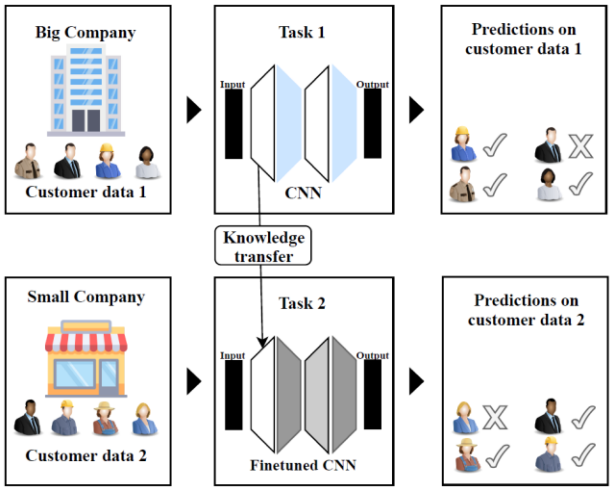


Figure 17: An example of knowledge transfer between two tasks with data from different social groups

T4.3 Anonymization and de-anonymization

Following the focus on developing de-anonymisation risk analysis modules in the first half, the focus shifted to corresponding anonymisation methods in the second half of the project. An application was created by RSA and FORTH that combines both - risk analysis and anonymisation. The risk analysis built upon the results of the Safe-DEED project (Bampoulidis, 2020a) and has reduced its limitations.

An overview of the risk analysis component improvements:

- Generalisation: The tool is now no longer limited to the data sets available in Safe-DEED.
- Extension of the data types: The support of different data types has been extended. New additions are spatiotemporal and textual data.
- New privacy model: Not only k-anonymity is supported, but now also l-diversity.
- Application: In cooperation with FORTH, a professional application for risk analysis was developed, which simplifies the operation and makes it more accessible.

In the final step of the task, corresponding anonymisation methods were identified and implemented. The aim was to offer corresponding anonymisation methods based on the results of the risk analysis. With this in mind, the application architecture was updated and expanded with a new anonymisation component. Furthermore, expert feedback was taken into account and the UI was significantly revised. The visualisations have become more appealing and informative. For the anonymisation of the datatypes the methods have been identified:

- Tabular data (Hierarchies)
- Aggregated data (Hierarchies and Microaggregation)
- Invoice data (Hierarchies, Bucketization and Clustering)
- Textual data (Named entity recognition and sentiment analysis)
- Location data (Clustering)

In the following, each of the complex and high-dimensional data types are discussed in detail. The complete process is shown in each case. This means the risk analysis on the one hand and the corresponding anonymisation methods on the other. All of the methods presented were integrated into the application:

Tabular data: In addition to complex and high-dimensional data, conventional tabular data sets are also supported. This includes all tabular data sets that do not contain an additional dimension such as time and location or aggregated values. Anonymisation of tabular data is done with the utilisation of hierarchies. With the help of these hierarchies, the data controller defines rules for anonymisation and the data is anonymised on the basis of these rules. For this data type 2 different privacy models are available: (1) k-anonymity and (2) l-diversity. Figure 18 demonstrates the visualisation of the risk analysis of a tabular dataset with enhanced tooltips and legends.

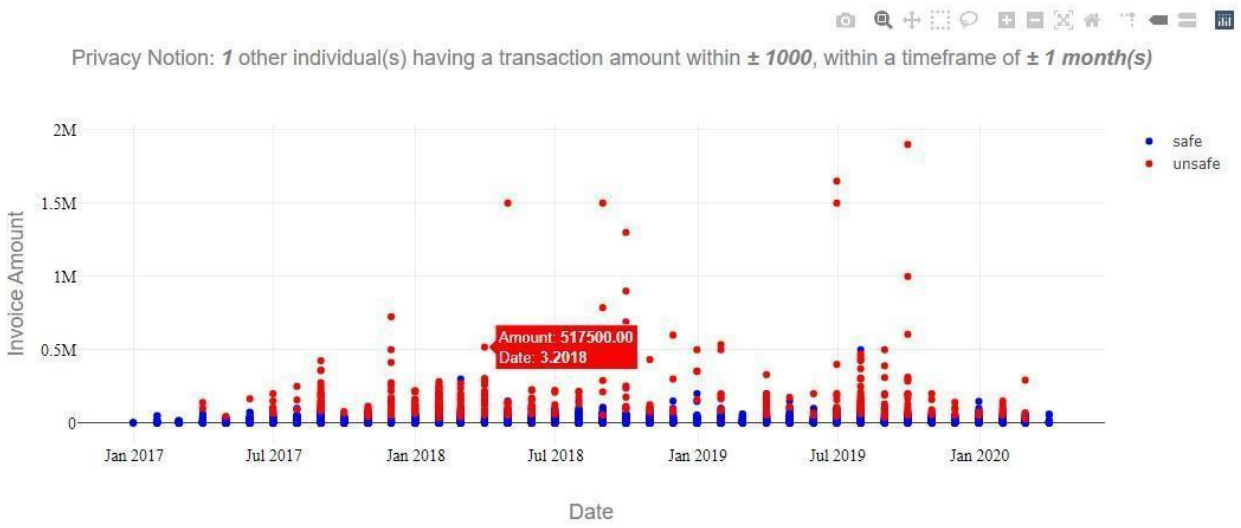


Figure 18: Examples of enhanced visualisations with more descriptive tooltips and legends

Spatiotemporal Data: Spatiotemporal data combines location and time of individuals. Therefore it consists of two dimensions: (1) geographical information (e.g., location) and (2) information about time. Figure 19 shows the enhanced UI with more descriptive legend and tooltips. For anonymisation of the location data we use a clustering approach which combines locations which are close to each other according to the desired k-value.

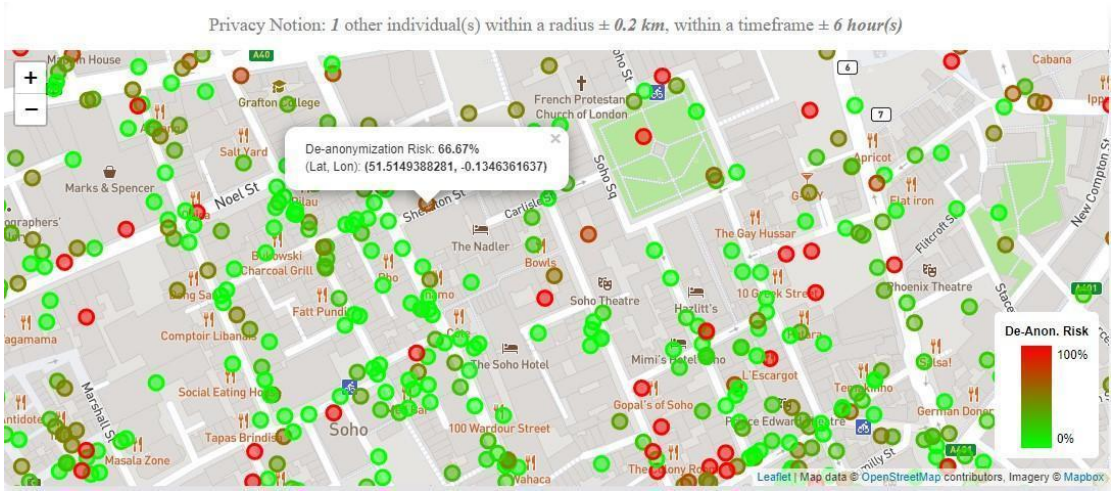


Figure 19: Screenshot of the enhanced output for spatiotemporal data risk analysis (gowalla dataset)

Textual Data: The category Textual Data includes all data sets that mainly consist of long text-based information. Examples are comments in social media, product reviews in webshops or blog posts. Figure 20 demonstrates the output of the risk analysis. Two different anonymisation methods were developed for addressing this category within the framework of the project: (1) Sentiment analysis, the respective text entries are replaced with the sentiment of the post. For example, whether the review was positive or negative. In this case, a large part of the text is replaced, but the information about the opinion is retained. And (2) automatic identification of named entities, methods from the field of natural language processing (NLP) are used to automatically recognise and replace named entities. The data controller can decide which

type (location, persons and organisations) he wants to have anonymised.

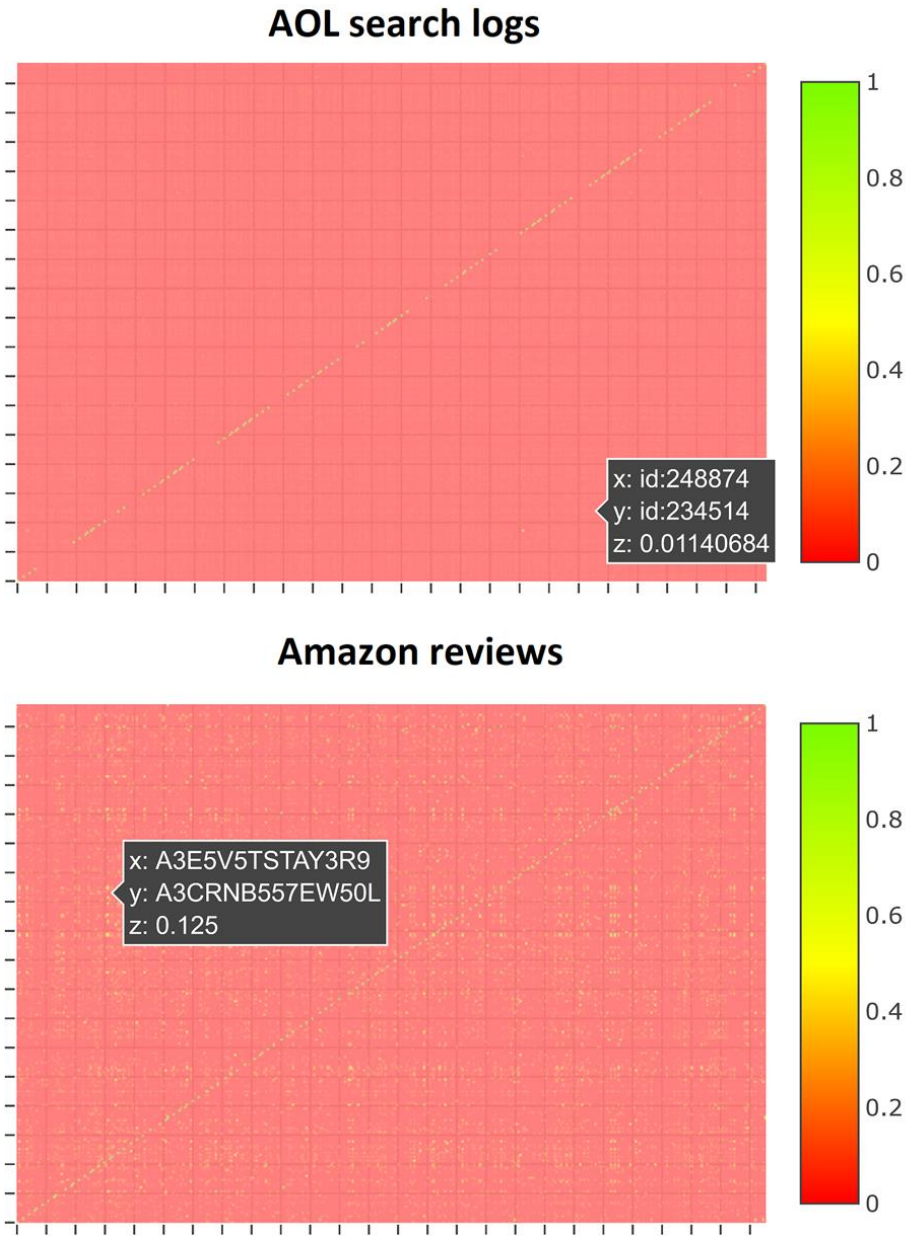


Figure 20: AOL search logs and amazon reviews

Financial Transactions Data contains two different dimensions, on the one hand the financial information and on the other hand the time dimension. They show at what time and with what value the transaction took place. Figure 21 shows the enhanced visualisation of the risk analysis results. Three different anonymisation methods were implemented for the anonymisation component. Here, depending on the output of the visualisation, the data controller can decide which anonymisation method is best suited for the respective data set. For example, if there are many similar values close to each other, it might make sense to combine them into a range using a self-created hierarchy. The other two methods are automatically combining values and group them together according to statistical criteria without additional user input.

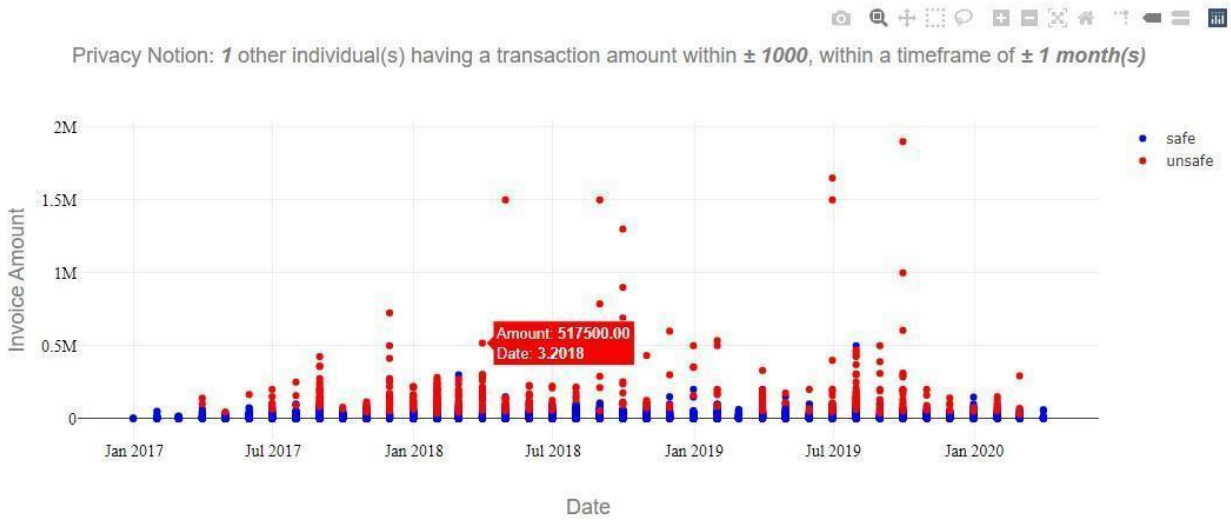


Figure 21: Enhanced point plot for financial datasets

Aggregation-Based Data: This data type contains values that have already been processed. These can be operations such as sum, number, average, etc. Figure 22 shows the visualised results of the risk analysis. Two different methods were developed for anonymisation: (1) generalisation with hierarchies, where the data controller independently defined hierarchies, and (2) microaggregation, where the time dimensions are grouped together and the transaction values aggregated accordingly. Here, the data controller can choose on which level (day, month, year) the anonymisation takes place.

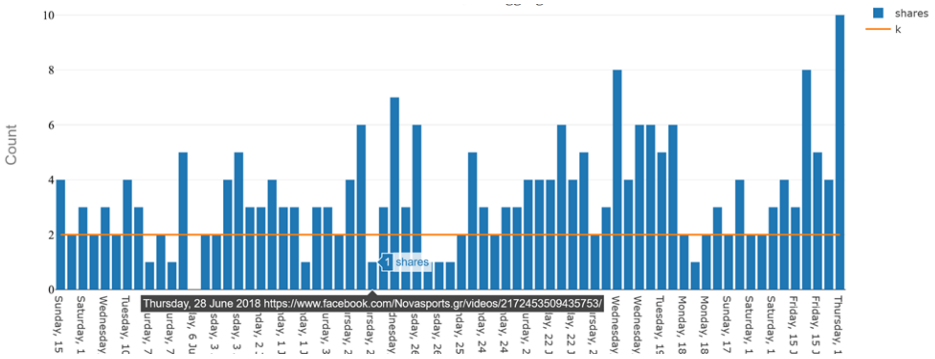


Figure 22: Bar chart for aggregation-based data

Application

The application developed by FORTH constitutes a read-to-use toolkit, designed and developed for incorporating the aforementioned risk analysis and anonymization methods while also providing end users with an intuitive and usable UI. The tool was created in a loosely coupled manner, with each component being a standalone entity in its own Docker image. A single docker-compose file is used to deploy all of the tool's components/images. The main components of the tool's architecture are the following:

- The *Frontend/GUI* of the application.
- The *Coordinator Server*, which is responsible for the necessary backend operations regarding the coordination of the backend components according to specific workflows.

- The *Risk Analysis Server* as well as the recently introduced *Anonymization Server* both developed by RSA which undertakes the ingestion of the dataset as well as the execution of the risk analysis and anonymization processes described in this section.

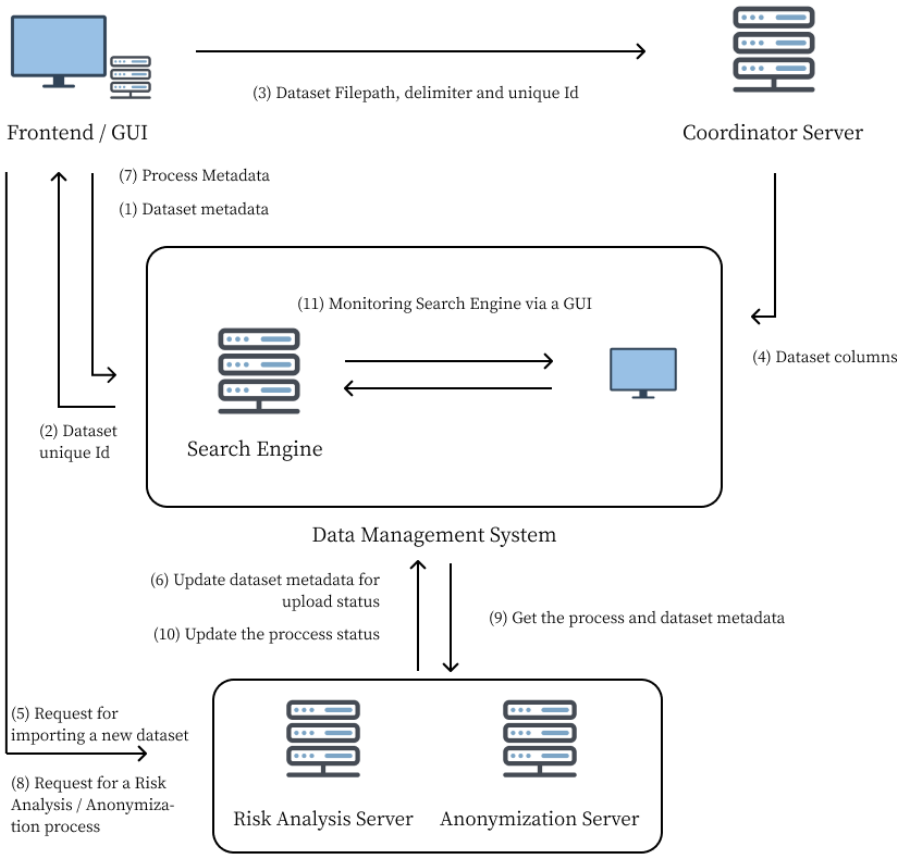


Figure 23: Updated architecture including the anonymization component

T4.4 Federated Deep Learning methodologies

Generally, FL can be divided into two different types: Horizontal Federated Learning (HFL) and Vertical Federated Learning (VFL). HFL is introduced in scenarios where datasets share the same feature space but are different in sample. Collaboration via HFL rarely occurs when it comes to different companies and different domains, but it is very common in telecommunication use cases for example. In contrast, VFL is applicable to use cases where two data sets share the same sample ID space but differ in feature space. This scenario is much more common in the industry and constitutes our focus in the TRUSTS project.

We started with a kick-off of our research efforts focusing on VFL techniques that will enable TRUSTS parties to collaborate over their private and sensitive data while preserving data privacy. We began with a survey of recently published research papers related to privacy challenges for FL applications, such as open search and recommender systems. In these scenarios FL has been found as an efficient solution against data leakage. However, open challenges still prevail, for example related to unintended memorization of data instances by the federated model. Such data instances may represent users' personal information, preferences, or behaviour. A corresponding overview was presented at the 3rd International Open Search Symposium and

we also started implementing a FL prototype for textual data.

In a separate publication, we systematically reviewed privacy-preserving DL models used for natural language processing tasks, including those applied to distributed settings such as FL. Textual data may include private information implicitly, such as the context of a sentence or the sentiment polarity associated with text topics, such as politics and demographics. Since the TRUSTS platform is expected to store data in different formats, which may include text, this systematic review frames the big picture of privacy risks, defenses, and tradeoffs for DL models combined with PETs. For further details, we recommend the reading of "How to keep text private? A systematic review of deep learning methods for privacy-preserving natural language processing" in Artificial Intelligence Review[4].

The evaluation of FL models has proved to be often limited to benchmarking the model performance on a task, without strong attention to side effects in terms of underlying privacy issues, such as unintended model memorization and the prediction of private attributes by the FL model. So, we started a study on the latter issue aiming at measuring how likely to encode and predict private information a FL model is. A LSTM-based prototype model was developed for FL tasks involving text data as aforementioned. In terms of training data size, we started our experiments on a data sample with over 50 million data instances. Beyond robustness to privacy risks we target our experiments for comparing FL training runtime for networks with different sets of parameters. The results and findings of our experiments are to be submitted for publication soon. As previously mentioned, this research paper is currently in its final phase.

In collaboration with Task 4.5., we also started to work on an encrypted FL version, based on a recently published multi-key HE scheme[5]. Here, the model updates of the FL system are encrypted using a homomorphic encryption scheme before sharing with a server for aggregation. This encryption prevents that the server learns the gradients from any client which would potentially allow it to deduce potentially private information about clients training data. Consequently, this greatly enhanced the security of typical FL algorithms and the published results also show that this scheme preserves model accuracy and reduces the computational cost compared to other secure solutions. While the public key is known to everyone, the corresponding decryption key is kept secret – each client only knows a share of the key. Thus, no-one can decrypt the gradient from an individual client, only all clients together will be able to decrypt the aggregated gradients. We depict a schematic description of FL using multi-key HE in the following image.

