TRUSTS Technology

Equipping European Data Markets with Technological Innovations

Authors: **Ahmad Hemid, Ohad Arnon, Stefan Gindl, Alan Barnett, Victor Mireles-Chavez**

Review: **Benjamin Heitmann, Petr Knoth, Nina Popanton, Hannah Engel**

Whitepaper on the technological basis of TRUSTS – Trusted Secure Data Sharing Space

30 June 2021

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

Disclaimer

Copyright message

Authors: **Ahmad Hemid, Ohad Arnon, Stefan Gindl, Alan Barnett, Victor Mireles-Chavez**

Review: **Benjamin Heitmann, Petr Knoth, Nina Popanton, Hannah Engel**

Whitepaper on the technological basis of TRUSTS – Trusted Secure Data Sharing Space

30 June 2021

Table of Contents

Glossary of terms and abbreviations used

Abbreviation / Term	Description
TRUSTS	Trusted Secure Data Sharing Space
AML	Anti-Money-Laundering
MPC	Multi-Party Computation
EOSC	European Open Science Cloud
DMA	Data Market Austria
SOA	Service Oriented Architecture
UI	User Interface
SLA	Service Level Agreement
IDS	International Data Spaces
DaaS	Data as a Service
CKAN	Comprehensive Knowledge Archive Network
RoD	Registry of Data markets
FHE	Full Homomorphic Encryption
EDMI	EOSC Data Set Minimum Information
IDS-IM	IDS Information Model
DCAT	Data Catalogue Vocabulary
CLI	Command Line Interface
SSH	Secure Shell

0. Outline for this Whitepaper

TRUSTS - Trusted Secure Data Sharing Space - is an innovation action funded from the European Union's Horizon 2020 research and innovation programme under grant agreement Number 871481. The project's goal is to create a secure and trustworthy European data market for personal and industrial use by interconnecting different user groups and providing generic functionalities for innovative applications and services.

Our consortium consists of seventeen partners based in nine countries across Austria, Belgium, Cyprus, Germany, Greece, Israel, the Netherlands, Romania, and Spain. TRUSTS brings together technology providers, data providers, research institutions, and multipliers. The project runs from January 2020 to December 2022.

The aim of this whitepaper is to give the project stakeholders - i.e. data providers, data consumers, similar EU project consortiums, technology providers; in general the European Data Ecosystem - an overview of the technological basis of the future data market or data market federator. TRUSTS maintains an open communication policy and would like to share its own learnings from the project activities with all interested parties.

To provide a general overview of the technological developments in the project, this whitepaper explains which reference architectures TRUSTS builds on, how these have been further developed, and which innovations are necessary for the future, and thus for the achievement of the project proposal.

1. Introduction

With the increasing opportunities for use of data-driven approaches within industry as well as academia, there is an emerging need to find new solutions enabling the reuse of non-personal and personal data in the development of machine learning models powering a wide range of applications. For example, improving the Anti-Money-Laundering (AML) model or developing a new model in the medical field. Existing data markets do not support the trading of sensitive private data and sensitive data - at least not in a legal framework that supports European values. For the reason that such trading is obliged to preserve the privacy of the data, illegal data markets came into being where all sorts of data sets can be traded. Therefore, the need has arisen for a new data market that supports these capabilities in a legal framework that keeps data sovereignty as its highest imperative.

Supporting these capabilities requires a paradigm shift in data trading. Unlike existing data markets that trade data in a way where party A pays money to party B in exchange for transferring a plain text data file or a set of binary data to party A, TRUSTS is required to provide entities with the ability to collaborate on data analysis without compromising data and without disclosing data between the parties. These capabilities are enabled by using a number of approaches:

A. Use of advanced encryption such as homomorphic encryption and computational protocols such as Multi-Party Computation (MPC) that allow analysis of encrypted data without the ability to decrypt it.