[4] https://link.springer.com/article/10.1007/s10462-022-10204-6
[5] https://arxiv.org/pdf/2104.06824.pdf

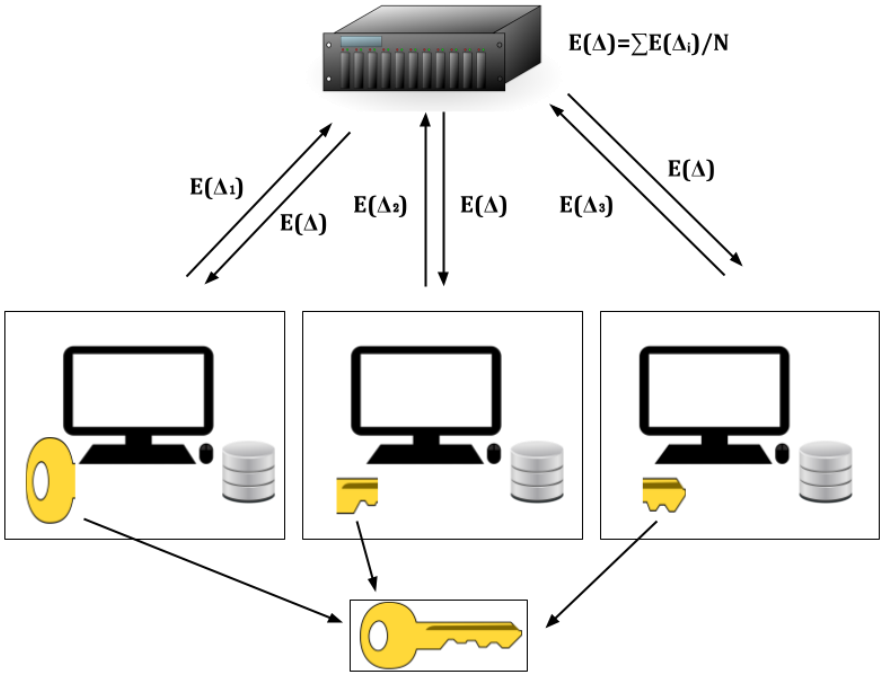


Figure 24: Schematic depiction of federated learning using multi-key homomorphic encryption

In order for this to work, the clients need to choose the shared public key in a certain way. This mandates a key exchange step before the actual training can start. The keys of the clients can be interpreted as an instance of a secret-sharing cryptographic scheme. The shared private key corresponding to the shared public key is never directly instantiated. It can be computed from different secrets held by the clients.

So, as long as at least one client does not collude with the others it is impossible to get hold of the shared private key and break privacy this way. However, if all clients but one collude, they can subtract their gradients from the sum of all gradients to get the gradients of the only honest client. This is a flaw inherent to every aggregation protocol. The protocol is thus secure if at least two clients do not collude. This is a strong privacy improvement over plain FL.

We have implemented this protocol in Apache SystemDS (Boehm et al., 2019, https://github.com/apache/systemds), an industry-strength ML software suite. Our code is also already merged into the original SystemDS codebase. We have made extensive performance tests to quantize the performance cost of using HE with FL. One benchmark can be seen in Figure 25 where we compare the runtime of FL for different numbers of workers with and without using HE. Our results hint that the overall runtime performance on a cluster is less than 10% worse using HE. The effectiveness of the learning process is not reduced. Interestingly, the contrary seems to be true. The random noise introduced by the HE scheme improves the learning efficiency. This is a known effect of adding randomness to the training calculations. The network overhead is approximately a factor of three. However, our experiments show that the networking and aggregation part do not contribute a lot to the overall runtime. The vast majority of the time is spent calculating the gradient updates. This part of the training stays unchanged with the HE protocol. We have chosen the parameters of the benchmark in a way that reduces network and aggregation overhead to a minimum.

Figure 25: Performance of model training with and without HE for different numbers of workers

T4.4 also continued our efforts from previous tasks based on ensemble learning, where multiple learning algorithms are used to obtain better predictive performance compared to any of the constituent learning algorithms individually. Following the assumption that the goal of any ML problem is to find a single model that best predicts our desired outcome, and since we can often not produce a model that is most accurate in all cases, ensemble methods take a myriad of models into account, and average these models to produce one final model. Thus the common approach to use ensemble learning is to train several models on the same dataset, and aggregate the results using one single ensemble model. In addition to our other implementations we have also followed this approach in collaboration with partners from UC2, the main idea is also related to FL. We have applied an ensemble model to aggregate distributed ML results for predicting/classifying the same problem, trained on different local datasets at servers of the involved parties.

This approach allows parties to collaborate with others in order to jointly solve a problem, without exposing their private data to each other and thus preserving the data privacy. Depending on the parties datasets, and their description, whether they have the same feature set or different feature set, there is a use case where the parties should share their trained model between each other in order to retrain the ensemble model avoiding the need of sharing their data for that purpose. Only the final results of local evaluations are aggregated, the actual training data is not shared with others. We also want to point out that the security guarantees for methods based on data aggregation (ensemble learning, FL), are different compared to encryption methods.

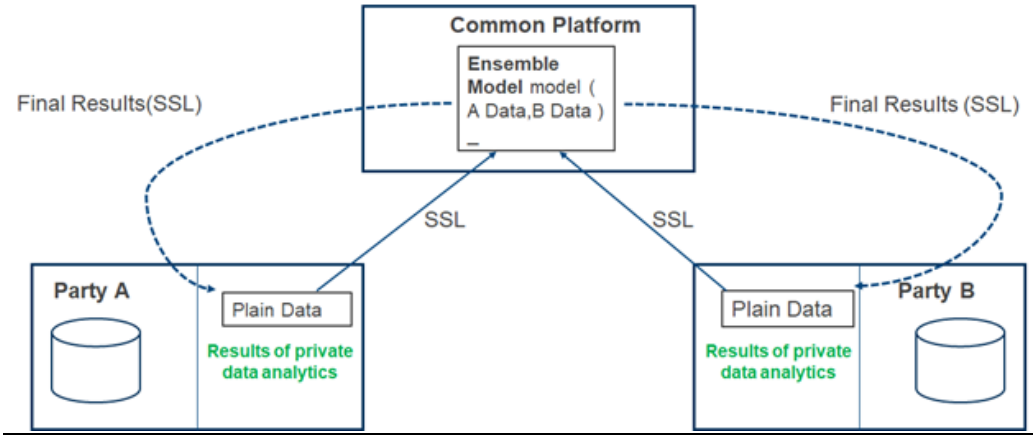


Figure 26: Common Platform for Federated Deep Learning

VFL using SHAP values:
SHAP values interpret the impact of having a certain value for a given feature in comparison to the prediction we'd make if that feature took some baseline value.
The suggested solution provides a capability to run classification ML algorithms over more than one datasets belonging to different and, at times, rival parties. Training is performed without sharing any of the raw data between the various parties, and the final model provides one single prediction while keeping data privacy and security.
The way to withhold these constraints is by running federated ML models, over each of the data sets separately, and then share only the SHAP values generated by each of the models.
The SHAP values from all of the federated ML are used as input to a new classification ML algorithm, which provides a single prediction based only on it incorporating the information from each dataset in the shape of SHAP values.

Superseded federated learning
All of the methods mentioned above require full collaboration of the involved parties from the training phase up to the inference one. This makes the collaboration too complex, and sometimes this complexity even prevents collaborations.
This method suggests a way to perform VFL while reducing the complexity of it by limiting the collaboration only to the training phase.
For having this we should use a generative adversarial network (GAN). Given a training set, this technique learns to generate new data with the same statistics as the training set. It is a ML model in which two neural networks compete with each to generate new, synthetic instances of data that can pass as real data - to become more accurate in their predictions.
GANs typically run unsupervised and use a cooperative zero-sum game framework to learn.

The stages to perform superseded FL are:

The pretraining stage:
The pretraining and training stages are almost like the VFL while superseded FL add another stage in the middle as described in the flowchart below:
First the parties use PSI to identify the common sample IDs across their datasets securely and privately (as per Figure 27 below).

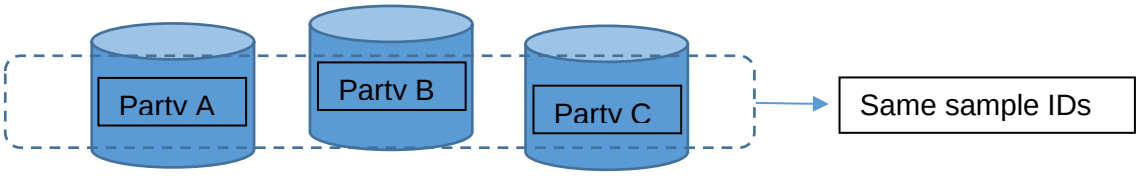


Figure 27: Common sample IDs cross datasets

Once they find out there is a logical sense to collaborate, each party creates a local model relevant to the collaboration purpose.
For each model, each party creates a GAN that simulates its data depending on the inputs.
A VFL model is created for all parties.
Each party shares its own model and a GAN with all involved parties.

The inference stage:
The second stage, the inference, is almost like HVL while superseded FL adds a stage prior the inference as described below:

1. When a party has a new record and wants to perform inference, it uses all party's GAN models (shared during training) to generate a complete data set.
2. The new data record plus the GAN models are used as inputs for all the models of the involved parties.
3. The results of each model are used as input into the VFL model to perform an inference.
4. Since the non overlapped data is simulated, the accuracy of the inference will increase in correlation to the number of the overlapped features (as per Figure 17 below).

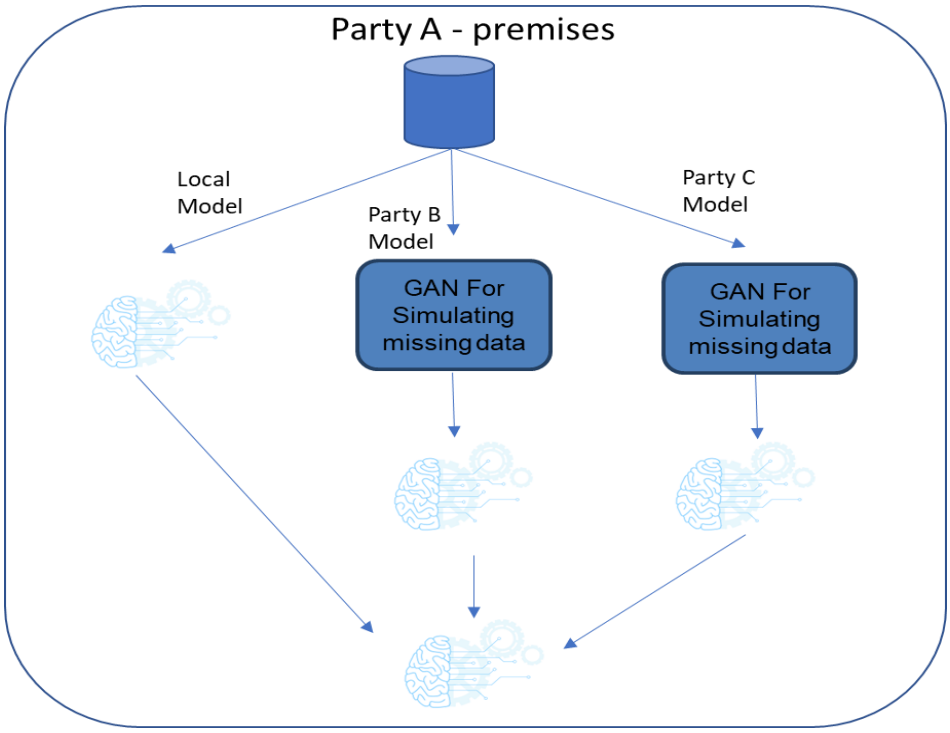


Figure 28: Superseded Federated Learning flow

T4.5 Transformation of algorithms to privacy-preserving certified

Our progress in this task is interlinked with the other tasks in WP4, where on one hand we continued with the development of our privacy-preserving solutions (e.g. our prototype for encrypted TL and the new library for private set intersection, both are outcomes of T4.1 and T4.2) and on the other we also started to work on more secure solutions for FL (T4.4) base for example on multikey HE as already described above.

We also included our PSI library to the software catalogue of EUHubs4Data and we wrote a newsletter contribution to inform about the functionalities of the new solution[6]. We additionally protected the communication channel between the two PSI parties using a TLS connection. For this, we used the *rustls* library, an implementation of TLS in the Rust programming language. Our implementation allows for both self-signed certificates, as well as traditional public-key infrastructure. We also carried out additional intensive benchmarks for one setting where both parties are in the same network (e.g. a datacenter in Frankfurt) and for two further settings where the two parties are in two separate geographical areas (Frankfurt-Paris and Frankfurt-Ohio). The benchmarks were executed on Amazon Web Services (AWS) EC2 servers with both parties running an Ubuntu Server 20.04 LTS image on a c5.xlarge configuration. The following graphic depicts the performance results with respect to the set size of the new PSI library for these settings.

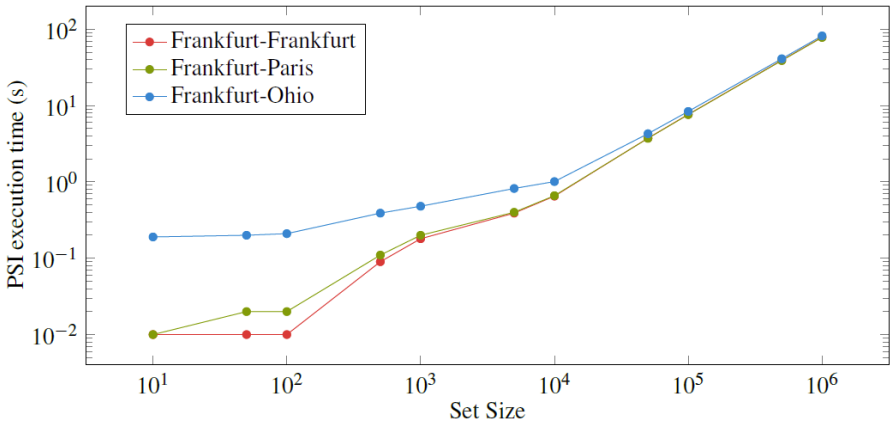


Figure 29: Relation of Performance Results to size of PSI Library

We can see that for small set sizes, the additional latency in the Frankfurt-Ohio scenario leads to an increased runtime, however, this small additional latency is insignificant for larger set sizes and the three different networking scenarios are practically identical in terms of runtime. We have compared these results to the prototype PSI solution that has been developed in the H2020 project SafeDEED, where only benchmarks of small data sets were possible due to the memory usage constraints of the old solution. The new PSI library is usually about 10x times faster than the old one and now also allows the usage of very large data sets. If both parties hold a set of 5 000 items, the new PSI demonstrator takes about 0.39s, while the old SafeDEED solution took 4.54s in the Frankfurt-Frankfurt scenario. The underlying PSI protocol used in the PSI demonstrator is suited to the scenario of imbalanced set sizes, where larger server set sizes are more beneficial for the protocol.

The latest version of our new PSI library is already in use by project partners and has been integrated into the

[6] https://www.trusts-data.eu/private-set-intersection/

prototypes of UC2.

3.4.3 Future Outlook

The tasks of the WP4 were completed. The conclusions and recommendations will be monitored and potentially adapted in light of the review conducted by the EC in February 2023.

3.5 WP5 Demonstration of the TRUSTS Platform in 3 business-oriented Use Cases

WP5 was led by eBOS, and the aim was to **demonstrate the TRUSTS Platform in three business-oriented use cases** which examined the sharing, trading, (re)use of data and services. The work under WP5 reported to the overall TRUSTS objective 4 (Table 4 below).

The work of WP5 was organised in three tasks as illustrated in the Figure x below:

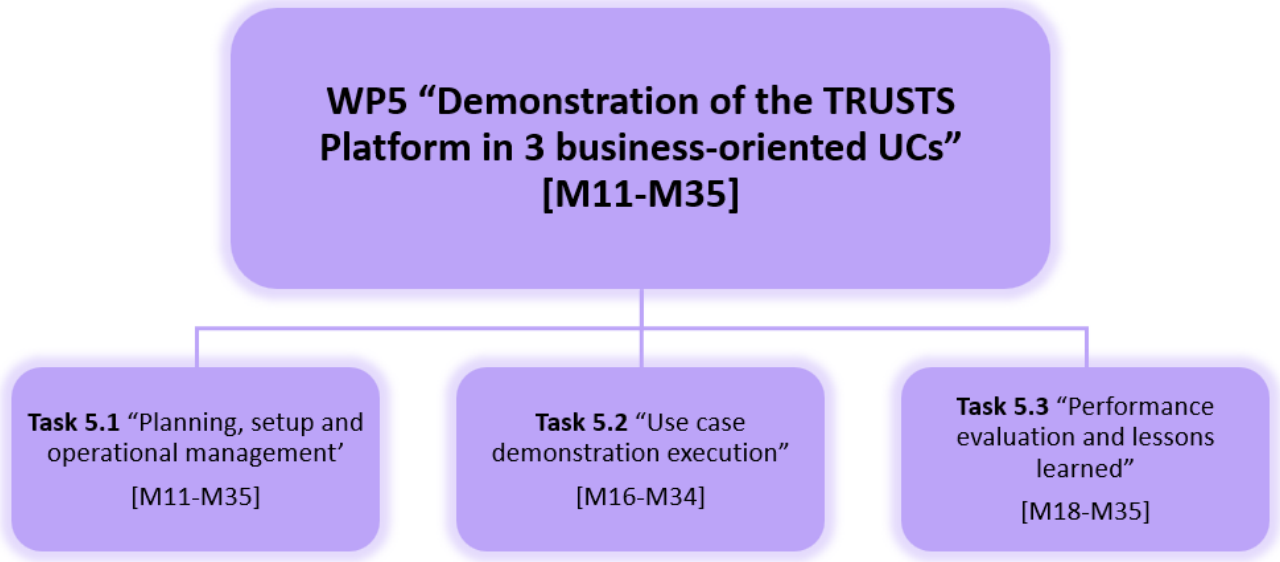


Figure 30: WP5 organisational chart

3.5.1 Objectives

The Table 4 below states the TRUSTS objective 4 that was associated with WP5 and the work performed under this fruitful WP. Achieving this objective required the implementation of the three projects UCs that demonstrated the added value of the TRUSTS platform as determined:

- **UC1 "The Anti-Money Laundering compliance use case"**: Smart big-data sharing and analytics for Anti-Money Laundering (AML).
- **UC2 "The agile marketing through data correlation use case":** Agile marketing activities through correlation of anonymized banking and operators' data.
- **UC3"The data acquisition to improve customer support services use case":** Data processing and visualisation services for Big Financial Data, specifically to advance new ways of human-computer interaction (e.g. chatbots).

Table 4: TRUSTS Objective 4 associated with WP5

TRUSTS Objective 4: **WP5 Demonstration of the TRUSTS Platform in 3 business oriented UCs**
Targeted Effort
To demonstrate the added value of the TRUSTS Platform in 3 business-oriented UCs which showcase the sharing, trading, (re)use of data and services and result in added value generated through innovative applications built on multiple open and proprietary data sources.

WP5 focused on:

1. Defining and setting up the test environment while performing the relevant planning and pilot operational management for trials in the three defined pilots;
2. Conducting advanced field trials within the following sectors of: Financial Institutions, Telecom Operators, Corporate data providers, etc.;
3. Using the test results and data to deliver impact analysis and impact assessment reports to systematically address the pilots' stakeholder perspectives.

3.5.2 Results achieved

During the third year of the TRUSTS project, WP5 focused on setting up the test environment and the relevant planning and operational management for the execution of the second cycle of the TRUSTS demonstration that was set to start by February 2022 until September 2022, while concluding on the lessons learned derived from the platform.

The second version of the operational report (D5.2) under the WP5 was initially produced and submitted (in January 2022) reporting on the overall plan of the second cycle of the TRUSTS trials. Additionally after the conclusion of the second cycle of the TRUSTS trials (November 2022), the third and final version (D5.3) of the report was also submitted concluding on the conclusive plan followed in November 2022.

Three reports were prepared, one for each UC (UC1: D5.5, UC2: D5.7, UC3: D5.9), reporting on the actual field trials executed during the Second Cycle of the TRUSTS trials. These 'demonstrators' laid-out each UC scenario executed for the evaluation of the TRUSTS platform. The three reports were submitted in October 2022, following an internal amendment to allow more time to the development team for final alterations to the platform.

The final performance evaluation and lessons learned report was submitted in November 2022 (D5.11) following the conclusion of the three UCs second cycle execution as well as the overall WP5 effort.

Furthermore, WP5 and an insight of the work done participated in the European Big Data Value Forum (EBDVF) 2022 showcasing the platform usage and benefits as well as lessons learnt gathered throughout the project progression.

Through close internal collaboration between the WP5 participants and the other WPs of the project, the objectives were achieved. In detail:

Task 5.1 Planning, setup and operational management

Task 5.1 was led by EBOS, with the purpose to manage and monitor the WP5 tasks, following and

coordinating the WP activities as well as defining the planning and preparation of the three UCs trials strategy.

TRUSTS cycle 2 trials were:

- TRUSTS_UC1_Trials on MVP v2 duration: 16 February - 6 May 2022
- TRUSTS_UC1_Trials on MVP v3 duration: 16 June- 15 July 2022
- TRUSTS_UC1_Trials on MVP v4 (final product set to be tested) duration: 18 July - 30 September 2022

The second version of the operational report (D5.2) under the WP5 was produced and submitted (in January 2022) reporting on the overall plan of the second cycle of the TRUSTS trials the three UCs followed. Additionally after the conclusion of the second cycle of the TRUSTS trials (November 2022), the third and final version (D5.3) of the report was also submitted concluding on the conclusive plan followed. The **final Business Validation (BV)** was accommodated as per the WP2 and Task 2.3 endeavour. The final BV has been performed from June 2022 – November 2022 (M30 to M35), allowing the evaluation of the complete environment from a performance and business point of view, via the measurement of the UCs KPIs and validation of their results to define the gap towards commercialising the environment.