B. Use of local computational methods such as federated learning or ensemble modeling, which allow models to be run on the data owner's servers and product sharing of the algorithm for joint analysis, without sharing sensitive private data between the parties.
C. Anonymization of the data prior to its transfer.

Using these methods requires TRUSTS to provide the ability to trade in services (data encryption and sharing) and applications (e.g. trained models) in addition to the ability to trade in plain text data.

In this sense, the required collaboration with other data markets the following aspects are necessary to be fulfilled:

A. Interoperability with external data markets and the European Open Science Cloud (EOSC) Initiatives.
B. Access and Usage Control to Datasets and Services. E.g., when access to an asset is received, TRUSTS needs to have a component, which checks if there is a contract between provider and consumer for the specific asset, and if that contract is in a valid state.

1.1. Building Block One: Data Market Austria (DMA)

One of the two approaches on which the TRUSTS platform builds up is Data Market Austria (DMA). The DMA, started as a flagship project founded by the Austrian Federal Ministry of Transportation, Innovation and Technology (then BMVIT, now BMK). It was envisioned as a single point of entry to a federated network of data and data-service providers. It aimed at providing a user-friendly portal with a catalogue of data products through which organisations could see a list of available datasets, and then contact the respective provider to gain access to the infrastructure that hosts them or the data itself. The DMA project finished in August 2019.

The DMA was envisioned as a Service-Oriented-Architecture (SOA) with a distributed set of nodes hosting a variety of data products, and a central node hosting the metadata describing them and other support services. Each node was conceptually planned to consist of a set of containers serving a series of core components, which include access control, metadata harvesting, asset ingestion user interface (UI) and an Ethereum blockchain node. The central node fulfilled the role of several metadata management pipelines, along with a user authentication and access control service. Together, these services and an orchestrated exchange of information (e.g. IP-addresses and public keys for verifying authentication tokens) realised the distributed DMA architecture.

The reuse of the architecture is only conceptual and the TRUSTS team is putting resources in the implementation of components and service inspired by the DMA. Those components and accompanying requirements are listed in Table 1 below.

Table 1 - Requirements for reuse of DMA components

Requirements for reuse of DMA components and concepts	
AR 3.D.1	**Ability to operate as a distributed set of nodes.** The different providers and consumers of assets must remain capable of operating their own infrastructure in order to maintain data sovereignty. This infrastructure should be connected in a well-defined and easy to set-up manner in order to realize the business models.
AR 3.D.2	**Asset metadata distribution and aggregation.** Organisations should be able to offer existing assets on the platform. This requires mechanisms to ingest, map and distribute metadata about assets in a way that is searchable and actionable by the other participants of the platform.
AR 3.DMA.3	**Components must be easily deployable and connected.** The different nodes involved in the platform will each deploy a set of services. These can be developed or packaged by the platform operator, and they should be easily installable by every participating organisation.
AR 3.DMA.4	**Node infrastructure metadata accessible to all components in a node.** All components running in a node must have access to a single and up-to-date source of basic metadata about the node, such as name, identification numbers, as well as metadata about other components it interacts with.
AR 3.DMA.5	**Single source of truth for controlled vocabularies.** In order to adequately manage metadata coming from different organisations, some of which might have been created with distinct purposes in hand, it is necessary to have a set of controlled vocabularies that are centrally maintained and which can be used in mapping of metadata schemas and items.

The DMA model consisting of independent nodes and an additional central node has been conceptually inherited by the TRUSTS platform architecture presented in this document. On top of this, TRUSTS is adding

security-enhancing technologies that have been developed by the IDSA, as well as a series of new components developed specifically by the TRUSTS project. Four important architectural commonalities exist between the two projects:

A. Data providers federation: The notion of independent nodes that host the data products offered by the organisation.
B. Data products catalogue: The centralised metadata catalogue.
C. Knowledge Graph: A set of controlled vocabularies delivering a knowledge graph powering the application logic of the federated data market platform such as search and recommendation are powered.
D. Supporting corporate in-house as well as hosted environment: Third, the idea of a set of components being developed and distributed to different organisations so that each organisation can set up their own participating node by running instances of the provided components.

1.2. Building Block Two: International Data Spaces (IDS)

The second approach the TRUSTS platform is inspired by and builds on is the International Data Spaces (IDS). IDS provides a set of design principles and software components which data markets can be built on. The IDS is a decentralised software architecture for exchanging data in a sovereign, secure and interoperable way. Data sovereignty of data owners can be supported by certifying the actors that participate in a data space as well as the technical components they operate to exchange data and by technically controlling the usage of data on the data consumer's side according to metadata by which the data owner described data usage policies.

The IDS Reference Architecture Model is defined by the IDS Association (IDSA) and its 100+ member organisations. In a minimal IDS, participants exchange data peer-to-peer. They do so by operating a standardised communication interface called Trusted Connector. A meaningful data space that allows for multiple participants that neither know nor trust each other initially and that is open for additional participants to join requires further infrastructure called *essential services*. For convenience, further non-essential services enhance the functionality in a data space. The following Table 2 lists them all:

Table 2 – Essential and non-essential services for meaningful data space

Service	What is it?	Essential?
Certification body	Governance body empowered to grant IDSA certification for components and participants	Yes
Certification authority	Authority that is in charge of the certification to make sure that only compliant organisations are granted access to the trusted business ecosystem	Yes

Dynamic provisioning service	Management of certifications and metadata for all components and participants	Yes
Participant information system	Registry of certified participants that is accessible to all participants	Yes
Dynamic trust management	Governance body empowered to enforce basic security rules of IDS as a whole	Yes
IDS (metadata) brokers	IDS connectors will register descriptions of data endpoints with IDS brokers. This allows data consumers to find the data they need.	Yes
App store	Outlets providing data apps that can be deployed in IDS Connectors to execute tasks like transformation, aggregation or analytics on the data. Provided by IDS members, certified under IDS standards.	No
Vocabulary provider	Offer "vocabularies" such as ontologies, reference data models and metadata elements, which can be used to annotate and describe datasets.	No
Clearing houses	These intermediaries will provide clearing and settlement services for financial and data exchange transactions in the IDS.	No

Just as the commonalities outlined in the section above, several outstanding differences can be identified between the two, which are introduced by the usage of software components from the International Data Spaces (IDS). On the one hand, the communication protocol between the different nodes is replaced in TRUSTS by the IDSCPv2 protocol, which incorporates an additional layer of security and trust by the use of cryptographic certificates and third party attestation. On the other, TRUSTS introduces the notion of a portable application, which in turn necessitates a more adaptable routing mechanism within each node. In the DMA, routing is configured in a reverse proxy configuration, which only requires alterations when a new core component is installed. This contrasts with the TRUSTS routing mechanism, which allows dynamically for services to appear, disappear or change names within a node. Finally, the TRUSTS platform envisions a federated user information system, distributed across all the nodes.

1.3. The outcome: TRUSTS, data market and data markets federator

We envision TRUSTS as an IDS-compatible data markets federator. TRUSTS should support and implement at least the essential services, as listed above. The technical services for dynamic provisioning, participant information and (metadata) brokerage are being adopted and will be piloted in turn within the TRUSTS use cases. By the end of the TRUSTS project, operating organisations that will, among others, take care of certification and trust management will be identified.

The following architecture requirements are inherited by the TRUSTS architecture from the IDS (Table 3):

Table 3 - Requirements for future alignment with IDS

Requirements for future alignment with IDS	
AR 3.I.1	**Essential services (technical):** Services for dynamic provisioning, participant information and (metadata) brokerage shall be put into operation.
AR 3.I.2	**IDS Connectors:** All participants required for demonstrating the TRUSTS use cases shall be equipped with IDS Connectors and should be able to expose their data offerings through these connectors' interfaces, including self-describing metadata in terms of the IDS Information Model.
AR 3.I.3	**Essential services (operational):** Organisations that provide the essential services of certification (i.e., certification body and certification authority) shall be identified. A body in charge of dynamic trust management shall be established.