Task 5.2 Use case demonstration execution

Task 5.2 was led by NOVA, with the purpose to perform actual testing and validation activities in cooperation. The project team collected the results generated and validated the effectiveness of the Platform within the three UCs, highlighted relevant interference observed, gaps in the expected results, difficulties in the adaptation of the solution and other peculiarities of the context that might act as a constraint, so as to continuously improve the Platform.

During the third year of the project, the second cycle of TRUSTS trials were performed, by the three UCs, both individually and in common, evaluating the TRUSTS data marketplace platform:

During the second cycle of TRUSTS trials **UC1** performed twenty-nine (29) trial sessions with the collaboration of fifty-seven (57) participants/stakeholders. The trial sessions concluded with sixty-six (66) questionnaires answered giving several improvement feedback and remarks to the project from a business and a technical perspective (see Table X below). All trial sessions were accompanied with screenshots and are further discussed and illustrated in the UC1 respective Deliverable 5.5 "Actual field trials of Use Case 1" submitted in October 2022.

Table 5: TRUSTS UC1 trial sessions for Cycle 2

UC1 trial sessions	UC1 stakeholders	UC1 participants	UC1 questionnaires
MVP v2			
09-03-2022	2	3	2
15-03-2022	2	3	3
21-03-2022	1	1	1
22-03-2022	3	4	3
30-03-2022	2	2	2

06-04-2022	3	2	3
27-04-2022	2	2	2
27-04-2022	3	3	3
02-05-2022	3	2	3
MVP v3			
28-06-2022	1	1	1
05-07-2022	1	1	1
08-07-2022	2	2	2
13-07-2022	2	2	2
MVP v4			
26-07-2022	2	2	2
27-07-2022	2	2	3
29-07-2022	3	3	3
02-08-2022	2	2	3
03-08-2022	2	2	2
05-08-2022	1	1	1
08-08-2022	2	2	2
12-08-2022	2	2	3
17-08-2022	2	3	3
23-08-2022	2	2	2
23-08-2022	2	3	3
24-08-2022	1	2	2
26-08-2022	2	3	3
30-08-2022	2	3	2
31-08-2022	2	2	2

26-09-2022	1	2	2
Total:	**57**	**64**	**66**

During the second cycle of TRUSTS trials **UC2** performed eighteen (18) trial sessions with the participation of fifty-three (53) stakeholders. The trial sessions ended with the completion of seventy-nine (79) questionnaires containing various suggestions for improvement of the project from a business and technical perspective (see Table 6 below). All trial sessions were screenshotted and are further explained and illustrated in the UC2 Deliverable 5.7 "Actual field trials of Use Case 1" submitted in October 2022.

Table 6: TRUSTS Cycle 2 trials of UC2

UC2 trial sessions	UC2 stakeholders	UC2 participants	UC2 questionnaires
MVP v2			
24-03-2022	4	5	5
31-03-2022	3	4	4
04-04-2022	1	2	2
08-04-2022	4	6	6
11-04-2022	5	7	7
28-04-2022	3	4	4
MVP v3			
19-07-2022	4	7	7
21-07-2022	3	5	5
22-07-2022	3	6	6
MVP v4			
26-07-2022	3	8	8
28-07-2022	3	4	4
29-07-2022	4	7	7
03-08-2022	1	1	1
04-08-2022	4	4	4
05-08-2022	4	4	4

UC2 trial sessions	UC2 stakeholders	UC2 participants	UC2 questionnaires
25-08-2022	4	4	4
29-08-2022	3	5	5
31-08-2022	4	5	5
Total:	**53**	**79**	**79**

During the second cycle of TRUSTS trials **UC3** performed thirteen (13) trial sessions with the participation of twenty-six (26) stakeholders. The trial sessions ended with the completion of thirteen (13) questionnaires containing various suggestions for improvement of the project from a business and technical perspective (see Table 7 below). All trial sessions were screenshotted and are further explained and illustrated in the UC3 Deliverable 5.9 "Actual field trials of Use Case 3" submitted in October 2022.

Table 7: TRUSTS trials cycle 2 of UC3 trial sessions

UC3 trial sessions	UC3 stakeholders	UC3 participants	UC3 questionnaires
MVP v2			
11-04-2022	2	5	1
18-04-2022	2	5	1
29-04-2022	2	5	1
03-05-2022	2	5	1
05-05-2022	2	5	2
MVP v3			
05-06-2022	2	5	0
15-06-2022	2	5	0
09-07-2022	2	5	0
MVP v4			
02-08-2022	2	5	1
10-08-2020	2	5	1

29-08-2022	2	5	1
30-08-2022	2	5	2
31-08-2022	2	5	2
Total	**26**	**65**	**13**

Beyond the trials that each UC performed on its own, all three UCs performed 5 **common trials** to imitate real life transactions testing among other scenarios, scalability, and federation. Multiple corporate nodes were created, and each node uploaded several assets to populate the platform. Enriching the feedback with more responses with questionnaires from more stakeholder's engagement and trials session popularity, supplementary external stakeholders were employed to use the platform in the second demonstration cycle. By these means a more populated platform was validated with a simultaneous access to the TRUSTS platform. This intended to have the evaluation before implementing the final version of the platform. The Table 8: TRUSTS UC common trial sessions for Cycle 2 below shows the common trials executed during the TRUSTS Cycle 2 period.

Table 8: TRUSTS UC common trial sessions for Cycle 2

Common UCs trial sessions	Common UCs stakeholders	Common UCs participants	Common UCs questionnaires
MVP v2			
07-04-2022	6	7	2
14-04-2022	6	8	4
21-04-2022	6	6	2
28-04-2022	6	6	2
MVP v4			
14-10-2022	3	3	3
Total:	**27**	**30**	**13**

A video[7] was produced by all three TRUSTS UCs, as a common trial session reflecting the second demonstration trial cycle status during the final month of the trial's execution, September 2022 in order to capture all available functionalities/developments. The validation principles were to provide the end-to-end platform operation and to reveal the key functionalities and performance achieved. The common lessons

[7] YouTube video link https://www.youtube.com/watch?v=MSXeLpNNiUY

learned were circulated to the development team (WP3) for consideration in regard to the final TRUSTS data-market version, and are additionally included as input to the D5.11 submitted in November 2022.

Lastly, under the scope of task T5.2 and in collaboration with NOVA, LSTech developed an admin-dashboard for the TRUSTS platform, called Business Support Services, which is a basic but essential tool for monitoring the usage of the platform. Through an intuitive dashboard information related to registered organizations, users and data sets is available.

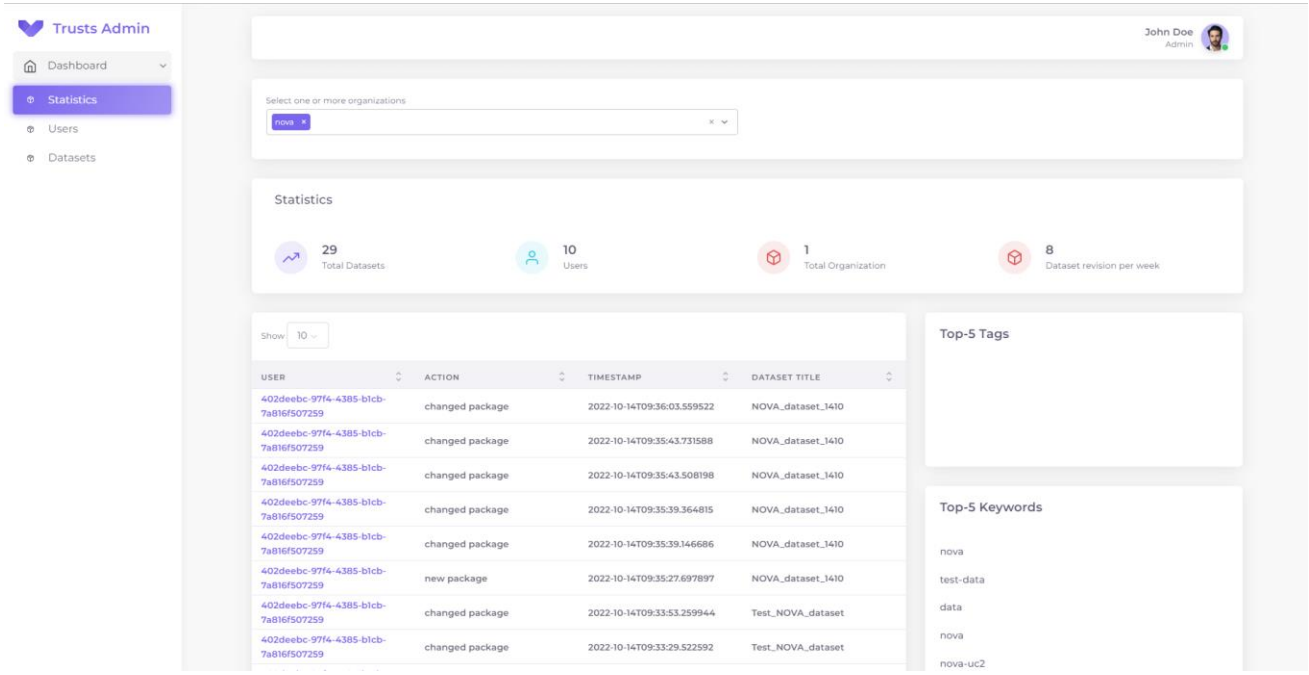


Figure 31: Screenshot of the TRUSTS admin dashboard

Task 5.3 Performance evaluation and lessons learned

Task 5.3 was led by NOVA having as purpose two aspects. First, the performance of each use case particularly from the KPI perspective to illustrate how the TRUSTS platform capabilities could be leveraged for different applications in each use case. Secondly, according to the results received from each use case in every agile-based iteration, the task should provide requirements and suggestions to further improve both functional and non-functional capabilities of TRUSTS. Throughout the validation testing period, knowledge and findings of the third project year were documented in deliverable D5.11 together with evaluation reporting and impact assessment for the use cases, and extracting lessons learned. The lessons learnt are described in detail in the following paragraphs.

UC1 established and validated how data shared via TRUSTS fed into an existing AML solution (two applications) enhanced with big data analytics. Moreover, this enriched data was securely traded via TRUSTS to interested customers who need to perform AML checks, such as financial institutions, internal corporate audit departments, fiduciaries, and corporate service providers but also tax advisors, automotive dealers, estate agents. Faster and more accurate detection of financial crime and money laundering was achieved. Several recommendations for improving the testing of the TRUSTS platform in general were also derived from the stakeholder participation and the completed feedback questionnaire. A conclusion from the tests carried out is that improvements are still needed, and that further developments and test functions are

missing. The project development team will duly consider this conclusion for the final product. TRUSTS platform is being developed to create a fully operational and GDPR-compliant European Data Marketplace for personal and non-personal related data. Towards this goal, a systematic process was followed to collect requirements and FRs from a wide set of sources (electronic surveys, interviews, literature search, regulatory framework, analysis of past deliverables, etc.). The resulting FRs are listed in D2.2 and became the basis for the detailed definition of the UC scenarios and the subsequent Trials. UC1 lessons learnt concluded that the feedback was positive regarding the steps followed and the flow, although the current stage of the TRUSTS marketplace environment development is still non-operational as an integrated platform. This led to being unable to get a complete picture of the platform as a fully operational product. More decentralised and clear processes with a user-friendly UI should be considered for the final product. Overall, the business applications that were demonstrated met with notable success while they were improved compared to the first cycle of the trials. The UC1 applications UI and performance was most liked. Their flow and process were well structured and performed and the UC aim was established. Data sharing and trading platforms such as TRUSTS Platform, represent an opportunity to securely share and trade data for AML purposes and thus to maximise operational effectiveness whilst maintaining or reducing costs. The lack of a consolidated and widely viable data marketplace, secure and GDPR compliant adequate to benefit various business collaborations in the framework of AML services enhanced with AI, is a necessity to the data market. Such marketplace collaboration could be a benefit for the whole economy since innovative procedures and productions with added value will be inaugurated into the market. Financial institutions, corporate audit departments, tax advisors and many more, need to regularly perform AML checks.

UC2 demonstrated capabilities of the TRUSTS Platform as a "Trusted Secure Data Sharing Space" for advanced marketing activities through correlating anonymized banking and telecommunications data. The feedback for improving was derived from the stakeholder participation and the completed feedback questionnaire. UC2 tested TRUSTS data marketplace platform data assets' exchange mechanism in terms of security, reliability, consistency, and the speed of upload/download. The general outcome was that the operation was performed successfully and quite smoothly. Innovations like the smart contracts and the recommendation mechanism were integrated into TRUSTS platform, providing the TRUSTS platform users with extra functionality. Regarding its scalability, TRUSTS platform seemed to be scalable at least to a certain level (Consortiums with several organisations exchanging data assets). Another aspect that was tested, is TRUSTS platform ability to interoperate with external open-data libraries and external federated marketplaces which was a functional operation, but still needs to be improved in terms of being automated. Finally, the business applications that were developed within the context of UC2 were also liked, as those applications added value to the TRUSTS platform, providing functionality that for instance was essential for the preservation of security (Deanonymization/Anonymization application). Regarding possible suggestions for improvement, platform stability and reliability needs to be improved to achieve better response time and eliminate some down-time issues that were faced during the tests. Another aspect of the platform that needs further assessment is the platform's security and GDPR compliance. TRUSTS aims to become a federated and trusted data marketplace; thus, it should be ensured that there are no security gaps within the platform. The last two points of recommendation for improvements are referring to the UI and the usability, in terms of making the platform as simple-user friendly as possible in terms of diminishing the need of technical background for the platform users. UC2 "lessons learned" concluded that in general the feedback was positive regarding the steps followed and the flow, although improvements are still needed, and that further developments should be carried out. The project development team should consider this conclusion for the final product. The aim of UC2 was to establish and validate how big data analytics techniques applied on data shared in a secure and effective manner can provide timely and meaningful information towards targeting profitable customers at a local level. TRUSTS provided UC2 stakeholders with exactly that; a

sustainable and GDPR compliant manner to be able to demonstrate and validate sharing anonymized up-to-date data in target marketing actions to specific local areas or even individuals.

UC3 was able to test and demonstrate the capabilities of the TRUSTS platform and provide information and feedback based on the trials performed. UC3 tested "The data acquisition to improve customer support services" with the general outcome being that the result achieved meets the expectations of the project. Participants with a technical background, appear to focus more on the technical aspects of the platform (e.g., underlying technologies used to implement a feature), whilst those with a business background focused on more quality-of-life aspects of the platform (e.g. how easy it was to navigate the user interface).During all trials it proved necessary that the participants were guided by the technical observers, because otherwise they could become confused and uncertain as to what they needed to do in order to complete the trial sessions. Regarding possible suggestions for improvement, platform reliability and stability along with possible performance improvement where the ones noted during the trials. Regardless, further assessment at platforms security and GDPR compliance is needed. UC3 lessons learned concluded to positive feedback regarding the steps followed and the flow, despite all the issues, ultimately the platform managed to deliver the services required for the successful completion of the UC3 trials, albeit a bit rough around the edges.

Finally, the **second Technical Validation (TV)** has been performed between January 2022 (M25) to September 2022 (M33), allowing the validation of the Marketplace and the provided services during the second set of the UC trials by utilising the defined test procedures and the reporting structure, and validation of results regarding technology. This validation has been aligned with the milestone's timeline since it is initiated right after Milestone 4 "End of second period" (M24) and performed by the UC participants during the second set of the UCs trial period, allowing them to check and validate the outcome of the technical implementation through predefined scenarios and document the results using the above templates. This last round of technical validation has also evaluated the complete environment from a technical, performance, expandability (e.g., federation etc.) point of view and defined the quality of the implementation. The respective documents for the second Technological Validation (TV) are reported in deliverable D5.11 "Platform evaluation and lessons learned II" of WP5, which was delivered in November 2022 (M35).

3.5.3 Future Outlook

The tasks of the WP5 were completed. The conclusions and recommendations will be monitored and potentially adapted in light of the review conducted by the EC in February 2023.

3.6 WP6 Legal & Ethical Framework

3.6.1 Objectives

The overall objective of WP6 is to provide an analysis of the relevant legal acts and develop a robust legal and ethical framework for the TRUSTS Platform to ensure sustainability and compliance of the innovation brought by the project with all relevant regulations and ethics principles. The main objectives of WP6 are to:

- provide a set of requirements in order for the project to be carried out in compliance with the principles of research ethics;

- analyse the European laws and regulations relevant to data transactions and the TRUSTS Platform development;
- define a set of legal and ethical requirements and identify potential legal and ethical obstacles; and
- generate recommendations for policy makers and stakeholders in the field based on best practices and potential identified gaps.

3.6.2 Results achieved

In WP6 so far KUL provided an overview of legal frameworks in order for the project to be carried out in compliance with the principles of research ethics; analysed the European laws and regulations relevant to data transactions and the TRUSTS Platform development; defined a set of legal and ethical requirements and identified potential legal and ethical obstacles; carried out the legal and ethical assessment of the TRUSTS project and activities; and generated recommendations for policy makers and stakeholders in the field based on best practices.

In the framework of our research we have submitted four deliverables. Our D6.1 on research ethics provided all information regarding the compliance of the project research activities with research ethics and, in particular, with the H2020 Programme Ethics Guidance. D6.2 on Legal and Ethical requirements studied the legal frameworks applying to data transactions and elicited legal and ethical requirements stemming from these frameworks. KUL performed research on thinking of data as a commodity that could be turned into a tradable asset. In addition, the analysis was performed on data market ecosystems as those based on the concept called the 'commodification' of data. D6.3 on Legal and Ethical Assessment took stock of the legal and ethical requirements developed in D6.2 and disseminated thereafter, and evaluated the extent to which the TRUSTS platform, both in its project activities and its architecture envisaged for real-life use, is ready to accommodate them; KUL then focused on the most problematic/uncertain aspects of applying the current legal frameworks and provided a legal analysis of current challenges and possible developments. D6.4 on Legal and Policy Recommendations connected the dots from the analysis in D6.3 and transformed it into actionable recommendations for policy-makers on the current (and evolving) legal frameworks, and for stakeholders.

In Task 6.1 KUL provided all information regarding the compliance of the project research activities with research ethics and, in particular, with the H2020 Programme Ethics Guidance. D6.1 was submitted on 28 February 2021 (M14). In the framework of this task, KUL analysed the research ethics principles in order to address the legal and ethical issues arising from the research activities that will be conducted in the course of the TRUSTS project. The development, testing and validation must comply with ethical principles to respect the individuals involved and to prevent harm.

In Task 6.2, backed by an understanding of the technical ambitions for TRUSTS provided by the other Consortium Partners, KUL identified the relevant EU legal frameworks applicable to various data transactions that are envisaged in TRUSTS. More specifically, it provided insight into the privacy and data protection legal framework supporting the data sharing in compliance with the EU rules. It informed partners on the main concepts of the ePrivacy legal frameworks and their relationship with the GDPR. Furthermore, this deliverable was a continuation of the work done in WP9 with regard to anonymisation of personal data. The present deliverable provided further conceptual legal information on privacy preserving techniques and some of techniques that might be relevant for TRUSTS partners. KUL analysed legislation applicable to platforms and data sharing intermediaries ('Platform-to-Business' (P2B) Regulation); EU and national legislation applicable to unfair commercial practices; best practices in the drafting of data usage agreements;

regulatory frameworks governing data processing in the field of financial transactions and Anti-Money Laundering (AML); the legal rules governing the use of blockchain and smart contracts; and ethical principles governing the use of AI within the TRUSTS platform.

In Task 6.3 KUL assessed the TRUSTS platform from a legal and ethical perspective. By constantly engaging with the other Consortium Partners - in particular the technical partners LUH, FhG, KNOW, eBOS and NOVA - KUL assessed to what extent and with which methodology the requirements identified in Task 6.2 have been implemented in the TRUSTS platform. The assessment is not confined to the compliance of the TRUSTS platform with the legal and ethical requirements: it also acknowledges, as was clear from the guidance provided to the Consortium Partners responsible for the platform and use case implementation, that the observance of these requirements is not always straightforward, and that the applicable legal framework is prone to favouring more than one approach. In this vein, the present deliverable delves into the legal and ethical debate surrounding compliance with the (mostly evolving) legal framework applicable to several features and operations of the TRUSTS platform. In Task 6.3 KUL first analysed the core technology and architecture of the TRUSTS platform - based on Federated Learning and anonymisation services. The assessment focused on the ability of these two components, and of their interaction, to minimise the data protection and privacy risks while enabling cooperation on data sets – including personal data – between several organisations with the support of data analytics and artificial intelligence (AI) techniques. While the main applicable legal framework in the above assessment is the EU data protection framework, the deliverable has also analysed the impact and implications of specific legal frameworks to the TRUSTS platform and assessed how the platform is equipped to comply with them. This assessment has focused on both existing laws and ethical principles – i.e., EU legal instruments governing digital markets and digital services, as well as the EU competition law and consumer protection framework – and on proposed legislation – i.e., the Data Governance Act (DGA) and the AI Act. Particular attention was paid – as per the objectives of Task 6.3 – to the competition law implications of business agreements between organisations participating in the TRUSTS platform operations, and to the consumer protection implications of market practices based by AI-enabled recommendations given by TRUSTS services.

KUL then carried out the legal and ethical assessment of the three TRUSTS use cases (UCs), both with reference to the pilot use cases deployed during the project; and to the real-life scenarios envisaged to be deployed upon project completion. In so doing, KUL analysed the legal challenges and issues arising out of the delivery of the UCs in close connection with the legal frameworks and requirements researched in Task 6.2. KUL focused in particular on AML law and data protection law (UC1); and competition law, consumer protection law and ethics of the use of AI (UC2 and UC3).

In Task 6.4 KUL took stock of all the open points and issues stemming from the research carried out previously and from the legal and ethical assessment. It further elaborated on these open points and issues, which may have stemmed from legal uncertainty and/or an evolving legal framework (in particular with the proposals for the Data Governance Act; Digital Services Act; Data Act; and AI Act), and turned them into actionable recommendations. Two types of recommendations were provided: first, recommendations to policy-makers (essentially, the European Commission) with regard to strategies for improving the degree of legal certainty and foreseeability of the legislation; second, recommendations to stakeholders and interested parties in the data marketplace environment on how to navigate the current legal and ethical landscape and how to prepare for the upcoming developments. TRUSTS Consortium Partners were brought onboard and consulted during the elaboration of both types of recommendations.