2. Federated technology for the future

2.1. Industry Requirements for a data market federator

The architecture of the TRUSTS platform has to accommodate the requirements and priorities of a wide range of stakeholders. In order to accomplish this, requirements have been collected from two groups of stakeholders within the project. The first set of requirements are the functional requirements (FRs), which were be collected mainly from the nontechnical participants of the project and therefore not outlined in this whitepaper due to its focus on technology within the project. Additional information can be found here.

Table 4 - Industry Requirements

Industry Requirements	
FR1	**Data required by the industry** • All relevant Open Data as a basis • All types of data may be supported e.g. streams, static data, etc.
FR2	**Data usage processes and services** • Data as a Service (DaaS) • It should be possible to browse and explore data and services openly, but when it comes to the commercial case, data and services may have to be exchanged point-to-point. Additionally, this data should also be protected from unauthorized duplication. • Sometimes long-term-preservation of product (-performance) data is key to ensure quality, meet regulations and show long-term stability. In case the data marketplace deals with such data, standards for long-term-preservation have to be met and guaranteed. • User interface has to follow business logic on the first level (browse) and then be detailed for data experts. • Rooms for developing and testing data driven business ideas are important. Often such rooms will be the only place where all facilities (indicatively cloud, data, processing, IP, algorithm development, etc.) are present to get data products developed.

FR3	**Services required by the industry** • Matchmaking services which act as bridge builder for other domains, in recruiting, to research. • Data aggregation / anonymizing services, which allow to process personalized data. Such a service may be run by a special trustee, who guarantees conformity with privacy regulations. • A strong metadata layer as a basis for quality and interoperability. • Blockchain technology can constitute a prominent candidate for ensuring information transactions integrity.
FR4	**Operational quality required by the industry** • Transaction based billing models • Guaranteed quality and legal certainty for the trade • Standardized Service-level-agreement (SLA). • A mechanism that ensures that only “serious vendors” trade on the data marketplace. • The trust in the data and services provided may be strengthened by a certification process of providers and/or concrete dataset or service provision. • Support in acquiring and marketing by the data marketplace
FR5	**Business model requirements** • Operational commencement should be done with core functions and core data and services instead of a “very broad and potentially unclear approach" in order to ensure focus and comprehension. • The mission as a commercial project should be made clear from the very beginning. The idea of a commercial marketplace should be placed in front of the appearance. • Clear statements on the business model and ownership of data marketplace convey trust into the superstructure.

An additional set are the architectural requirements (ARs). They were collected from the technical participants of the project, and are grouped by the different areas of concern for the TRUSTS architecture.

These areas of concern are as follows:

- Architecture requirements from alignment with Data Market Austria (DMA) components
- Architecture requirements from alignment with International Data Spaces (IDS) components

- Architecture requirements from future alignment with Gaia-X
- Architecture requirements related to smart contracts
- Architecture requirements related to interoperability of data marketplaces
- Architecture requirements related to data governance
- Architecture requirements related to platform development and integration
- Architecture requirements related to brokerage and profiles for users and corporates
- Architecture requirements related to privacy enhancing technologies
- Architecture requirements related to anonymization and de-anonymization
- Architecture requirements following from the usage of Comprehensive Knowledge Archive Network (CKAN) software

2.2. Privacy Preservation

Due to different breakthroughs in recent years and the development of new machine learning and cryptographic approaches the often-illustrated problem that one has to give up privacy if you want to do data analytics is not true anymore. Several methods allow for more privacy, ranging from transfer or federated machine learning to cryptographic primitives like homomorphic encryption or multi-party computation. The corresponding security guarantees depend on the respective method, usually one has to find the use case related trade-off between security and performance or usability. In this section we introduce the most promising approaches in connection with data sharing spaces while discuss their advantages with respect to TRUSTS.