3.6.3 Future Outlook

The tasks of the TRUSTS projects assigned to KUL were completed. The conclusions and recommendations will be monitored and potentially adapted in light of the review conducted by the European Commission in February 2023.

3.7 WP7 Business Model, Exploitation & Innovation Impact Assurance

3.7.1 Objectives

The objectives of the WP7 "Business Model, Exploitation & Impact Assurance" were to develop a feasible business model to sustain the results of the project, to put measures in place to mobilise an ecosystem upon readiness of the technical platform, and to conduct concrete actions for enabling future commercialization of the data market platform.

Thus, the WP set out to conduct research on what business models for data markets exist to identify business model patterns. The main focus is on business models combining scientific and non-scientific founders since TRUSTS has the same mixed private and public ownership structure.

The main deliverables during the project were on conceptualising a future TRUSTS ecosystem and its needs regarding the innovation aspects and intellectual property and data management. The WP established what the pre-conditions for successful business models and best practices would be.

To achieve the same, the WP was divided into the following tasks:

T7.1 Sustainable business models
T7.2 Developing and structuring the platform engagement
T7.3 Intellectual Property and Data Stewardship
T7.4 Standardisation uptake and recommendations
T7.5 Commercialization initiatives and action plan
T7.6 Innovation Impact Assurance

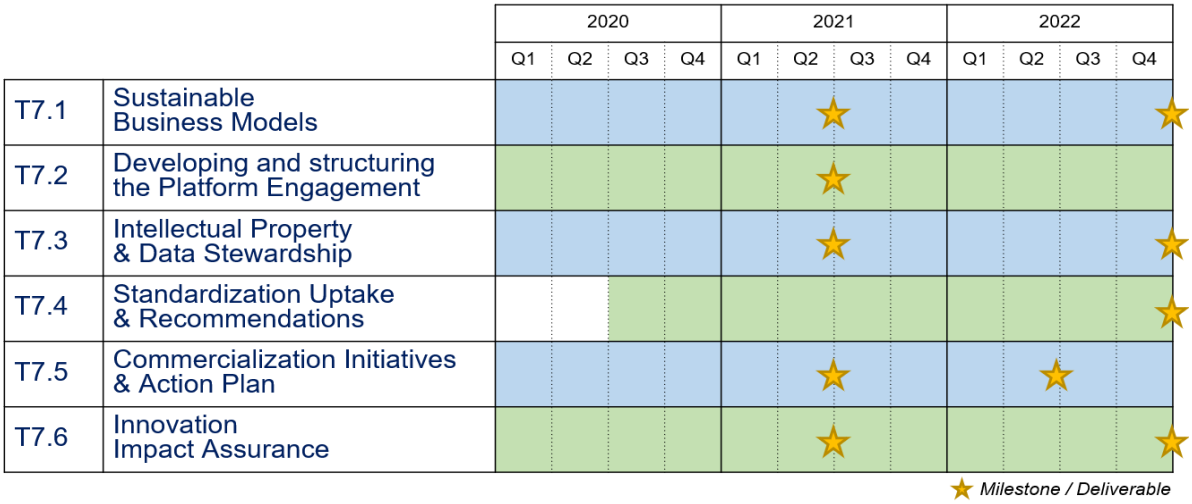


Figure 32: Milestones & Deliverables of WP7

All work tasks were fully activated and delivered against the formal deliverable structure as per the DoA and the above table. Accordingly, at the end of year 3 of the project, interim reports created mid of project were updated and expanded, and - building on high profile, technical workshops with external stakeholders, Task T7.4 formed recommendations for standardisation that will see further development and adoption, beyond TRUSTS.

3.7.2 Results achieved

Overview

The work in WP7 (Sustainable Business Models, Exploitation, and Innovation Impact Assurance) has been reported in the final set of reports created in 2023, namely D7.2, D7.5, D7.6, D7.8 and D7.10. Research in data markets and data market federation (T7.1) yielded a business-model centric, unified taxonomy which was used as the basis for evaluating viable business model options. This is aligned and builds on the wider market study conducted earlier in T2.1. The select business model for "*TRUSTS as a data market*" got developed and evaluated based on internal workshops as well as interviews. It was detailed through a base business model, which contains the minimum components needed for a viable exploitation. An add-on business model is created with additional value-adding offerings. The business model "*TRUSTS as a federator of data marketplaces*" elaborates how TRUST can take on additional activities to evolve into a federator of an ecosystem of data marketplaces. The related approach to exploitation and commercialization (T7.5) got detailed further, based on aforementioned business model selection and primary research into product-market-fit, utilising the stakeholder engagement strategy and plan (as per mid of project D7.3). To inform auxiliary services of a future data market operator, and to ease data preparation particularly for onboarding of data sellers, mechanisms for DS and IPR protection were elaborated (T7.6). Our "Report on standardisation activities" (D7.6) of T7.4 highlights TRUSTS's recommendations discussed in high profile workshops co-organized with the World Wide Web Consortium (W3C) and during the European Big Data Value Forum 2023 (EBDVF2023). Lastly, WP7 continued to complement the administrative project management approach of WP1, in a series of targeted interventions to help alignment and focus across all project work packages, as part of innovation impact assurance (T7.6).

That said, absence of a full-fledged (operational) MvP of the TRUSTS data market (including transaction processing capabilities) precluded WP7 from complementing its conceptual work with aspired experimentation for insights arising from the study of early adopters of a future TRUSTS data market. Hence, it will be left to a post-project Data Market Operator (DMO) to fine-tune the initial real-world instantiation of the TRUSTS data market. On the one hand this carries the advantage of inherently higher flexibility post-project in shaping the commercialization pathway as per such DMO's mission and focus, e.g. implementing and supporting a pure-play industry focus such as Financial Services or Telecommunications, and thereby also will allow for a wider array of potentially suitable DMOs. On the other hand, feedback arising from such a "beta" phase would have uniquely complemented the original requirement elicitation gathered predominantly in relation to the three project use cases, by T2.4. Also such beta-phase insights from entities with vested commercial commitment and exposure would have added additional, "real world" insights to the commercialization plan.

T7.1 Sustainable business models

T7.1 was successfully concluded by producing D7.2. The deliverable D7.2 provides and evaluates business model options for the TRUSTS platform. The basis for the deliverable was the earlier deliverable D7.1, which provided taxonomies of business models for data marketplaces, based on existing cases. In D7.2, designs are

made for new business models, tailored to the setting of TRUSTS. Tools were used such as the business model canvas and stress-testing method. Workshops and interviews with stakeholders within and external to the project were utilised to develop ideas and evaluate these. Quantitative studies via surveys were done with prospective users to evaluate part of the offerings of the business models.

For the business models designed and evaluated in D7.2, two main scenarios were considered:

TRUSTS as a data marketplace: The assumption for this scenario is that the data marketplace operates in the current landscape of the data economy. This is further detailed through a base business model, which contains the minimum components needed for a viable exploitation. An add-on business model is created with additional value-adding offerings. The business models were developed and evaluated based on internal workshops as well as interviews. They also incorporate and build on findings of the preceding Data Market Austria (DMA) project. Close cooperation with the other work packages and use case leaders helped to assure that the business model is in line with the actual work developed in TRUSTS.

TRUSTS as a federator of data marketplaces. The assumption for this scenario is that TRUSTS takes on additional activities or evolves into a federator of an ecosystem of data marketplaces. Federation could help resolve the fragmentation of today's data economy, without interfering in health competition between existing data marketplaces. As federation is complex to achieve, a federation business model likely becomes possible only in the longer term. The value propositions of such a federator platform involve an (advanced) search engine, comparison site, and one-stop shop. Since a federator platform does not exist yet in the data economy domain, inspiration was drawn from aggregator business models in other industries.

Figure 33 shows the positioning of TRUSTS with current offerings, which fits with the comparison archetype. This is because TRUSTS has had the vision to create a federated data marketplace based on International Data Space (IDS) and Data Market Austria (DMA) since the beginning of the project. TRUSTS developed APIs to enable interoperability between data marketplaces. Moreover, TRUSTS provides offerings beyond mere data discovery (e.g., data protection). In the long run, TRUSTS could evolve to match the "one-stop-shop" archetype to achieve the full vision of the federation by exercising advanced offerings such as compliance checking support, certification, or data asset pricing benchmarks.

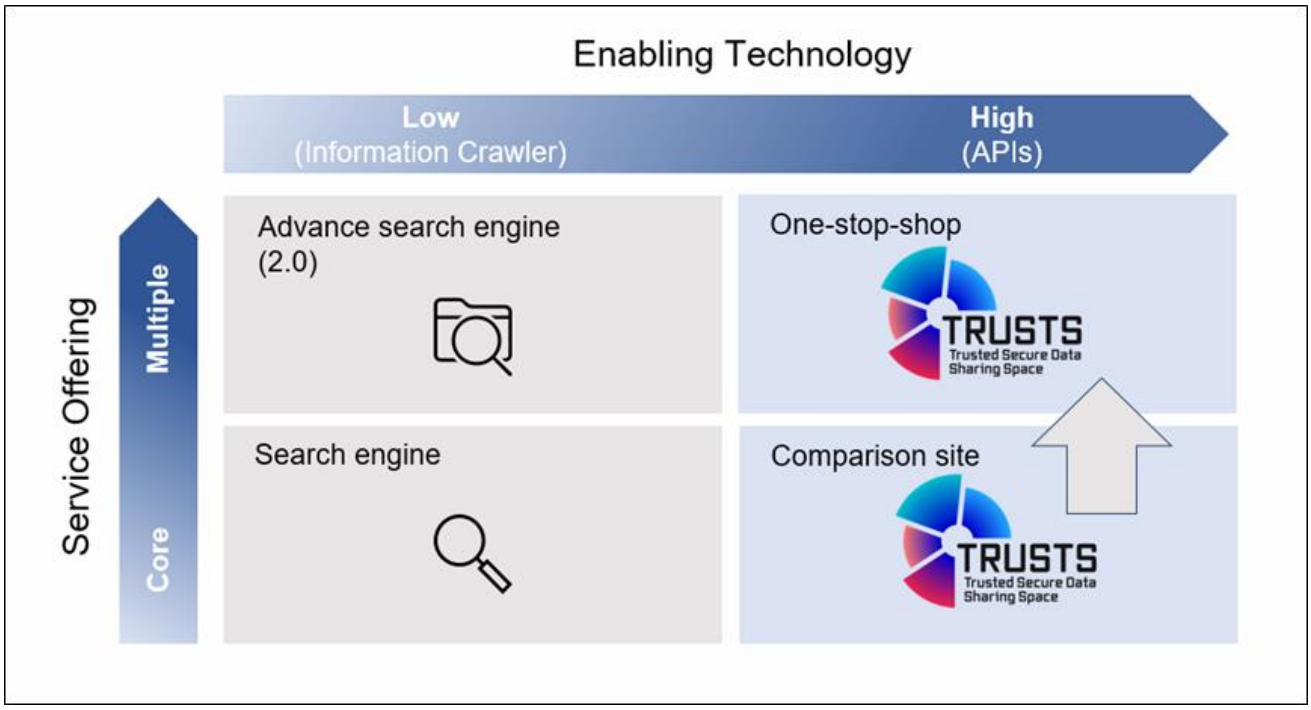


Figure 33: TRUSTS business model dynamics as a federated data marketplace

Potential offerings were evaluated in empirical work, involving a large-scale survey among a representative sample of businesses. This work shows that the offerings of the federator business model positively contribute to trust, risk perceptions and willingness to share data (Figure 33).

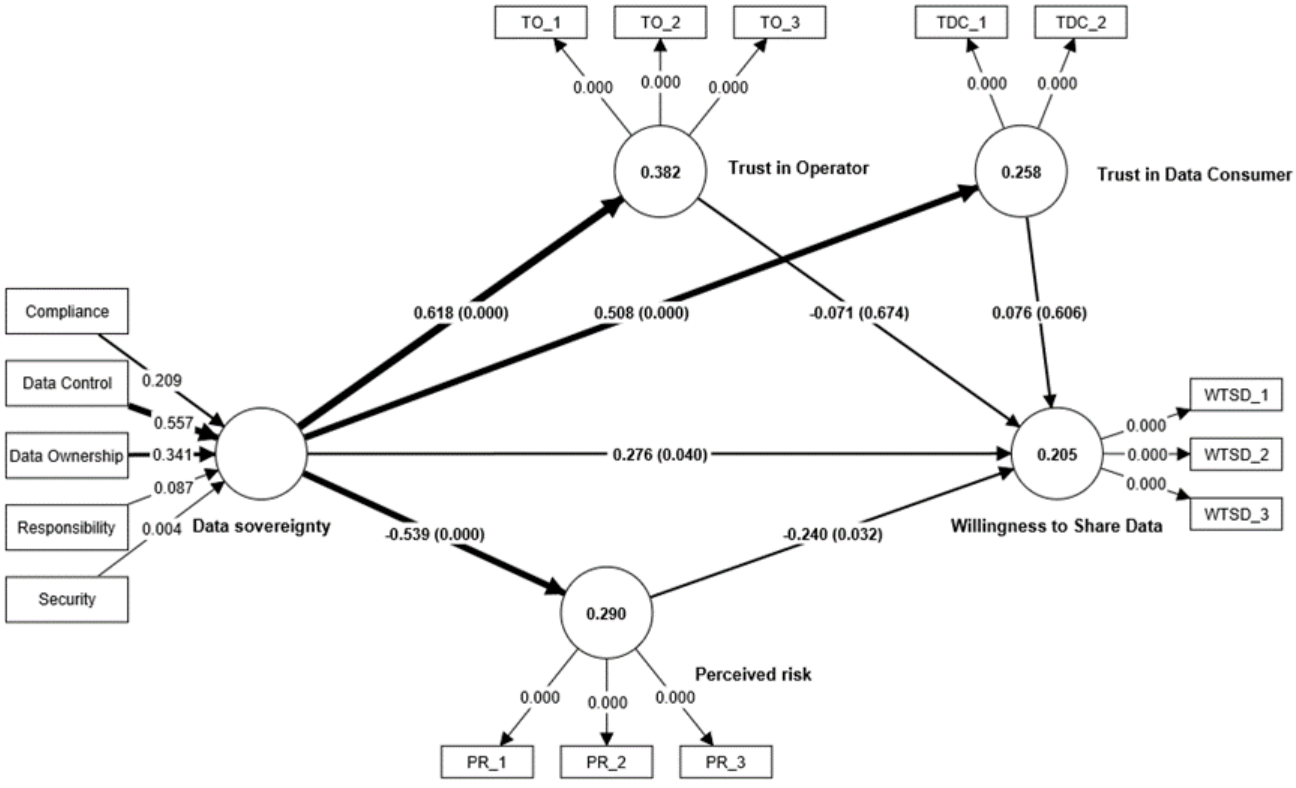


Figure 34: The homological net model (the number in arrow shows path coefficients and p value; the number in the variable refers to R-square)

Risks and actionable recommendations have been derived. These recommendations involve the pricing model, subsidisation to kick-start the platform, offerings, promotion and key technologies to focus on. The work informs a future operator of the TRUSTS platform on different business model options to consider, scenarios to choose from and practical recommendations to realise the business model. To sum up, the TRUSTS functionalities and developments demonstrate how the project has significantly contributed to the federation's long-term vision (which never existed before).

T7.2 Developing and structuring the platform engagement

During this period IDSA has continued supporting the Stakeholders Engagement Plan implementation; this plan identifies how the consortium members will engage stakeholders from the different categories and subcategories in outreach activities, e.g. workshops, trainings, webinars, so stakeholders can strengthen one another and join understanding, and approach is created. As part of this engagement activities IDSA has identified and communicated the engagement activities to the IDSA community and specially to key stakeholders.

T7.3 Intellectual Property and Data Stewardship

Task 7.3 in WP7 was successfully concluded. In deliverable D58 (7.10) the intellectual property rights (IPR) aspects of data exchange portals, specifically focusing on the organisational and operational aspects of IPR protection for the TRUSTS operator and the internal IPR of the software used in the TRUSTS platform by the consortium partners were investigated. The economic mechanisms for cost and revenue sharing within TRUSTS consortia were examined, as well as legal tools for the protection of data exchanged via the TRUST platform.

The task also delved into concepts for data governance and data stewardship for users of the TRUSTS platform, which includes establishing control over data ownership, access, and usage decisions in order to minimise the risks associated with data sharing. Additionally, it highlighted the benefits of open datasets for companies and the different types of open datasets available, such as open government data, open research data, and data openly shared by other companies.

The task also developed a process of threat modelling, which is a method for identifying, analysing, and assessing potential threats to an organisation or system. The TRUSTS threat modelling process was defined as an iterative loop, starting from an early phase of the design of an application or data model, continuing throughout its whole life cycle. The importance of supporting data sharing and commercialization while taking into account the needs and requirements of various stakeholders, including data providers and users, prioritising security, reliability, scalability, flexibility, and simplicity was emphasised.

Furthermore, T7.3 proposed the establishment of a TRUST-DAO (Decentralised Autonomous Organization) model for managing services, software licences, and cost sharing within the TRUSTS operating company (OpCo) using dataNFT-based services and licence cost sharing system within a TRUSTS-DAO framework. It was explained that implementing dataNFT in a TRUSTS-DAO model can provide a secure and transparent way to protect members' intellectual property rights (IPR) and manage the usage and ownership of software licences and software components in the TRUSTS platform.

WP	Functional Context	Name of TRUSTS module / set of software components	Description
WP3	Smart contracts (T3.2)	Smart contract executor	Tool providing and executes smart contracts
WP3	Semantic layer (T3.4)	Vocabulary Management System	A UI where users can manage vocabularies that are to be use throughout the project
WP3	Semantic layer (T3.4)	Metadata Broker	Central metadata repository of the platform. Is compliant to the IDS communication protocol
WP3	Semantic layer (T3.4)	Metadata Storage System	The triplestore (database) where the metadata is actually stored in RDF format.
WP3	Semantic layer (T3.4)	Platform Interface	The base component of the user interface that each node in the platform will have, allows for onboarding searching and consuming assets.
WP3	Semantic layer (T3.4)	IDS Extension for CKAN	An extension that is required to make the CKAN platform interact with IDS components.
WP3	Semantic layer (T3.4)	Vocabulary Extension for CKAN	An extension that is required to have the CKAN platform software to use the vocabularies in asset onboarding
WP3	Semantic layer (T3.4)	TRUSTS Client	
WP3	Brokerage (T3.6)	Recommender system	Providing services to recommend connections between datasets, services and users
WP3	Transfer learning methodology		
WP4	De-anonymisation / anonymisation toolkit (T4.3)		
WP4	Metadata schema for data assets		
WP4	Protocol for metadata exchange		
WP4	Protocol for Private Set Intersection	PSI library PSIttacus	Java library that enables two parties to find identical data in their data sets without sharing the full sets with each other

Table 11 chapter 6.3.4 from D58 (D7.10): Functional context of software components used in TRUSTS

In T7.3, the importance and necessity of creating specialised contracts for TRUSTS OpCo to protect the intellectual property rights (IPR) of users on the TRUSTS platform were discussed. It was found that data, which is not typically protected by patent or copyright laws, can be owned but enforcing legal claims for it can be difficult if it is taken without permission. There is a need for contracts that regulate the use of the TRUSTS platform and provide legal certainty. Two draft contracts were presented: a "Code of Conduct for using the TRUSTS Platform" (CC) and "Terms and Conditions for using TRUSTS Services" (TC). The CC serves as general guidelines for user behaviour on the platform and does not contain any enforceable provisions. The TC, on the other hand, governs the conditions under which transactions between users take place, defining the rights and obligations of data providers and data consumers, as well as the legal position of the TRUSTS OpCo. It is acknowledged that the drafts presented will require revision and enhancement as the TRUSTS OpCo is established.

The draft "Code of Conduct for using the TRUSTS Platform" (CC) serves as a framework for amicable cooperation on the TRUSTS data trading platform. The code aims to establish and promote efficient and targeted data exchange within the framework of the trading platform, with the goal of improving and optimising the use of data, and achieving positive outcomes for employment and growth, as well as sustainable social stability and prosperity. The code sets out general principles and rules of conduct for participants, including compliance with legal provisions, particularly the General Data Protection Regulation (GDPR) and transparency regarding the origin and traceability of data collection. Participants are expected to act in accordance with principles of integrity, fairness, and partnership, and to communicate with each other in a respectful manner. The code also recognizes that data is sensitive and emphasises the importance of preserving informational self-determination and protecting privacy. The code is intended to be a living document and will be supplemented and expanded in the future to include sanctions and penalties if relevant findings are obtained through the operation of TRUSTS.

During the project, a draft of the "Terms and Conditions for using TRUSTS Services" (TC) was developed as a proposal for what the terms and conditions could look like when the TRUSTS OpCo is operational. The draft TC is intended to provide a legal framework for the platform, but it is acknowledged that certain decisions regarding the organisation and structure of the platform may need to be changed or adapted at a later stage. The draft TC is formulated in such a way that it can apply to different legal forms of the operating company. The TC defines key terms such as "TRUSTS Platform," "Data," "Transaction objects," and "Participant." It also explains the process of "Listing," which is a requirement for all participants to go through before they can offer or request data on the platform. The TC also outlines the different functional roles on the platform, including Data Provider, Data Demander, and Operator. It states that the TC governs the rights and obligations of all participants in relation to TRUSTS OpCo.

T7.4 Standardisation uptake and recommendations

The overall objective of task T7.4 is lower hurdles for data sharing (and therefore data markets and TRUSTS) by supporting the development of standards. The main objectives for this task are: (1) elaboration, assessment, and identification of requirements of a variety of concepts and standards (2) provision of recommendations to key standardisation bodies and (3) share and present recommendations to standardisation bodies' representatives during two dedicated workshops.

The standardisation activities have been developed in two phases, phase 1. Scanning and phase 2. Processing and Presenting

During this year IDSA, SWC and G1 have developed the phase 2 Processing and Presenting: consisting of the following activities: prioritisation of standards and definition of current requirements for standards. Preparation of workshops with Standardisation Bodies. And finally, preparation and finalisation of the standardisation report (D7.6). More details of these activities can be found in D7.6 "Report on standardisation activities".

In this reporting period, we TRUSTS project has organised two standardisation workshops, namely:

a) **Workshop on Data Spaces and Semantic Interoperability**, organised by TRUSTS as a full-day workshop on 3rd of June 2022 in Vienna at the University of Economics Vienna, co-organised by the World Wide Web Consortium (W3C) and the International Data Space Association (IDSA), and

b) **Workshop: Towards Data Spaces Interoperability Workshop on standardisation co-organized by BD4NRG, TRUSTS and IDSA**, taking place on 23rd of November 2023 as a one hour session in the course of the European Big Data Value Forum 2023 (EBDVF2023).

The First workshop "**Workshop on Data Spaces and Semantic Interoperability** " aimed to identify and specify gaps regarding interoperability in data spaces.

The chair of the workshop Sebastian Steinbuss[8] (CTO of International Data Space Association[9]) moderated a panel with: Sabrina Kirrane[10] (University of Economics Vienna), Pierre-Antoine Champin[11] (W3C), and Christoph Lange-Bever[12] (Fraunhofer Germany) about interoperability and related standardisation efforts and the topic of data usage control.

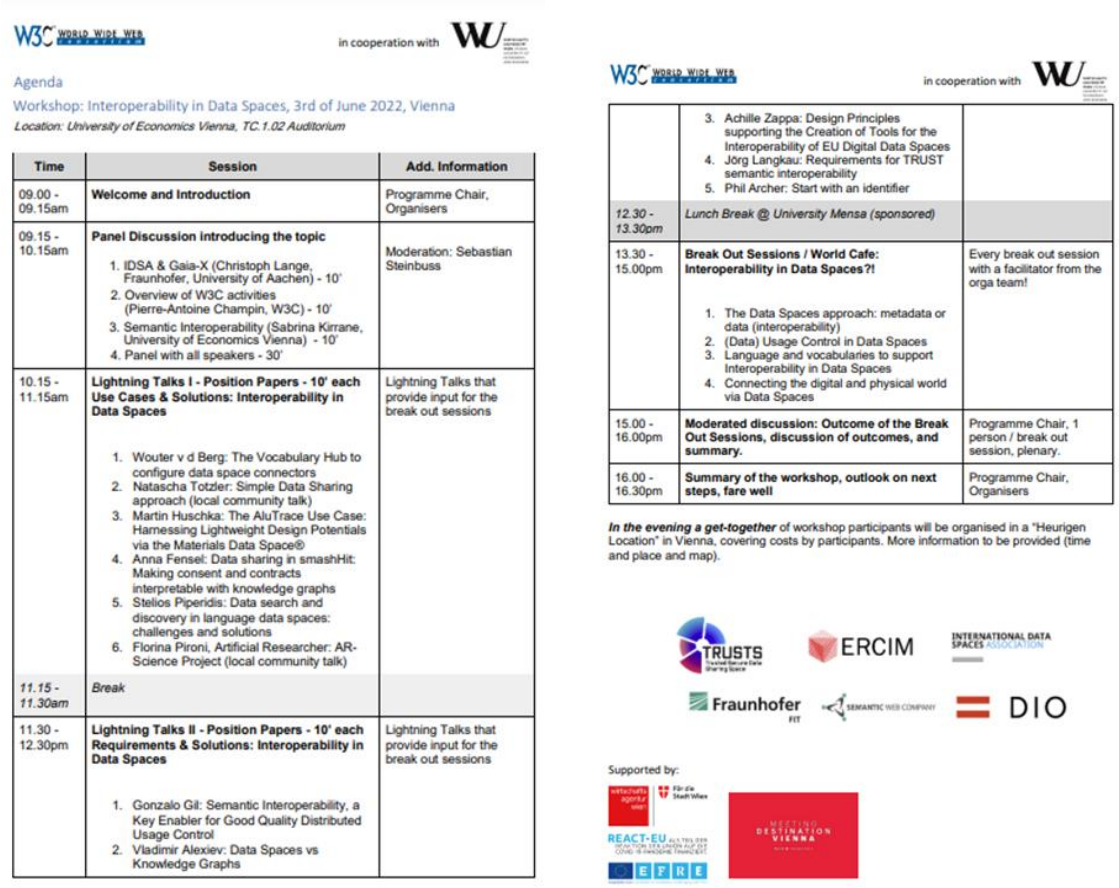
This introduction into the event's topic was followed by 10 lightning talks – for details of speakers and topics see the workshop agenda[13] – that were selected by the workshops' Programme Committee from the submitted position papers. After the lunch break the interactive part of the event started with 4 moderated break-out sessions discussing the following topics:

- The Data Spaces approach: metadata or data (interoperability)
- (Data) Usage Control in Data Spaces
- Language and vocabularies to support Interoperability in Data Spaces
- Connecting the digital and physical world via Data Spaces

In the next page the agenda for the workshop and some pictures are illustrated.

On the Trusts website, there are available papers, as well as recordings and slides of the presentations[14].

[8] LinkedIn profile page: https://www.linkedin.com/in/sebastiansteinbuss/?originalSubdomain=de
[9] Company website: https://internationaldataspaces.org/
[10] LinkedIn profile page: https://bach.wu-wien.ac.at/d/research/ma/13928/
[11] LinkedIn profile page: https://www.linkedin.com/in/pierreantoinechampin/?originalSubdomain=fr
[12] LinkedIn profile page: https://www.linkedin.com/in/langechristoph/?originalSubdomain=de
[13] https://www.trusts-data.eu/wp-content/uploads/2022/05/Workshop_Interoperability_3rdJune2022_Agenda_Status20220527-1.pdf
[14] https://www.trusts-data.eu/data-spaces-semantic-interoperability/workshop-report-pictures-slides/



in cooperation with

Agenda

Workshop: Interoperability in Data Spaces, 3rd of June 2022, Vienna

Location: University of Economics Vienna, TC.1.02 Auditorium

Time	Session	Add. Information
09.00 - 09.15am	**Welcome and Introduction**	Programme Chair, Organisers
09.15 - 10.15am	**Panel Discussion introducing the topic** 1. IDSA & Gaia-X (Christoph Lange, Fraunhofer, University of Aachen) - 10' 2. Overview of W3C activities (Pierre-Antoine Champin, W3C) - 10' 3. Semantic Interoperability (Sabrina Kirrane, University of Economics Vienna) - 10' 4. Panel with all speakers - 30'	Moderation: Sebastian Steinbuss
10.15 - 11.15am	**Lightning Talks I - Position Papers - 10' each Use Cases & Solutions: Interoperability in Data Spaces** 1. Wouter v d Berg: The Vocabulary Hub to configure data space connectors 2. Natascha Totzler: Simple Data Sharing approach (local community talk) 3. Martin Huschka: The AluTrace Use Case: Harnessing Lightweight Design Potentials via the Materials Data Space® 4. Anna Fensel: Data sharing in smashHit: Making consent and contracts interpretable with knowledge graphs 5. Stelios Piperidis: Data search and discovery in language data spaces: challenges and solutions 6. Florina Pironi, Artificial Researcher: AR-Science Project (local community talk)	Lightning Talks that provide input for the break out sessions
11.15 - 11.30am	*Break*	
11.30 - 12.30pm	**Lightning Talks II - Position Papers - 10' each Requirements & Solutions: Interoperability in Data Spaces** 1. Gonzalo Gil: Semantic Interoperability, a Key Enabler for Good Quality Distributed Usage Control 2. Vladimir Alexiev: Data Spaces vs Knowledge Graphs	Lightning Talks that provide input for the break out sessions

in cooperation with

	3. Achille Zappa: Design Principles supporting the Creation of Tools for the Interoperability of EU Digital Data Spaces 4. Jörg Langkau: Requirements for TRUST semantic interoperability 5. Phil Archer: Start with an identifier	
12.30 - 13.30pm	*Lunch Break @ University Mensa (sponsored)*	
13.30 - 15.00pm	**Break Out Sessions / World Cafe: Interoperability in Data Spaces?!** 1. The Data Spaces approach: metadata or data (interoperability) 2. (Data) Usage Control in Data Spaces 3. Language and vocabularies to support Interoperability in Data Spaces 4. Connecting the digital and physical world via Data Spaces	Every break out session with a facilitator from the orga team!
15.00 - 16.00pm	**Moderated discussion: Outcome of the Break Out Sessions, discussion of outcomes, and summary.**	Programme Chair, 1 person / break out session, plenary.
16.00 - 16.30pm	**Summary of the workshop, outlook on next steps, fare well**	Programme Chair, Organisers

In the evening a get-together of workshop participants will be organised in a "Heurigen Location" in Vienna, covering costs by participants. More information to be provided (time and place and map).

Supported by:

Figure 35: Agenda of "Workshop: Interoperability in Data Spaces"

Figure 36: Presentation at the "Workshop: Interoperability in Data Spaces"

The second workshop was titled "**Towards Data Spaces Interoperability Workshop on standardisation" and co-organised by BD4NRG, TRUSTS and IDSA**"

Date: November 23, 2022 - 9:00 - 10:00 (the organisations has proposed to move to 22nd if it is better for us)

Description:

One of the significant challenges of data spaces is interoperability; when closed data ecosystems evolve to open ecosystems and federated ecosystems (data spaces) increase the requirements for interoperability between data spaces.

Data spaces require data interoperability and metadata for data exchange and shared use of data. In this case, vocabulary is needed to harmonise the understanding of the meaning of the data itself. Participants in one data space can operate in other data spaces, so a unique digital identity is needed to identify and authenticate participants.

Several initiatives and projects are working on overcoming this challenge and contributing to making data spaces interoperable.

During this session, we will have four presentations explaining to the audience how this project has contributed to data space standardisation.

Agenda:

Moderator: Sebastian Steinbuss (IDSA)

- **DSBA Architecture convergence** and standards from DSBA and DSSC project. – **Juanjo Hierro - FIWARE**
- Data sharing spaces and interoperability position paper presentation – **BDVA – Antonio Kung**
- **TRUSTS & W3C semantic** standardisation workshop results presentation – **Robert David and Victor Mireles-Chavez from Semantic Web**
- **Energy data spaces** interoperability challenges. – **Matthijs Punter (TNO) from BD4ENG project**
- Best practices for supporting **data spaces and marketplaces interoperability – Achille Zappa (Insight) – i3-Market project**

More information about the outcomes and recommendations for standardisation bodies is available in D7.6 "Report on standardisation activities".

T7.5 Commercialization activities and action plan

The goal of Task 7.5 has been to explore and define the strategy for bringing TRUSTS to the market. In order to do so, we have defined the TRUSTS value proposition, enumerating the features, services and key developments which differentiate TRUSTS solution in front of potential competitors. Specifically, TRUSTS aims to fulfil three roles in the EU data economy, and these are:

1. A data marketplace
2. A platform federator
3. An ecosystem facilitator of data marketplaces

This task has also conducted a market assessment, enabling the Consortium to understand the need and demand for what TRUSTS is offering in the market, and the market competitiveness. It also helps to detect opportunities, growth drivers and market trends.

With the objective of elaborating a benchmark and exploring the more extended business models for data trading, a total of 180 companies offering data products on the internet have been analysed. For the identification of the target companies, data trading businesses have been identified, by either searching the internet with specific keywords, or by browsing articles on the web, whitepapers, public videos, product brochures and presentations. After an initial assessment, the entities were classified depending on parameters like type of data traded, target industry, and business models. We then proceeded to discard the ones not offering paid data products in the market, online advertising platforms, internet service providers not specifically offering data products, concept projects, and open data repositories, which resulted in a total of 97 selected companies revised in detail.

Within this context, LSTech have analysed:

- How different entities are selling data in the market?
- What kind of relationships are taking place in the value network?
- How is data trading evolving?
- What challenges must be overcome in order to leverage the power of data in the markets?

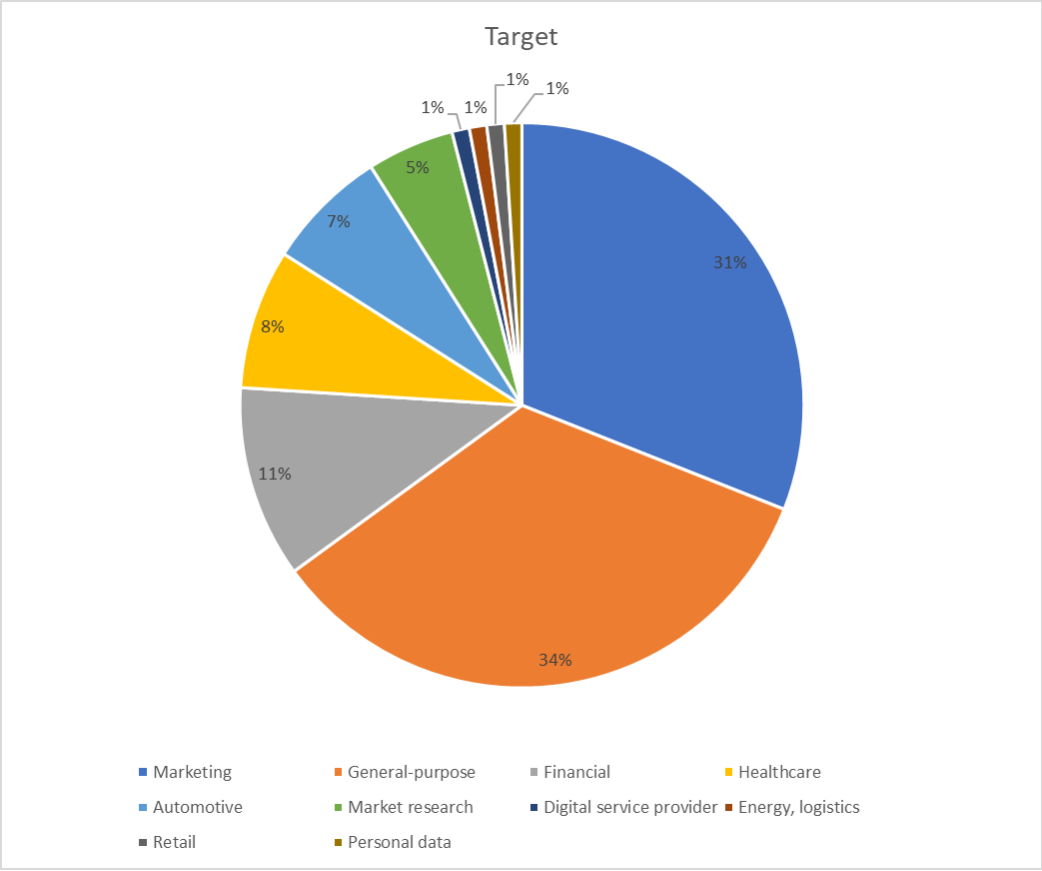


Figure 37: Types of data traded in the sample

LSTech has continued with the exploration of the different exploitation pathways from two different perspectives, first as TRUSTS as a single solution to be offered to the market and secondly, as a breakdown of components and pieces of software feasible to be exploitable.

Table 9: Overview of roles in the commercial exploitation

Entity	Platform provider	Intelligence services provider	Subcontracting agreement for support / development	IP licensing	No involvement
	Operates a shared infrastructure enabling intelligence services providers to leverage it for their own business model	*Ability to deploy and/or manage an intelligence service to be provided through TRUSTS platform or stand-alone service*	*Deep knowledge or expertise regarding a service or its inputs*	*IP licensing of IP developed during TRUSTS project*	*Will not be involved in the commercialization (except for informal facilitation of contacts/ dissemination)*
LUH					✓
SWC		✓ (Semantic layer T3.4)		✓ (GNU Affero)	
KNOW		✓ (Brokerage T3.6)	✓	✓ (Proprietary)	
TUD					
KUL					
FHF		✓ (Smart contracts (T3.2)		✓ (Apache License 2.0)	
RSA		✓ (De-anonymisation/anonymisation toolkit (4.3))		✓ (MIT License)	
G1					
IDSA					✓
DIO					✓

NOVA	✓				✓
PB					
EBOS					
LST		✓			
REL					
FORTH					
EMC Israel		✓ (Compute intense neural networks over several nodes)			

Then, following the SWOT (Strengths, Weaknesses, Opportunities and Threats) model, LSTech has proceeded to identify the situational assessment related to business competition, which can help in decision-making processes because it evaluates the strategic position of the project results.

Finally, the conclusions of the business plan analysis and commercialisation strategies, together with the next recommended steps for bringing the TRUSTS solutions to the market have been compiled and detailed in the final version of the deliverable D7.8 Business plan and implementation action plan II, delivered by the end of December 2023.

T7.6 Innovation Impact Assurance

Aspiration of this EU funded programme is to bridge from research to market, that is to move beyond (research) output to outcomes and defined impacts. Thus, research findings, concepts and prototypes shall be usable for the next level of development and adoption by pertinent (industry) players in the wider business ecosystem. To enable this, task T7.6 was tasked to work with all work packages and tasks to both ascertain from the outset and throughout the project that the aspired Outcomes and Impacts are kept in mind and guide Output creation. The previous experience from the Data Market Austria shows that this dramatically improves research transferability and hence business viability, whilst it also reduces efforts for conceptualization or technology development. Thus, continuous interactions with all WPs and tasks through regular check-ins, coordinated with project management (WP1) were deemed of paramount importance.

In facilitating and delivering these, T7.6 also complemented and enriched WP1 by enabling a firmer content-involved challenger role of project management as compared to a more coordinating role.

The formally agreed deliverable of T7.6 was a continuous interaction with all WPs and tasks, acting as a cross-function to the program to ascertain and optimise innovation impact. Thus, building on the preceding work within the TRUSTS project, during the final year, "Innovation Impact Assurance"

- Ascertained linkage, increased synergies, and consistency between prior deliverables of tasks T2.1, T7.1, T7.5 and the updated / final reports of of tasks T7.1 and T7.5
- Acted as link pin to task T2.4, aligning emerging business architecture and technical architecture. Regular participation in technical conference calls and working sessions
- Conducted a range of evangelist interventions to focus and align all consortia partners to intra-ecosystem interoperability and TRUSTS architecture as both, data market and data market federator

3.7.3 Future Outlook

A critical evaluation of the project's overall achievements vis-a-vis innovation ambitions will be provided in the final set of project deliverables and during the project review conducted by the EC in February 2023.

3.8 WP8 Dissemination, Communication & Community Building

3.8.1 Objectives

WP8 includes dissemination, communication and community building. Efficient internal and external communication, as far as it does not fall under the tasks of WP1, is the overall goal of WP8. Efficient communication within the project is achieved through regular virtual meetings where reports on WP8 actions are shared and further planning is discussed. External communication is achieved through the quarterly newsletter and the design, production and publication of regular online content (via the website, social media, Youtube, podcast tool) to inform stakeholders and a wider public at national, European and international level about the project objectives and outcomes. The existing channels also serve the purpose of community building.

Another objective is to ensure open access to (non-confidential) research results and to make sure that these results can be securely accessed and preserved beyond the duration of the project. The project website has been expanded to include a research section to make it easier to read and find the research papers.

At the end of each project year, WP8 collects and documents the dissemination activities of all partners and reports on them in the annual dissemination report (D8.3[15] and D8.4[16]). Also, an overview of all activities from the whole project time is documented in the final dissemination report (D8.5).

3.8.2 Results achieved

This part is an excerpt of the Final Dissemination Report (D8.5), which was elaborated and published by WP8 in a detailed manner. It can be found on the TRUSTS website.

In 2022, the basis of project communication from previous years was expanded and effectively used with regard to the communication of processes and results. Content generation was strengthened through more project output and diversely placed in the media landscape.

[15] https://www.trusts-data.eu/wp-content/uploads/2020/12/D8.3_TRUSTS_Annual-Dissemination-Report-I.pdf
[16] https://www.trusts-data.eu/wp-content/uploads/2022/01/D8.4-Annual-Dissemination-Report-II_Dec2021.pdf

T8.1 Dissemination and Communication Strategy, design guide, materials, and communication channels

The communication and dissemination work carried out in WP8 follows the general outline of the GA and D8.1 Dissemination and Communication Strategy, Design Guide, Materials, Communication Channels[17].

Through the different formats and channels used within WP8 (LinkedIn, YouTube, podcast, blog posts, webinars, workshops, etc.), the visibility of the project was strengthened throughout the project period. In addition, the project partners participated in important events (in person as well as virtually) to promote the visibility of TRUSTS in an interpersonal way. A focus in the last project year was on communicating results and preparing communication beyond the end of the project.

T8.2 'Visual identity, website, and promotional materials'

A coherent and consistent recognition of the project is indispensable for a holistic success of the H2020 project. Within every communication action the in 2020 defined branding and visual identity of the TRUSTS project has been respected.

The essential website was set up prior to the beginning of the project in September 2019. It represents the main communication channel of the project. Within the duration of the project, it was regularly updated and filled with new content.

Promotional material (e.g. in the form of different leaflets and RollUps) were produced in 2021 - a virtual version as well as a printed one, to be distributed at live events and also virtual ones. In consideration of the environment, only a small print run (depending on demand) was printed. Besides general information about the project, material for the final project year was developed to show the process and results of TRUSTS. The focus was on the Use Cases, interoperability and the legal side of data sharing.

T8.3 'Large scale dissemination of projects impacts and results'

A key component in the communication and dissemination activities to engage stakeholders was continuity, meaning that it is important to publish content regularly. Therefore, the TRUSTS newsletter was published quarterly. Blog posts and posts on social media were published when needed (a frequency was only used for orientation), on the one hand to attract the attention of stakeholders and on the other hand to be able to react flexibly to processes and results and communicate them in the best possible way.

TRUSTS Consortium made efforts in community building with other initiatives and exchanges with various projects (e.g. safe-DEED, i3-market, truzzt, Green Data Hub). Partnerships were built while projects that started later than TRUSTS can build on existing project outputs.

Under the title "The Federation of Data Markets and the Importance of Data Sharing in the EU'' partners of the TRUSTS Consortium examined relevant aspects of business, legal and ethics perspective as well as privacy issues when it comes to data markets and data sharing at the TRUSTS MidTerm Event in March 2022. The online event showed important aspects and where TRUSTS contributes. Target group of this event were similar initiatives such as e.g. i3Market, DOME, possible follow-up project partners / initiatives as well as partners from academia, data-driven businesses and public authorities. 49 people registered for this event - afterwards the recording was also uploaded to YouTube for others interested, those who could not join and also the possibility to follow TRUSTS developments after the end of the project.

[17] https://www.trusts-data.eu/wp-content/uploads/2020/09/TRUSTS_D8.1_-Dissemination-Plan_submitted.pdf

In total TRUSTS has organised 8 hands-on workshops/webinars, additionally to general events and event slots. It was important to the Consortium to depict a broad variety of topics to interested stakeholders and test out their interest in different aspects. So, following an introductory workshop in the first project year, topics like business models for data markets, legal aspects of federated data sharing, technical privacy preservation in federated data architectures, learnings from the TRUSTS use cases were featured among others. Average real-time viewers per webinar were 30, via additional promotion on various project channels, the Consortium was able to raise that number to 85 in total (via e.g. Youtube). To the consortium, this is a success because the personal exchange with interested parties anchors the achievements in perception and raises awareness for the possibility of further exchange with project partners.

TRUSTS had its final event at the European Big Data Value Forum 2022. To inform about the process and results TRUSTS had a booth at EBDVF as well as a 60 minutes session. Under the title "Future of Europe's Innovations: Federated Data Sharing Environments – TRUSTS'' partners of the Consortium gave an overview of the project and its development, gave insights into federated data sharing environments and terms, as well as a high level technical overview of interoperability and its importance, talked about legal frameworks for such federated environments and about how TRUSTS applied the legal and ethical rules and technical interoperability into the TRUSTS UCs.

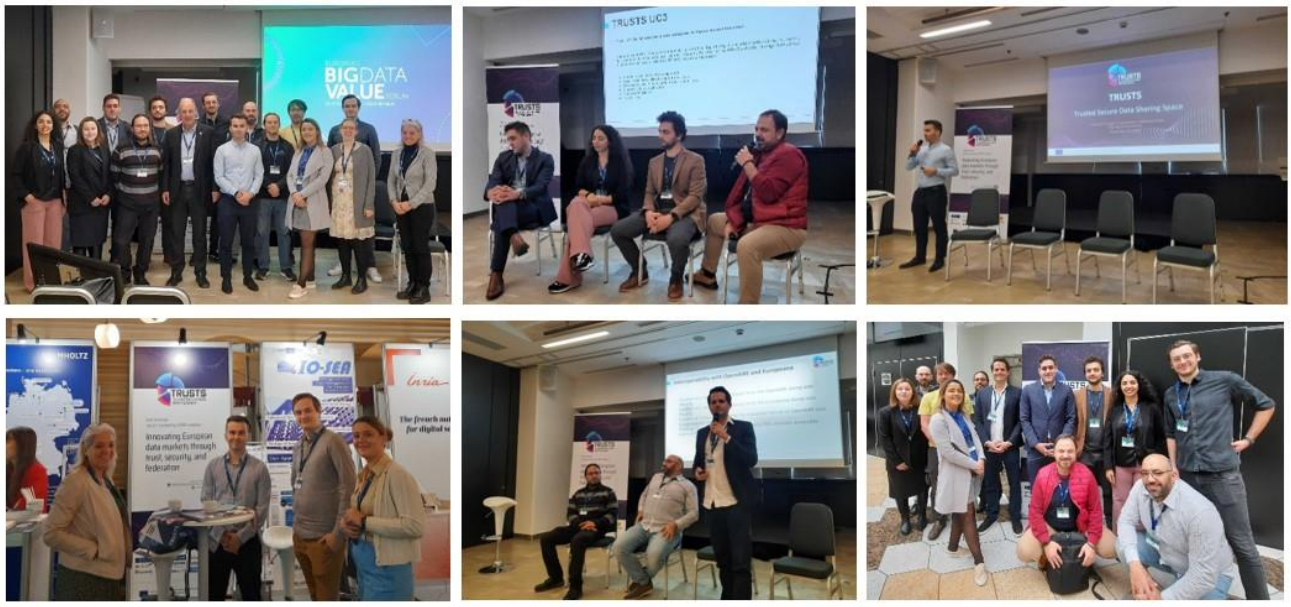


Figure 38: TRUSTS Partners at the European Big Data Value Forum 2022 in Prague, Czech Republic

In terms of KPIs for communication and dissemination, TRUSTS performed very positively and overachieved many of the KPIs by the end of the last project year.

Table 5: Impact of communication and dissemination activities

Channel	KPI and estimated number of persons reached	Type of audience reached in the context of the dissemination & communication activities
Project website (including blog posts on news page)	13,434 visits/month 6,851 visitors/month	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.
Social media (Twitter, LinkedIn, YouTube ResearchGate)	Twitter: 472 follower, 129 tweets LinkedIn: 527 follower, 145 posts YouTube: 36 subscribers, 3 posts ResearchGate: 8 follower, 12 updates	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.
Scientific publications	11 publications	Scientific community (researchers, universities, etc.), policy makers, EU projects, media representatives
Conference attendances	9 attendances	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.
Meet-up attendances	9 attendances	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.
Press releases	3 press release[18]: 9,000 editors; 21,000 mail subscribers[19] 44 visits on website	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.
Newsletters	4 newsletters[20] 975 subscribers	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology

[18] 1 more is planned for publishing in December 2022

[19] https://apa.at/produkt/ots-verbreiten/

[20] 1 more will follow in December 2022

	Opening Rate 6th NL (addendum 2021): 15,04% 7th NL: 15,35% 8th NL: 14,14% 9th NL: 13,38%	platform, data market standardisation body.
Podcasts	1 podcasts 31.08.2022: 55 views (YouTube, Website, Podigee)	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.
Webinars / Workshops	1 webinar, 86 participants/viewers	Scientific community, media representatives, policy makers, data and service providers, data consumers, EU projects, competence center/digital innovation hub, technology platform, data market standardisation body.

T8.4 'Training and capacity building programme'

Several reusable capacity-building assets were generated throughout the development of the Linked Open Statistical Data (LOSD) Pipeline. These assets will support the continued use and adoption of Pipeline in the future. TRUSTS will create a European data market based on secure & trustworthy data exchanges with a focus on the telecom and banking/fintech sectors, building upon the reference architecture model for data spaces of the IDSA2 and the knowledge gained in the project "Data Market Austria". During the development of the TRUSTS data market, several reusable capacity-building assets were produced. These assets will support the continued use and adoption of TRUSTS pipeline in the future.

The learning objectives for internal capacity training were:

1. To be able to define key terms relating to TRUSTS Knowledge Transfer Methodology.
2. To be familiar with the Knowledge Output collection process, including Knowledge Output Table completion.
3. To be able to assess, analyse and prioritise Knowledge Outputs.
4. To be able to determine and describe the necessary pathway to achieve an Eventual Impact.
5. To be able to identify and profile potential end (and Target) users and audiences.
6. To learn how to plan, carry out an=- measure Knowledge Transfer.
7. To be able to assess and measure the impact that has been achieved from implemented Knowledge Transfer activities.
8. To be able to develop case studies illustrating successes of the TRUSTS Knowledge Transfer Methodology.

Combining Existing Materials with New Trainings

Within the capacity building activities, TRUSTS has relied on a hybrid approach where we have combined mapping of existing training and capacity building materials with new activities and new materials developed

within the framework of the TRUSTS project. In this way, we have aimed to limit the replication of effort and leverage on already existing and relevant materials. Therefore, other projects have been scouted to see what (training) materials they offer. Overview of identified relevant materials was first provided in D8.6. and the following section offers an update with new materials that can potentially be referenced in the TRUSTS community. Materials from other projects can be found on TRUSTS portal under Training here.

Peer exchange and the LXP portal

The capacity building via peer exchange is also supported via a Learning and Exchange Platform (LXP) which aims to stimulate the continuous exchange among hubs. The platform has two main functionalities:

1) It provides access to content organised in courses, divided in various modules. Each of these provide content on a specific topic, stimulating self-study in small, easy-to-follow pieces (a video, article, template, etc).

2) Possibility to directly 'chat' and exchange with other hubs. The function of these chats is to start discussions on a particular topic. This chat is moderated by topical experts. The LXP is mostly supporting and acting as a follow-up of the peer exchange meetings. The link to the LXP is also provided under Tools of the TRUSTS portal. The LXP tries to balance the value of peer-to-peer interaction and the time and effort it takes versus the reusability and a-synchronous use of online tooling.

TRUSTS Webinars

Webinars were created to further explain the possibilities and usability of the TRUSTS platform.

- **The Core of TRUSTS**
  What is the TRUSTS project all about? Watch this webinar to get to know the project and its central aspects as well as the link to the European Data Strategy. The webinar can be found here: https://youtu.be/vPzQZXhm7uM
- **Business model options in the TRUSTS data ecosystem**
  The consortium members Andreas Huber (CEO, Governance One) and Bert Utermark (Partner, Trusted Data Analytics) discussed business model considerations of the emerging TRUSTS data market and delved into the topics of data markets taxonomy, value creation and USPs en route to business sustainability. The webinar can be found here: https://youtu.be/8PW5s9PH6j0
- **TRUSTS & Safe-DEED: Sharing data legally**
  What does the lack of legal clarity on data processing and the Data Governance Act have in common? Lidia Dutkiewicz (TRUSTS) and Alessandro Bruni (Safe-DEED) from KU Leuven discussed the legal aspects of data sharing platforms and answered frequently asked questions. The webinar can be found here: https://youtu.be/8qoMS7UejM0 -
- **TRUSTS & Safe-DEED: Privacy & Data Sharing**
  When it comes to data sharing, privacy and the preservation of privacy are the most future-relevant topics. Ioannis Markopoulos, (Forthnet, TRUSTS & Safe-DEED) and Alexandros Bampoulidis (RSA FG, TRUSTS & Safe-DEED) talked about privacy risks, and GDPR roles and demonstrated these risks. Lukas Helminger (KNOW Center GmbH, TRUSTS & Safe-DEED) shared insights and practical aspects from an end-user perspective. The webinar can be found here: https://youtu.be/8qoMS7UejM0
- **TRUSTS & Safe DEED Webinar Business Aspects of Data Markets**
  The third session of a collaborative webinar series by the EU Horizon 2020 projects TRUSTS (trusts-data.eu) and Safe-DEED (safe-deed.eu) was all about Business Aspects of and in Data Markets. Since

a few years the global business structure transforms into an intangible one, which means that tangible assets gradually lose their importance and are replaced by software, R&D, etc. Ioannis Markopoulos (Forthnet) and Gianna Avgousti (EBOS Technologies) address the importance of this development and give insight in business transformation and fruitful potentials in the webinar. The webinar can be found here: https://youtu.be/9MW7uWKv8n8

Several podcasts have been created by TRUSTS partners answering questions about what the TRUSTS project is and how you can get involved through the TRUSTS platform.

- Get an insight into TRUSTS: What is the project all about? What are the motivations, objectives, goals but also risks? Are there already existing data markets? How can data markets be connected? How could such a connection be implemented technically? We can find the answers to these questions here: https://trusts.podigee.io/1-data-markets-and-interoperability

- The business perspectives of TRUSTS and the chances and risks of data markets: How will data markets shape the European industry? What are the business perspectives of the TRUSTS project? What are the benefits and risks? We can find the answers to these questions here: https://trusts.podigee.io/2-how-will-data-markets-shape-the-european-industry

- Where are the major voids and controversies concerning the legal situation when it comes to data sharing? How will TRUSTS help the EU policymakers tackle the legal framework regarding data transactions? Yuliya Miadzvetskaya from the KU Leuven tells you more about the legal aspects of TRUSTS and the challenges in data sharing here: https://trusts.podigee.io/3-data-sharing-and-eus-digital-strategic-autonomy

- Business models and data governance aspects are essential to platform commercialization beyond the development phase. The interview partner of this episode – Antragama Ewa Abbas – and his colleagues from TU Delft are responsible for developing and evaluating sustainable business models for TRUSTS. In this podcast, he talks about what we do – and do not – know about data market research. This podcast can be found here: https://trusts.podigee.io/4-what-we-do-and-do-not-know-about-data-market-research

- Which criteria are relevant for developing a platform like TRUSTS data market federation, how the process looks like and gives an insight to what features the platform will provide? https://trusts.podigee.io/5-episode-5-trusts-platform-getting-into-shape

- Within this episode Natalia, who is currently project and innovations manager for the International Data Spaces Association (IDSA) – talks with Nina about what the IDSA is supporting TRUSTS with, about the IDS reference architecture and why it is guiding for TRUSTS, Data Sovereignty and Standards: https://trusts.podigee.io/6-episode-idsa-in-trusts

- Silvia Castellví, project manager of the TRUSTS project in the International Data Spaces Association (IDSA) talks with Nina Popanton about standardization activities, the latest workshop on Data Spaces & Semantic Interoperability, trustworthy collaboration, and the community. https://trusts.podigee.io/7-neue-episode

Internal Capacity Building

The Leader of TRUSTS Capacity Building Manos Paschalakis (RELA), was responsible for providing support to the Knowledge Fellows, updating the methodology and associated processes, which has evolved from previous EU funded Knowledge Transfer initiatives, and building capacity internally and externally to the project. As the Fellows were predominantly supported by the Competence Node Lead, it was determined that the first round of training would be provided to both the Knowledge Fellows as well as the Competence Node Leads. A further round of training would be provided to the wider TRUSTS partnership. Preparation for Internal Capacity Building In advance of the first TRUSTS Internal Capacity Training, RELA developed guidelines outlining the TRUSTS Knowledge Transfer Methodology. Significant resource was spent on finding the most suitable and efficient method to:

- Identify relevant and collect quality Knowledge Outputs.
- Record the status of collected Knowledge Outputs using a Knowledge Output tracker.
- Analyse and prioritise Knowledge Outputs for transfer.
- Identify an Eventual Impact.
- Visualise a Knowledge Output Pathway.
- Profile a Target User.
- Structure a Knowledge Transfer Plan.
- Determine impact indicators.
- Report on activities in the form of a case study.

TRUSTS Meetups

We have the opportunity to exchange thoughts and ideas through regular meetups. The meetups are dedicated to more general topics and provide a room much more open, than for example webinars for discussions, brainstorming etc. Meetups can be organised in different forms and follow different methods e.g., the World Café method, so that the participants can get together in smaller groups, discuss and get their questions answered. TRUSTS already had its first World Cafe meetup where 25 participants discussed for the following subjects:

- "Data sharing vs data trading" (moderated by: Ioannis Markopoulos, FNET)
- "Business models for datamarkets" (moderated by: Hosea Ofe, TUD)
- "Technical aspects of datamarkets" (moderated by: Martin Kaltenböck, SWC)
- "Environmental & social aspects of datamarkets" (moderated by: Stefan Gindl, RSA)

Besides the meetups TRUSTS also organized two public events, a mid-term in March 2022 where partners of the TRUSTS Consortium examined relevant aspects of business, legal and ethical perspectives as well as privacy issues when it comes to data markets and data sharing and a conclusive one in November 2022 that took place at the European Big Data Value Forum (EBDVF) 2022 an event titled "Future of Europe's Innovations: Federated Data Sharing Environments – TRUSTS'' where partners of the Consortium gave insights into federated data sharing environments and terms, along with technical shallow dive into interoperability and its importance, talked about legal frameworks for such federated environments and about how TRUSTS applied the legal and ethical rules and technical interoperability into the TRUSTS UCs.

3.8.3 Future Outlook

In order to ensure that the efforts carried out by the Consortium will remain publicly available to interested parties, the project website including all public project outcomes will remain online. DIO - which is Austria's national collaboration platform for the data community (currently with approx. 200 member organizations) - will further host the subpage of the project on its own website. Additionally the contact address will remain active if interested parties want to have a more detailed exchange with TRUSTS Consortium members. Relevant Outputs of projects that are relevant for the further development of Data Spaces, Data Markets and other federated data sharing infrastructures will be re-used in various initiatives (e.g. the Green Data Hub, and relevant projects) by all partners. All contents on project channels (e.g. Youtube, TRUSTS Knowledgebase) will also remain online for interested stakeholders. All partners commit to integrate project learnings in future projects and their communications and community building efforts.

3.9 WP9 Ethics requirements

3.9.1 Objectives

The WP9 "Ethics Requirements" was added by the EC in order to ensure that compliance mechanisms for ethics requirements as described in the GA, Annex 1 are established. Multiple ethics requirements and a set of measures that ensure compliance with these ethics requirements are laid out in terms of 10 deliverables of this WP. Compliance with ethics and legal requirements are considered a continued effort by the partners.

The following actions were taken in order to achieve the objectives of this WP:

- The templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) were kept on file.
- Prepared a statement from the designated Data Protection Officer that all personal data collection and processing will be carried out according to EU and national legislation.
- Explained how all of the data they intend to process are relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle).
- Described the anonymisation/pseudonymisation techniques that will be implemented must be submitted as a deliverable.
- Provided an explanation how the data subjects will be informed of the existence of the profiling/ tracking, its possible consequences and how their fundamental rights will be safeguarded. This must be submitted as a deliverable. The beneficiary must provide details on the Artificial Intelligence/ Data Mining system and related decision making procedures including information about human actors' roles and responsibilities.
- Described a set of precautions to eliminate or mitigate potential algorithmic biases and explain how the model will be able to justify the results it has provided for specific situations. This must be submitted as a deliverable.
- Confirmed that the beneficiary has a lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable.

3.9.2 Results achieved

WP9 has concluded at the beginning of the second year (M15, March 2021) with the submission of D9.9 OEI - Requirement No. 15. The results have been reported within the deliverables of WP9 as well as in the deliverable, D1.3 "Annual Public Report II". In terms of this WP, all consortium partners continuously monitored potential legal and ethical risks. KUL being the central contact point for ethics related questions and ongoing close collaboration between KUL and LUH and partner's legal departments and DPOs.

4 Progress within specific Leads

4.1 Scientific Lead

Objectives

As defined in "TRUSTS D1.2 Annual Public Report I", these are the key objectives of the scientific lead:

- Ensure compliance with the H2020 Open Access policy.
- Promote the application of research practices.
- Monitor and foster progress towards collaborative research within the project.
- Create and enforce the structure for reporting on scientific progress.
- Provide opportunities for identifying and/or enhancing research opportunities.
- Ensure research activities remain focused on and cover the Call's specific challenges and objectives.
- Facilitate learning of research lessons at a metalevel
- Maximise research synergies and opportunities

They have remained unchanged since annual reports I and II.

Results achieved

The publication output was estimated with 19 publication in the previous report. TRUSTS has exceeded this goal, the partners have published 22 articles in total. All "ICT13-2018-2019 specific challenges" have been addressed, in the following we list the publications for each challenge:

- C1 Lack of trusted and secure platforms for sharing personal and industrial data: **12**
- C2 Lack of privacy-aware analytics methods for secure sharing of personal data and industrial data: **10**
- C3 Lack of ICT and Data skills seriously limits the capacity of Europe to respond to the digitization challenge: **3**
- C4 Involving SMEs and giving them access to data and technology: **1**
- C5 IT standardisation faces new challenges as technologies converge and federated systems arise, creating new gaps in interoperability: **10**
- C6 Advance the state of the art w.r.t. scalability, computational efficiency of methods to secure desired levels of privacy of personal data and/or confidentiality of commercial data: **4**
- C7 Analyze and address privacy/confidentiality threat models and/or incentive models for the sharing of data assets: **4**

Note: the articles published per challenge do not sum up to 22 publications, because some articles address more than one challenge.

In 2020 (first year), TRUSTS had 2 publications, in 2021 7 publications, in 2022 11 publications, and there are 2 accepted articles which will be published in 2023.

The scientific coordinator has monitored the output of research efforts and actively ensured the achievement of publications in all ICT13-2018-2019 specific challenges.

Future Outlook

The scientific coordinator will support researchers during the last phase of TRUSTS and monitor research activities. The acceptance of a number of publications is still pending. The scientific coordinator will compile and summarise the research efforts for the review by the European Commission and also present the final number of publications in the last review by the EC.

4.2 Technical Lead

Objectives
In TRUSTS, the main objectives of the technical lead were: 1. Technical project management including overview of the work to be performed in WP3 in accordance with the DoA. **(TL-01)** 2. Coordination with the related work packages working in close collaboration with WP3. **(TL-02)**
Results achieved

In the third and last year of the project, the main task of the technical lead has been coordinating the project's technical work to ensure smooth development. Development had to proceed in accordance with the conceptual foundations gathered and further developed during the whole project lifecycle.

With regards to the objective **TL-O1**, the technical lead has established the following management instruments:

- A regular telephone conference for all WP3 participants (**every week**). This allows task leaders to report on progress and obstacles, and provides an easy way for participants to reach out beyond the context of their own task without formal overhead to allow synchronisation between tasks.
- A regular telephone conference for only the technical WP3 participants (**every week**) for coordinating the development sprints of the platform development, which brings together developers and technical experts from the work packages involved in the development sprints.
- Allocation of an urgent telephone conference in case the first two telephone conferences were not enough to discuss certain development tasks or other management issues.
- Availability for telephone calls to exchange feedback and ideas on short notice whenever urgently required by a project participant.

With regards to objective **TL-O2**, the technical lead has participated in or organised the following activities:

- Participating in plenaries led by WP1. In presentations of the technical lead, technical achievements were presented and discussed with the entire project consortium.
- Regular meetings with the WP5 participants to ensure a smooth development phase in which feedback from WP5 participants is continuously taken into account.
- Continuous tracking of tasks and responsibilities to ensure fluid communication within and between work packages.
- Coordinate meetings between a smaller number of organisations depending on discussion items.

Furthermore, the technical lead has participated in the European Big Data Value Forum in Prague (EBDVF 2022) for a one-hour session to present the Future of Europe's Innovation using Federated Data Sharing Environments with the TRUSTS platform. As well as we had a booth in the forum to find new and optimal partners and a community that support our project and also to discuss with the external stakeholders the future needs of the data markets and how TRUSTS leverages those gaps by its current and future functionalities and services.

Future Outlook

Once an operator is found to operate the TRUSTS platform, then architecture design can be improved to meet the up-to-date technologies at that time. Maybe also, the missing part which is related to the billing functionality can be added since what is available in the current platform contains only the base function which enables the customers to pay for their services and datasets. Furthermore, the operator can follow the same or different management strategies to keep track of the future development and testing tasks.

4.3 Innovation Lead

Objectives

Innovation management ensures that the development of both market and technical problems will be accomplished during the project, while enabling the implementation of appropriate creative ideas, so that new and improved products, services and processes will belong to the project's output ensuring thus its sustainable update beyond its duration.

Results achieved

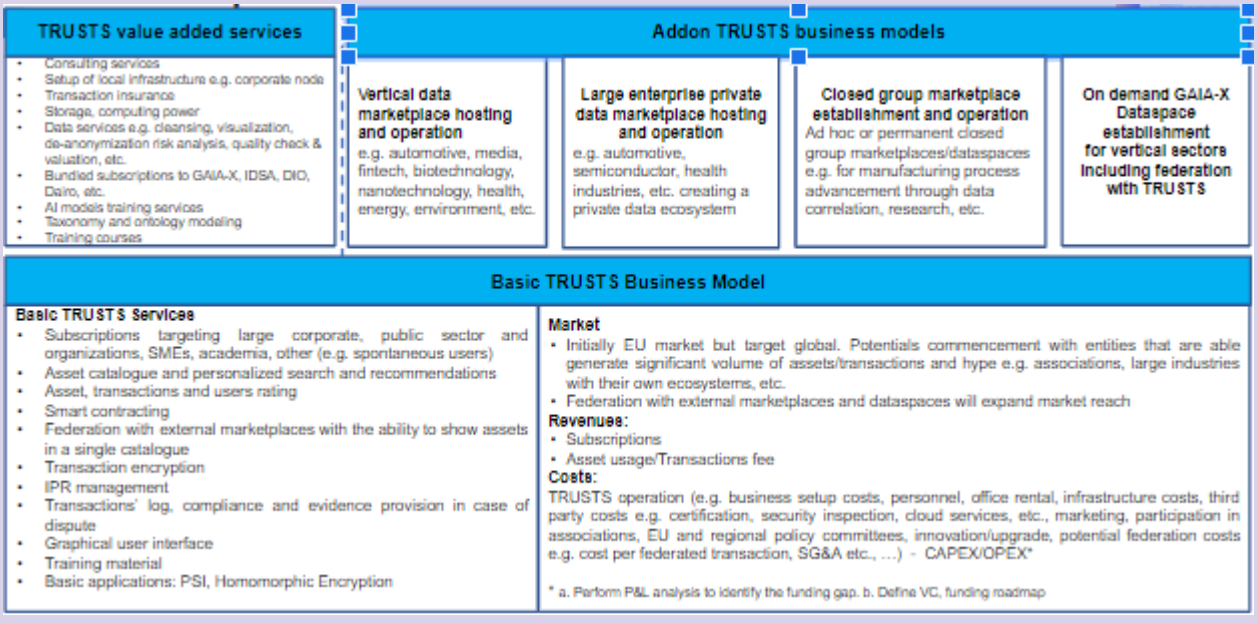
In the final year of the project, the TRUSTS business model was agreed within the consortium and finalised. This included three main parts. First the basic TRUSTS business model, second the value-added services and finally possible addon business models:

- **Basic TRUSTS Business Model**
  Basic TRUSTS Services
- Subscriptions targeting large corporate, public sector and organisations, SMEs, academia, other (e.g. spontaneous users)
  - Asset catalogue and personalised search and recommendations
  - Asset, transactions and users rating
  - Smart contracting
  - Federation with external marketplaces with the ability to show assets in a single catalogue
  - Transaction encryption
  - IPR management
  - Transactions' log, compliance and evidence provision in case of dispute
  - Graphical user interface
  - Training material
  - Basic applications: PSI, Homomorphic Encryption
  - Market
  - Initially EU market but target global. Potentials commence with entities that are able to generate a significant volume of assets/transactions and hype e.g. associations, large industries with their own ecosystems, etc.
  - Federation with external marketplaces and dataspaces will expand market reach
  - Revenues**:**
  - Subscriptions
  - Asset usage/Transactions fee
  - Costs:
  - TRUSTS operation (e.g. business setup costs, personnel, office rental, infrastructure costs, third party costs e.g. certification, security inspection, cloud services, etc., marketing, participation in associations, EU and regional policy committees, innovation/upgrade, potential federation costs e.g. cost per federated transaction, SG&A etc., …) - CAPEX/OPEX*
  - * a. Perform P&L analysis to identify the funding gap. b. Define VC, funding roadmap

- **TRUSTS value added services**

- Consulting services
- Setup of local infrastructure e.g. corporate node
- Transaction insurance
- Storage, computing power
- Data services e.g. cleansing, visualisation, de-anonymization risk analysis, quality check & valuation, etc.
- Bundled subscriptions to GAIA-X, IDSA, DIO, Dairo, etc.
- AI models training services
- Taxonomy and ontology modelling
- Training courses

- **Addon TRUSTS business models**
  - Vertical data marketplace hosting and operation
  - Large enterprise private data marketplace hosting and operation
  - Closed group marketplace establishment and operation
  - On-demand GAIA-X Dataspace establishment for vertical sectors including federation with TRUSTS



Future Outlook

- The above presented business model gives propositions to a potential TRUSTS platform operator highlighting the basic services that TRUSTS provides, the applicable market and financial aspects such as revenues and costs. In the future, potential operators will be able to extend these services with some of the proposed value adding ones, or with others of their own. The proposed additional TRUSTS business models will give alternatives for the transformation of TRUSTS data marketplace.

4.4 Security Lead

Objectives

The primary objectives of the security lead were as follows:

- Monitor the usage of different security and privacy preserving technologies and techniques on the various project tasks
- Flag security risks and vulnerabilities as they are discovered. A vulnerability in the blockchain development kit which was used on this project which could be exploited for a denial of service attack was discovered by the NIST national vulnerabilities database, and the subsequent patch released for this was applied to the TRUSTS development environment blockchain located within the Smart Contract Demonstrator component.
- Develop a list of real practical attacks against similar blockchain-based and smart contract utilizing systems
- Keep development choices relevant to security-based functional requirements
- Investigate security enhancing and privacy preserving approaches to apply to blockchains and smart contracts
- Monitor security enhancing and privacy preserving technologies brought into the TRUSTS project

The TRUSTS project should ensure data security by carefully evaluated for two main aspects:

1. GDPR Compliance – TRUSTS aims to create a GDPR-compliant European Data Marketplace by respecting the rules and principles through constant guidance from a leading expert partner in law and ethics in the Consortium, KUL, and by taking into account already existing national and international initiatives.
2. Privacy Preserving capabilities – The TRUSTS partners will develop and improve privacy preserving technologies to foster the European Data Economy and at the same time provide business and ethical/legal tools to make these technologies easily adoptable and sustainable.

Results achieved

WP3

- General security practices were used in WP3. Port restrictions saw ports closed by default and only opened where necessary. Access to the various containerized services was restricted by default and provided on request as needed. Google cloud authentication was used to managed general authentication to the development environment
- Research was conducted which collated a list of common vulnerabilities in blockchain based and smart contract utilising systems. This research was underpinned by writings based on sources which detailed past practical attacks against such systems. The full writings can be found in D3.3.
- Research was conducted to assemble a list of security enhancing and privacy preserving technologies and approaches which are applicable to blockchain and smart contract based systems, these included; approaches for updating smart contracts in the context of immutable blockchain, leveraging secure enclaves, secure multi-party computation, and more. This work can be found in D3.3, though technical implementation of this work was mostly out of scope.
- The research carried out on security enhancing and privacy preserving approaches for smart contracts and blockchain system was used to account for updating of smart contracts in a way

that circumvented the blockchain's immutability: on-chain pointers and off-chain isolated, containerized smart contracts (rather than on-chain smart contracts) was the model utilised for the TRUSTS smart contract demonstrator blockchain. This work is presented in D3.3.

- The IDS information model was used to underpin task 3.4. This model uses predicates which indicate the authentication for given endpoints, and necessitates mutual authentication between TRUSTS components using DAPS (discussed more in the next point).
- The IDSA DAPS component utilised in TRUSTS supports secure communication channels, default authentication that can perform actions such as issuing OAuth2 tokens, as well as authorization. DAPS is one of the essential services of IDS.
- IDS DAPS tokens are needed in order to access services and data of connectors on the TRUSTS platform. Certified connectors can use the protocol to connect and retrieve their access token, which is used for communication with other connectors. Permissions of access are specified by a connector that a requesting connector wishes to access.
- The IDS Trusted Connector component is an integral part of the TRUSTS platform which supports XML. The purpose of this component is to provide secure communications between applications within a participant, and between participants themselves.
- The TRUSTS platform addresses functional requirements as it offers its services, data and applications via secure peer-to-peer channels.

WP4

- The main objective of WP4 is focusing on privacy preserving capabilities.
- The main purpose of a data market is to be a platform for sharing data between different organisations and different entities.
- The main problem with data sharing is that from the moment the data is transferred to another entity, the data owner loses control over the use of the data, and in fact only a legal contract provides him with basic protection from misuse of his data.
- The problem is serious when it comes to companies' business data, the misuse of which harms the companies' IP, and it is even more serious when it comes to personal data, so there is also a regulation that comes to protect the individual and prevents the disclosure of his details to those who are not authorised to do so.
- In WP4 we explored the various possibilities to analyse the data in partnership with other companies, without disclosing it between the various participants.
- Our basic starting point was that in order to ensure complete protection of the data and its use, the raw data should not be allowed to leave the company's servers.
- Depending on the different needs of the collaborators, different methods were chosen for collaboration on the data without sharing it.
- One option is to use data anonymization functions, while assessing the risk of retrieving the original data.
- Additional options support data encryption like homomorphic encryption and multi-party computation, having the ability to decrypt the data only by the data owner.
- And finally, federated learning methods were examined and invented, which allow collaboration over the data without sharing the data itself and without revealing it to the various participants.
- Those capabilities actually change the definition of trust data market into "data market for non-sensitive data and collaboration platform for private and sensitive data."

Future Outlook
• The manual process of locating relevant system vulnerabilities is not sufficient to keep a system up-to-date and safeguard against attacks, for this an automated vulnerability scanner which generates reports should be utilised. • The research carried out on security enhancing and privacy preserving approaches for smart contracts and blockchain systems is of much use for protecting these elements of similar systems in future. • Future projects should focus on implementing collaboration platform, that will enable specific services for efficient collaboration

4.5 Legal and Ethical Lead

Objectives
The main objectives of WP6 (Legal and Ethical) as from M25 were the following: • To carry out the legal and ethical assessment of the TRUSTS project. This work is supposed to generate Deliverable D6.3. The legal and ethical assessment is based on a continuous analysis of the TRUSTS platform's technologies and workflows and on the legal and ethical requirements identified in Tasks 6.2. • To provide recommendations for policy makers and stakeholders. This work is supposed to generate Deliverable D6.4.
Results achieved
The work carried out under WP6 from M25 to M33 has resulted in the following: • KUL has provided continuous guidance on legal and ethical issues and questions of the TRUSTS consortium partners; • KUL has developed and circulated a legal and ethical checklist to receive input from the TRUSTS consortium partners concerning their implementation of the legal and ethical requirements; • KUL has drafted Deliverable D6.3 "Legal and ethical assessment" that contains the assessment of the TRUSTS platform from a legal and ethical perspective. The deliverable analyses the legal implications of the two pillars of the platform: the Federated Learning model and the anonymisation methods; then it discusses the implications of the three use cases on the application of several fields of EU law (platform regulation; competition law; consumer protection law; AI law; anti-money laundering law), identifying the areas where the law still needs to provide clear-cut answers; finally, the deliverable provides the legal and ethical assessment of the pilots conducted during the project to test the three use cases. • KUL has drafted Deliverable D6.4 "Legal and policy recommendations". This deliverable takes stock of the legal and ethical requirements and assessment conducted across the legal frameworks applicable to TRUSTS. It analyses challenges and opportunities stemming from this assessment and formulate recommendations addressed to both policy-makers - in order to improve legal certainty and clarity - and to stakeholders - in order to improve compliance.
Future Outlook

Review and adaptation of conclusions and recommendations based on feedback by the European Commission (February 2023).

4.6 Communication & Community Building Lead

Objectives
The main objectives of WP8 as from M25 were to ensure efficient internal and external communication and dissemination of the project. This year's focus was mainly on presenting relevant outcomes in diverse event formats, blogs, whitepapers and similar. The TRUSTS Consortium focused on outcome generation and communicated with respect to the results. The basis set in the previous years has been extended and utilised. Channels were further optimised and regularly filled with contents. 2022 followed a similar approach as the previous years to guarantee project communications consistency. Online activities and their reception (followers, reactions, etc. on social media platforms) was constantly rising.
Results achieved
The dissemination and communications efforts of TRUSTS bore fruits - in the sense of KPIs as well as in collaboration with other stakeholders and their interest in the project. Most of the KPIs set at the beginning of the project were exceeded, which shows that the communication strategy and approach 'Do good and talk about it' was adequate. The basis for project communications from the previous years was expanded and used effectively. The media mix was optimised and diversified. Content generation was strengthened through more project output and results and diversely placed in the media landscape. Those formats include blog posts, interviews, podcast, webinars; additionally, project partners attended key events to foster TRUSTS' visibility in an interpersonal manner. Also the final event took place at the European Big Data Value Forum 2022 as a 60 minutes session. This year's communication focus was more on the project's results, building on last year's progress of TRUSTS. The overall plan of WP8 was three-staged: general positioning, progress reports and the promotion of the (realistically expected) outcomes in the last project year. The KPIs defined in D8.1 were mostly overachieved.
Future Outlook
After completion of the project, the project website will remain online with all public project results. This will ensure that the work done will continue to be available to the interested community and that the (publicly accessible) results and learnings can be used for follow-up projects and the like. In addition, the contact address will remain active and maintained in case interested parties wish to have a more detailed exchange with the members of the TRUSTS Consortium. Relevant results of the project that are relevant for the further development of data spaces, data markets and other federated infrastructures for data exchange will be further used by all partners in various initiatives (e.g., the Green Data Hub). The project's channels and the content on them (e.g., Twitter, YouTube) will also remain online for interested stakeholders. The TRUSTS Knowledge base portal by EBOS will also remain live after the project's conclusion. All partners are expected to integrate the lessons learned from the project in future projects and in their communication and community efforts.

4.7 Business & Exploitation Lead

Objectives
The primary aim of WP7 was to investigate the business-related aspects of the development of the TRUSTS platform and to develop a concept for the business-like establishment of a TRUSTS OpCo. This involved exploring potential, possible, and promising business models and consolidating the results. The objective was to formulate concrete recommendations for the development and establishment of a TRUSTS operating company, which would be responsible for operating the platform. This work package played an important role in ensuring the long-term viability and sustainability of the TRUSTS platform and in creating value for all stakeholders involved.
Results achieved
The work carried out by WP7 of the TRUSTS project was focused on the business-related aspects and provided a solid foundation for the future establishment of TRUSTS OpCo. The project covered a wide range of business preparations, from exploring various business models (T7.1) to creating a comprehensive commercialization plan (T7.5). Moreover, the in-depth focus on aspects such as Intellectual Property Rights protection, Data Stewardship (T7.3), and Standardisation uptake and recommendations (T7.4) added further depth to the business considerations. Finally, the comprehensive Innovation Impact Assurance Analysis (T7.6) conducted a synthesis of all the business-related findings across all work packages, ensuring that all relevant aspects were taken into account. The outcome of WP7's efforts was instrumental in the successful establishment of TRUSTS OpCo, laying the foundation for long-term establishing a future TRUSTS OpCo. - A future TRUSTS OpCo operating company can draw on important groundwork. - Important and complex issues related to the business model have been comprehensively investigated and important groundwork has been laid for a future TRUSTS OpCo. - This ensures that the work done in the project will benefit a future operator of a TRUSTS OpCo or also other data platforms. - The publicly available results and lessons learned in terms of business models and usability can also be used by the general public for their own research or implementation or for follow-up projects and the like. - A (small) community of interested SMEs has been created, which can be activated and involved in further projects in this direction. The TRUSTS project laid important groundwork for the establishment of a TRUSTS OpCo by developing necessary artefacts and concepts. The notion of developing a self-sustaining data market was too ambitious. EU's efforts regarding the Gaia-X approach show that much more groundwork is needed in the areas of standardisation, interoperability, and particularly in preparing organisations that will later use the data market. A market for, say, vegetables does not develop on a "greenfield," but takes many years to grow from a single market stall to a large bazaar. The same applies to the TRUSTS project: it must start with a single (data) stall. The costs must be low enough for that single vendor to afford the stall fees. If this one vendor is successful, others will gradually join. In short, the chicken-and-egg problem is the biggest challenge in establishing a data market, and

specifically in the TRUST project, these costs are the technical costs of further development and the necessary costs of market development and market access. Adequate resources were not allocated for these three cost blocks.

To reduce the costs of further development, an innovative approach was developed within the project: TRUSTS-DAO, which distributes the development costs in a new way to the stakeholders of the future TRUSTS OpCo using a token-based approach. Translated to the vegetable stand image, the start-up costs are minimal and the profit grows with the success of the TRUSTs marketplace.

Future Outlook

During the project duration, it was not possible to establish an operating company with the existing consortium, which could have immediately started building and operating a TRUSTS platform after the project. The interests of the participants, who were composed of scientific and private companies, were too different. Scientific organisations had difficulties getting involved in a TRUSTs OpCo as shareholders because they are mostly public institutions. On the other hand, the participating SMEs did not have the financial room for the investments that would have been necessary to establish a TRUSTs OpCo. As a result, no one from the TRUSTs consortium wanted to continue operating the TRUSTs platform alone or together. One important reason for this was certainly that the technology with the TRUSTs platform has developed a functional infrastructure, but for a productive implementation in an industrial environment, the individual components have to be deeply interlinked. This task could only be done to some extent within the TRUSTs project. A future operating company would therefore have to first deal with the technical interlocking of the technical components and then move on to establishing the business model.

If it is possible to keep the initial start-up costs low enough through a model like TRUST-DAO, a TRUSTs OpCo can be established. But the consortium members must be willing to also take on entrepreneurial risk. Here, there probably needs to be special incentives, such as for research institutions, to be willing to carry entrepreneurial risk. If that is not the case, an investor group must be found to raise the funds for the start-up costs and then start entrepreneurially.

5. Update of the Data Management Plan

Within this chapter an update of the Data Management Plan (DMP) will be provided. The original version of the DMP was submitted as deliverable D1.6 in M6 (June 2020). A first update of this document was provided in M12 and submitted in terms of the Annual Public Report I. Two subsequent updates followed in M18, in terms of the mid-term review, as well as in M24 as part of the Annual Public Report II, reflecting the progress, current status quo and planning of the TRUSTS consortium. This is the fourth and last update as the project comes to an end.

The TRUSTS consortium was asked to provide updated information in order to report the latest progress and planning regarding the DMP. The content shared in this chapter is containing the following information:

- General information about DMP updates (sub-chapter 3.1)
- Information on processed and published data(sets) as of December 2022 (sub-chapter 3.2)
- Updates on relevant DMP dimensions (sub-chapter 3.3), including
    - Updates on data types, formats and files
    - Updates on FAIR and data security and
    - Report on actual data(sets) which were made available

5.1 General information about DMP Updates

The DMP (D1.6) provides information on TRUSTS data management policy and key information concerning the management of datasets created, processed and published within the TRUSTS project. Organisational and technical measures regarding data collection as well as the handling and storage of data are included in this deliverable. In addition to the original DMP, the DMP updates cover key aspects such as the responsibilities of the respective project partners, the compliance with the FAIR data principles (e.g. making data **F**indable, **A**ccessible, **I**nteroperable, **R**eusable) as well as information on data size, access, licensing and integration features in accordance with relevant legal framework and in particular the GDPR.

5.2 Processed and Published Datasets as of December 2022

So far, the published deliverables with included data have been made available on the TRUSTS website by the partner DIO. The respective items for the bibliography are described in Dublin Core[21]. The publications and the underlying public data are described in the metadata format of the respective repository, receive a persistent identifier such as Digital Object Identifier (DOI) or Handle wherever possible and are licensed under CC0 or CC-BY 4.0. Openly available data includes a bibliography of publications regarding the project (in text and XML format), as well as publications and underlying data, wherever possible according to H2020 open access policy and open research data pilot.

[21] The Dublin Core Metadata Element Set, short Dublin Core (DC), is a standardised metadata schema. http://dublincore.org/

5.3 Updates on Relevant DMP Dimensions

The following subchapter includes information about the updates on relevant DMP dimensions. The same approach as for the DMP Update for M12, M18 and M24 has been followed: the TRUSTS consortium has been asked to fill in corresponding templates, indicating what has been changed or achieved since M24 (December 2021). Some project partners have no updates on the DMP because they do not work with data. An overview of all data generated or re-used in the project can be found in Table 6 which is the update of Table 2 in the DMP (deliverable D1.6).

Updates on data types, formats and files

Eight out of 17 project partners updated information on data types, formats and files. EBOS partly acts as an open-public data provider and aggregator. EBOS in support of UC1 used two datasets in the scope of the project and WP5 trials in order to properly run the assets uploaded to the TRUSTS platform. The respective datasets (i.e., bank transactions) can only be used with their respective application, the data is anonymised and will not be available beyond the project duration.

G1 states that project documents like text documents, presentations and calculation tables have been collected in the context of TRUSTS. These are of the data types text (.docx), table (.csv, .xlsx) and presentation (.ppt) and comprise a data size of less than 1 GB. The documents as deliverables are accessible on the TRUSTS homepage.

IDSA has originally stated that together with TUD minutes from workshops are collected as textual and tabular data. Now IDSA does this alone. The minutes have been published as Workshop Report, Pictures & Slides on the TRUSTS website. Furthermore, IDSA has specified that the survey results conducted for the research across stakeholders were planned to be published on the TRUSTS website which has been done as part of Task 7.2.

KNOW has shared two more datasets via Zenodo. The one dataset is for studying popularity bias in recommender systems and the other for evaluating recommender systems for data markets.

KUL has added that the project deliverables are collected as textual data (.docx, .pdf). Their data size does not exceed 1 GB. The same is for the overview of literature and other sources used for legal and ethical research (e.g. journal articles and conference papers). For the bibliography of publications the textual data formats .docx, .html and .xml are used and for publications & data .pdf, .pdf/a and .docx. Descriptive metadata (abstracts, authors, publication tags, etc.) is also collected and published as TRUSTS deliverables. Publications used in the research are already in the public domain. The size of textual data (.docx, .pdf) is estimated to be small, less than 1 GB.

LST now collects scripts needed to facilitate project's implementation / development as well as parts of code. No personal or sensitive data is collected. The data size is estimated to be small, less than 100 MB.

RSA corrected the size of collected metadata of datasets from external datamarkets and EOSC initiatives from small to large with approximately 1 GB.

With TUD, Interview protocols and coding results for developing TRUSTS business model have been added. This textual data (.pdf) is of small size, less than 1 GB, and has been published. More data of the same type and size is collected which is included in the appendix of deliverable D7.2. The one dataset contains descriptive results of cross-case analysis for meta-platforms exercising aggregator business models. This

analysis is based on the secondary data available on the internet. The other dataset is a summary of workshop results for exercising TRUSTS business models. Furthermore, the online survey results for assessing TRUSTS business model impacts will be uploaded to the repository 4TU.Research Data when collection is finished.

Table 6: Details of data types, origin, format and size which have been collected, processed or generated within the TRUSTS project duration

Data that we will collect in the context of TRUSTS	**Expected format**	**Size**	**Partner**	**Planned publication of data (yes/no/TBD), if yes, where**
Project management data: time tables, deliverable plans, documentation & performance tables, information sheets	Textual (.docx) Tabular (.csv, .xlsx)	Small (<1GB)	LUH	Yes, at LUH Data repository (https://data.uni-hannover.de) and on the TRUSTS homepage (https://www.trusts-data.eu).
Metadata & semantic layer from TRUSTS Knowledge Graph; Mainly metadata, controlled vocabularies (e.g. country codes or industry classification). No sensitive data.	RDF in any serialisation	Small (<1GB)	SWC	Yes, in the form of the TRUSTS Knowledge Graph.
Algorithms design & implementation (transfer learning, recommender systems, privacy preserving analytics) to create publicly available data sets	Tabular (.csv, .xlsx) Code (.cpp, .json, .py) Textual (.pdf, .docx) Binary (Apache SOLR core)	Small (<1GB)	KNOW	In general, it is planned to share datasets via Zenodo or UCI Machine Learning Data (https://archive.ics.uci.edu/ml/index.php). T3.6: A dataset for studying privacy aspects of recommender systems was shared via Zenodo: https://doi.org/10.5281/zenodo.4031011. Another dataset for studying popularity bias in recommender systems is also shared via Zenodo: https://doi.org/10.5281/zenodo.6123879. And a dataset for evaluating recommender systems for data markets is also shared via Zenodo: https://doi.org/10.5281/zenodo.6517031.

A list of academic articles to investigate State of the art of data marketplace research. This data is also part of D2.1 deliverable "'Definition and analysis of the EU and worldwide data market trends and industrial needs for growth."	Tabular (.xlsx)	Small (<1GB)	TUD	Yes, https://doi.org/10.4121/14673813.v2 .
Documents collected for creating a taxonomy of data marketplaces	Tabular (.xlsx)	Small (<1GB)	TUD	Yes, https://doi.org/10.4121/14679564.v1 .
Overview of literature & other sources used for market research (e.g. journal articles & conference papers)	Textual (.doc, .docx) Tabular (.xls, .xlsx)	Small (<1GB)	TUD, IDSA	Yes, https://doi.org/10.4121/13142885.v2 .
Minutes from workshops	Textual (.doc, .docx) Tabular (.xls, .xlsx)	Small (<1GB)	IDSA	Workshop Report, Pictures & Slides - TRUSTS (trusts-data.eu)
Survey results conducted for the research across stakeholders	Textual (.doc, .docx) Tabular (.xls, .xlsx)	Small (<1GB)	IDSA	Survey results conducted for the research across stakeholders was a part of the Task 7.2 D7.3-Communities-Engagement-Strategy_June2021.pdf (trusts-data.eu).
Data from Use Cases by NOVA & EBOS, who will specify dataset properties (Task 4.3)	Textual (.docx,) Tabular (.xlsx, .csv) Code (.xml or .json)	Small (<1GB)	RSA	No, datasets do not belong to RSA.
Metadata of dataset from external datamarkets and EOSC initiatives	Code (.json, data from REST APIs)	Large (~ 1GB)	RSA	Yes. Depending on the licence for the respective metadata, it will be made available from within the TRUSTS platform. Users of TRUSTS can search through the metadata to find datasets relevant for them.
Data in relation to the dissemination & communication activities	Bibliography of publications (.docx, .html, .xml) Publications & data (.pdf, .pdf/a, .docx, .xls, .csv) Text documents (.docx, .xls, .pdf) & photos (.jpg, .eps, .tiff) Website (.html, .css, .jpg)	Small (<1GB)	DIO	Mostly. Content to be published on TRUSTS website (https://www.trusts-data.eu) and other communication channels (as defined in D8.1).

	Usage statistics from website & social media (.xlsx, .csv)			
Anonymized customer relationship management (CRM) data	Tabular (.xls, .xlsx)	Small (<1GB)	NOVA, PB	Partly. The data provision will follow a GDPR compliant process.
Service request data & financial data for the need of trials	Tabular (.xls, .xlsx)	Small (<1GB)	NOVA, PB	No. The provided data will not be openly accessible since sensitive information is included in bank data regarding physical persons or legal entities. The data processing will follow a GDPR compliant process.
Global data sources of legal entities & physical persons	Textual (.docx,) Tabular (.xlsx, .csv) Code (.xml or .json)	Small (<1GB)	EBOS	Partly, EBOS acts as an open-public data provider and aggregator. The data processing will follow a GDPR compliant process. Other data will not be openly accessible due to sensitive information about physical persons or legal entities. EBOS in support of UC1 used 2 datasets in the scope of the project and WP5 trials in order to properly run the assets uploaded to the TRUSTS platform. The respective datasets (ie., bank transactions) can only be used with their respective application, the data is anonymised and will not be available beyond the project duration.
Code / scripts needed to facilitate project's implementation / development. No personal data.	Code (textual, .json, .py)	Small (<1GB)	LST	No. Data will be stored in a cloud-based environment for the infrastructure set-up and technical operations, using Google Cloud. Secure environment for developing and hosting the project's components, accessible through one secure point using SSH and HTTPS protocols.

Anonymized / masked data for financial & personal data: customer profile information & loans information for trials related to Use Case 3, WP5.	Textual (.docx,) Tabular (.csv, .xlsx)	Small (<1GB)	REL	No. This data will be combined with data from credit card transactions and customer activity. The data provision will follow a GDPR compliant process.
Project documents like documents, presentations and calculation tables	Textual (.docx) Tabular (.csv, .xlsx) Presentation (.ppt)	Small (<1GB)	G1	Yes, as deliverables of the project on the TRUSTS homepage (https://www.trusts-data.eu).
Project deliverables	Textual (.docx, .pdf)	Small (<1GB)	KUL	Yes, in the form of TRUSTS deliverables.
Overview of literature & other sources used for legal and ethical research (e.g. journal articles & conference papers)	Bibliography of publications (.docx, .html, .xml) Publications & data (.pdf, .pdf/a, .docx) Text documents	Small (<1GB)	KUL	Yes, in the form of TRUSTS deliverables. Publications used in the research are already in the public domain.
Descriptive metadata (abstracts, authors, publication tags, etc.)	Textual (.docx, .pdf)	Small (<1GB)	KUL	Same as above
Interview protocols and coding results for developing TRUSTS business models	Textual (.pdf)	Small (<1GB)	TUD	Yes: https://doi.org/10.4121/21103867.v1 , https://doi.org/10.4121/19762360.v1 and https://static-content.springer.com/esm/art%3A10.1007%2Fs12525-022-00547-x/MediaObjects/12525_2022_547_MOESM1_ESM.pdf
Descriptive results of cross-case analysis for meta-platforms exercising aggregator business models. This analysis is based on the secondary data available on the internet	Textual (.pdf)	Small (<1GB)	TUD	Yes, this will be included in the appendix of D7.2 "Sustainable business model for TRUSTS data marketplace II."
Summary of workshop results for exercising TRUSTS business models	Textual (.pdf)	Small (<1GB)	TUD	Yes, this will be included in the deliverable D7.2. "Sustainable business model for TRUSTS data marketplace II."
Online survey results for assessing TRUSTS business model impacts	Tabular (.csv, .xlsx)	Small (<1GB)	TUD	Yes, when we finish the data collection, we will upload it to https://data.4tu.nl/info/en/.

Updates on FAIR and data security

Twelve out of 17 project partners can report updates on FAIR and data security. The KUL publications relied on in the research for tasks T6., T6.3 and T6.4 are findable through KUL library repository. For accessibility a DOI is assigned to all publications used in the research. The data is interoperable because the data is in .doc or .pdf format and can be easily exchanged and processed. KUL states that data is reusable: All publications used in the research can be consulted and reused for research. Resources and Data Security are not affected because the publications do not contain sensitive data. All publications are stored in the KUL project repository linked to TRUSTS.

EBOS uses standard data formats .docx, .xlsx, .csv, .xml and .json to make their data findable. Concerning accessibility and reusability, EBOS input data is solely used in TRUSTS trials (WP5) according to the company and UC1 processes. The analysis is performed (anonymised format) within EBOS premises along with data onboarding mechanisms / interfaces deployed by TRUSTS. The outcome of the analysis will only be visible to EBOS responsible employees and the anonymised models through the TRUSTS platform only for the trials purposes. EBOS UC1 data (two datasets supporting the two assets) is not shared between partners. Some downloadable datasets can be accessed through the TRUSTS platform (MVPv1) via the UC partners while performing UC trials, all anonymised and in a non understandable format. Regarding resources and data security EBOS states that data is stored in a secured cloud server provided by EBOS.

For KNOW, TUD and DIO the status remains the same as in M24. NOVA, REL and FORTH have no updates to report. FAIR and data security is not applicable for FhG, RSA, G1 and IDSA because they are not dealing with content-related data on plattform. LST states that no data and therefore no personal information is collected.

Report on actual data(sets) which were made available

Five out of 17 partners have made actual datasets available on TRUSTS website and elsewhere. IDSA published an interview with Alexandra Garatzogianni on the TRUSTS website, has sent out a newsletter on Reflections February and posted the hashtag #DataSpacesTuesday on LinkedIn and Twitter. The first press release about *TRUSTS in the Community: Standardization, Engagement, and Impact* is accessible on the TRUSTS website. This event is a live interview with Dr. Silvia Castellvi which was podcasted on YouTube and spread via Twitter and LinkedIn. Furthermore, IDSA announced a webinar on data sharing and the workshop *Data Spaces & Semantic Interoperability* on Twitter and called for participation and position papers on social media (LinkedIn and Twitter). The workshop report with pictures and slides can be found on the TRUSTS website.

EBOS has shared internally a dataset for AML RiSC application and one for AML TRM application in the TRUSTS repository. Both datasets were used in the scope of the project supporting WP5 trials (UC1) and will not be available beyond the project duration. Even though all partners that have access to the TRUSTS platform can download and access it, data is anonymized and cannot be reproduced or used only but only with the respective application requirements. EBOS input data is solely used in TRUSTS trials (WP5) according to the company and UC1 processes and the analysis is performed (anonymized format) within EBOS premises along with data onboarding mechanisms / interfaces deployed by TRUSTS. The outcome of the analysis will only be visible to EBOS responsible employees and the anonymized models through the TRUSTS platform only for the trials purposes. EBOS UC1 data (2 datasets supporting the 2 assets) is not shared between partners. Some downloadable datasets can be accessed through the TRUSTS platform (MVPv1) via the UC partners while performing UC trials, all anonymized and in a non understandable format. The dataset *AML*

Screening (RDC database) is accessible internally in the TRUSTS repository, too. AML Screening service is embedded and receives results from the open-source RDC database and was used in the scope of the project supporting WP5 trials (UC1) and will not be available beyond the project duration. This is occurring only when a user uses the specific service. Within the project only EBOS did.

KNOW has published three datasets on Zenodo: MetaMF user group data, FairRecSys datasets and OpenML dataset for data marketplace recommendation. The first two datasets were used for two Springer publications of the scientific events ECIR 2021 and BIAS 2022. The last one was reported in deliverables D3.12 and D3.13.

LUH in cooperation with DIO has published several news items on the TRUSTS website in the news section. All pieces can be accessed there (includes also news pieces not written by LUH). Examples are the participation in EU Industry Days 2022, European Research & Innovation Days 2022, and European Sustainable Energy Week 2022. While LUH was writing these news pieces, DIO as WPL for Communication & Dissemination, published it on the website.

TUD published research data on the repository 4TU.Research Data with a DOI. The first one is named *Toward Business Models for a Meta Platform: Exploring Value Creation in the Case of Data Marketplace* and the second *Preparing Future Business Data Sharing via a Meta-Platform for Data Marketplaces: Exploring Antecedents and Consequences of Data Sovereignty*. Both datasets are related with deliverable D7.2 and the related papers are published on ResearchGate. The last dataset *Appendices – Business model archetypes for data marketplaces in the automotive industry* is related to deliverable D7.1 and the related paper can be also found on ResearchGate.

All mentioned datasets are publicly accessible, except the datasets from EBOS for the reasons stated above. Only the datasets of KNOW and TUD were provided with DOIs. Posts on Social Media usually do not have PIDs. All other participants have not published any data.

6 Conclusion

Looking back at the third and final year (2022: M25-M36) of the project, the overall project progressed as anticipated. In terms of **WP1** the preparation and planning of the 22 remaining deliverables out of 70 deliverables was planned and quality measures were implemented. Minor deviations occurred which will be reported on in the final reporting, in terms of the final review. Aside from the many daily project management tasks, the coordination team facilitated many formats of exchange between partners including eight Project Management Board Telcos, one WP1 (Executive Board) telco, two plenary meetings (one online and one onsite), as well as some extraordinary telcos with relevant partners. Beyond that the coordinator represented the project in several events onsite and online, thus engaging external stakeholders with the project.

WP2 concluded at the end of the second year. Some final activities including the second technological validation, the third business validation and the finalisation of the update and evolution of the trials evaluation testing methodology were performed under WP5 aside from other contributions in WP3.

In terms of **WP3** the infrastructure has been set up for TRUSTS to support the development and provide a test environment, which will be available after the end of the project. Relevant documentation and information in order for other interested parties to set up such an infrastructure are provided as well. Conceptual and technical foundations for setting up smart contract infrastructure as well as a demonstrator, which showcases how more conventional payment systems can be used in tandem with smart contracts was developed, which is intended to be further used and explored by DELL EMC after the project. Furthermore, interoperability solutions were researched and developed to connect data spaces to EOSC initiatives, namely OpenAIRE and Europeana The results are intended to be used for future work and research by RSA. Furthermore the metadata and semantic layer of the platform moved into the implementation and validation phase and new software components including the IDS extension for CKAN, the TRUSTS client library and the vocabulary extension for CKAN have been developed. Using existing open source components many features of a secure federated data sharing platform have been enabled. The TRUSTS recommender system was evaluated using the OpenML data and service sharing platform, the resulting dataset was shared with the research community. The recommender system was fully integrated into the IDS-based infrastructure of the TRUSTS platform, leading to the development of 15 services. Furthermore five scientific publications have been produced in terms of T3.6.

The tasks T4.1 and T4.2 in **WP4** were finalised in M18 and their outcomes have been reported in D4.1. The outcomes mainly centred on the investigation of Cryptographic primitives involved in building collaborative trust systems, including Fully homomorphic encryption (FHE), Secure multi-party computation, Private Set Intersection (PSI), Homomorphic Encryption versus Multi-Party Computation. During the second half of the project, the focus shifted to corresponding anonymization methods. An application was created that combines both - risk analysis and anonymisation, partly building upon the results of the Safe-DEED project (Bampoulidis, 2020a). Corresponding anonymisation methods were identified and implemented based on the results of the risk analysis. Furthermore the application architecture was updated and enhanced with a new anonymisation component. The visualisation of the platform was adjusted to be more appealing and informative taking into account expert feedback for the UI. In addition to this, methods for the anonymisation of data types have been identified. Furthermore different federated learning models have been investigated, applied and after an evaluation implemented, resulting in enhanced security mechanisms.

WP5 focused on the preparation and execution of the second cycle of the TRUSTS demonstration while concluding on the lessons learned derived from the platform. For each UC one report was produced (UC1: D5.5, UC2: D5.7, UC3: D5.9).

In terms of **WP6** guidance and supervision was provided in order to ensure compliance with the legal and ethical framework. Through constant engagement with the consortium, the TRUSTS platform was assessed from a legal and ethical perspective in order to comply with legal and ethical standards, while acknowledging that due to the complexity there are in some circumstances more than one approach. A comprehensive analysis of the TRUSTS core technology as well as the UCs identified actions to be taken for compliance,multiple challenges as well as relevant legal frameworks to consider including the EU data protection framework, EU legal instruments governing digital markets and digital services, EU competition law, consumer protection framework and proposed legislation i.e. the Data Governance Act (DGA) as well as the AI Act.

For **WP7** the previous work of D7.1, which provided taxonomies of business models, was enhanced In terms of D7.2 to provide concrete options for business models through different tools and methods (e.g. business model canvas and stress testing). For the business models designed, two main scenarios were considered TRUSTS as a data marketplace and TRUSTS as a federator of data marketplaces. Via a large scale survey among several businesses the offerings of the platform were analysed. Furthermore recommendations for a potential future operator have been derived involving the pricing model, subsidisation to kick-start the platform, offerings, promotion and key technologies to focus on as well as different business model options. The project developed concepts and measures for Intellectual Property Rights (IPR) protection in data asset exchange through the TRUSTS platform. It started with a data stewardship concept for TRUSTS participants and conceptualised a threat analysis to counteract potential dangers for the platform during development and later operations. The project also developed concepts for addressing IPR issues within the TRUSTS partner consortium, focusing on IPR within the consortium, not on the IPR of the data exchanged on the TRUSTS platform. A concept was created to share costs and profits transparently and fairly among partners based on their efforts and contributions to the success of the TRUSTS platform. The focus was mainly on organisational and operational aspects of IPR protection for the TRUSTS operator and the internal IPR of the software used in the platform by consortium partners. A concept for a TRUST-DAO (Decentralised Autonomous Organization) model to manage services, software licences, and cost/revenue sharing within the TRUSTS operating company (OpCo) was developed. Additionally the prioritisation of standards and definition of current requirements for standards were produced and captured in D7.6. Further work includes the analysis of go to market strategies and SWOT analysis of TRUSTS captured in D7.8.

WP8 continued their efforts to promote the project as well as the project's results through different communication formats and channels (LinkedIn, YouTube, podcast, blog posts, webinars, workshops, etc.). Furthermore, for the final project year, some print materials were developed for onsite events, highlighting various learnings of the project. Furthermore the exchange with other projects (e.g. safe-DEED, i3-market, truzzt, Green Data Hub) was fostered so that they are able to build upon the learnings of TRUSTS. In addition to general events, eight workshops/webinars were hosted covering topics such as business models for data markets, legal aspects of federated data sharing, technical privacy preservation in federated data architectures, learnings from the TRUSTS use cases, etc. As part of the European Big Data Value Forum 2022 in Prague, TRUSTS shared insights and learnings from the project with other initiatives and stakeholders in terms of a 60 minutes panel discussion as well as on a dedicated booth. The work and major effort of WP9 has concluded in M15 (March, 2021). The consortium partners continued monitoring potential legal and ethical risks and communicated them to KUL, as the central contact point for ethics related questions.

This work is further solidified by our Scientific Lead, Technical Lead, Innovation Lead, Security Lead, Legal & Ethical Lead, Business and Exploitation Lead, as well as our Communication and Community Lead.

Within Year 2, TRUSTS increased its participation in the **scientific discourse** on topics such as trusted and secure data sharing platforms, privacy-aware analytics methods, ICT and Data skills, challenges for IT standardisation and more. Under the management of the Scientific Lead, the project increased its number of publications by seven, bringing the overall number of published research papers to nine. Ten more publications are planned for year 3.

The **Technical Lead** established consensus amongst technical project partners with regards to strategic questions in terms of architectural paradigm, the reuse of existing software and non-FR of strategic importance. Next steps include further iteration on architecture specification, if needed and the further refinement of the architecture.

The **Innovation Lead** implemented the innovation process, maintained the innovation registry and closely monitored and reported the innovation activities in terms of the Innovation Radar. Further steps include the finalisation of business and remuneration models and the further promotion of activities to increase commercialisation potential.

The **Security Lead** advanced the project's understanding of security issues and potential vulnerabilities. Next steps include the further implementation of security solutions especially with regard to GDPR, ethics and regulatory issues.

The **Legal & Ethical Lead** provided an overview of legal frameworks, identified potential obstacles and provided recommendations to overcome them. Next steps include further research and analysis of legal frameworks discussed in the EU such as the Data Governance Act, Digital Services Act and Digital Markets Act.

The **Business & Exploitation Lead** delivered the necessary groundwork for establishing a TRUSTS OpCo. Business Model and monetization strategy are in place, but nevertheless it was not possible to legally establish a TRUSTS OPCo during project duration. The necessary initial investment for establishing exceeded the consortia partners possibilities.

The **Communication and Community Lead** guided and expanded the outreach, focusing the communication efforts more on the project's progress and achievements. Strengthening ties with networks and programmes such as Safe-DEED, DOME4.0 or i3-market and engaging the SAB with the European Data community. The Business & Exploitation lead guided and coordinated the alignment among partners on important topics as per WP7 e.g. Lessons learned from DMA, Platform federation, TRUSTS business model, and the Datamarket platform operator, etc. Further work will focus on key questions pertaining the balance of IPR and commercial interests, the potential operation of an entity commercialising TRUSTS, attracting early adopters and more. Under the Communication and Community Lead the media mix was diversified and optimised in order to properly communicate the progress of the project, exceeding multiple KPIs. The focus of the communication shifted more towards communicating the tangible results of the project and in this regard a final event was organised with a 60 minute session as well as a booth for the project.