In general, one of the main advantages of homomorphic encryption is the ability to outsource computation without giving up any privacy. Sensitive data can be homomorphically evaluated on a data platform or cloud and only the data owners can decrypt the computed results. Suppose one wants to benefit from the evaluation of a machine-learning model from a service provider, but does not want to share her data with anyone outside her company. Setting up an FHE framework will allow her to do this without having to trust the service provider, since they are not able to access the actual content of her data.

Secure multi-party computation is a subfield of cryptography that enables privacy-preserving computations between multiple participants. It first appeared in computer science literature around 1980. In recent years, secure multi-party computation has become practical due to extensive ongoing research and exponential growth in computing power. Every traditional computation involving two or more participants can be made privacy preserving through secure multi-party computation. However, this transformation's computational overhead varies depending on the underlying computation and sometimes can be prohibitive. To illustrate the privacy and confidentiality guarantees offered by secure multi-party computation, we consider the case of anti-money laundering. As with most anti-fraud activities, anti-money laundering benefits from collaboration. However, financial institutions are reluctant to share data because of competition and data privacy regulations.

Private set intersection is a special-purpose secure multi-party computation. It allows two participants to compute the intersection of their data sets. Thereby, neither participant learns information from the

protocol execution, except for the data entries in the intersection. For instance, private set intersection enables two companies to find out common customers privately - information that can subsequently be used for a joint advertising campaign. Private set intersection is the most mature secure multi-party protocol, and computational overhead is small. Therefore, when parties engage in a private set intersection protocol, they do not have to expect significant performance issues.

2.3. Interoperability

Interoperability with external data markets is a key design principle. It enables TRUSTS to act as a **data markets federator**. We see a data market federator as an entity that can ingest data products (i.e. datasets, data services and applications) from other external data markets, enabling their trading within the TRUSTS platform and its wider ecosystem. Similarly, a data market federator should be able to expose information about its data products to other data markets.

Our interoperability work strives to create the guidelines, interfaces and standards to connect TRUSTS with **third party data markets** and **EOSC** initiatives. TRUSTS accomplishes the above using the following three components:

- The **Registry of Data markets (RoD)**
- The **Data Exchange TRUSTS component**
- The **Data Exchange client component**

The Registry of Data markets (RoD) lists existing third party data markets and relevant initiatives of EOSC. It is essential for the mapping and creation of a harmonised community of data markets and a precondition for standardising the operations of data markets. It works as an address book routing the communication between the Data Exchange TRUSTS component and the Data Exchange Client component. The Data Exchange TRUSTS component will be deployed in TRUSTS nodes to ingest as well as expose information about data products from third-party data providers and into the TRUSTS catalogue. It can either communicate directly with compliant external services using established protocols, such as OAI-PMH, or receive input from the Data Exchange Client component developed by TRUSTS and installed at a third party data market. It maps the external metadata schema into a format understood by TRUSTS. In the following, we describe the components in more detail.

Registry of Data markets

The RoD is a **catalog of relevant third party data markets**. It contains several types of information, e.g. basic information, such as company headquarters, scope and specialisation, as well as technical features. The data market properties listed in the RoD are mapped with a business-model based **taxonomy of datamarkets**[1] (see Figure 1). This taxonomy allows fine-grained categorisation of data markets by domain (e.g. financial), which is itself split into dimensions (e.g. “revenue model” or “pricing model” for the domain “financial”). Lastly, dimensions are in turn sub-divided into categories (e.g. “freemium” or “pay-per-use”

[1] van de Ven, M.R. (2020). Creating a Taxonomy of Business Models for Data Marketplaces. Master Thesis, TU Delft Technology, Policy and Management.

for the dimension “pricing model”). The RoD features **faceted-search** along these categorizations as well as a **full-text search** in text fields provided by data markets (e.g. title, description, etc.). After registering a data market in the RoD, the assets of the respective data market are ready for harvesting by the Data Exchange TRUSTS component.

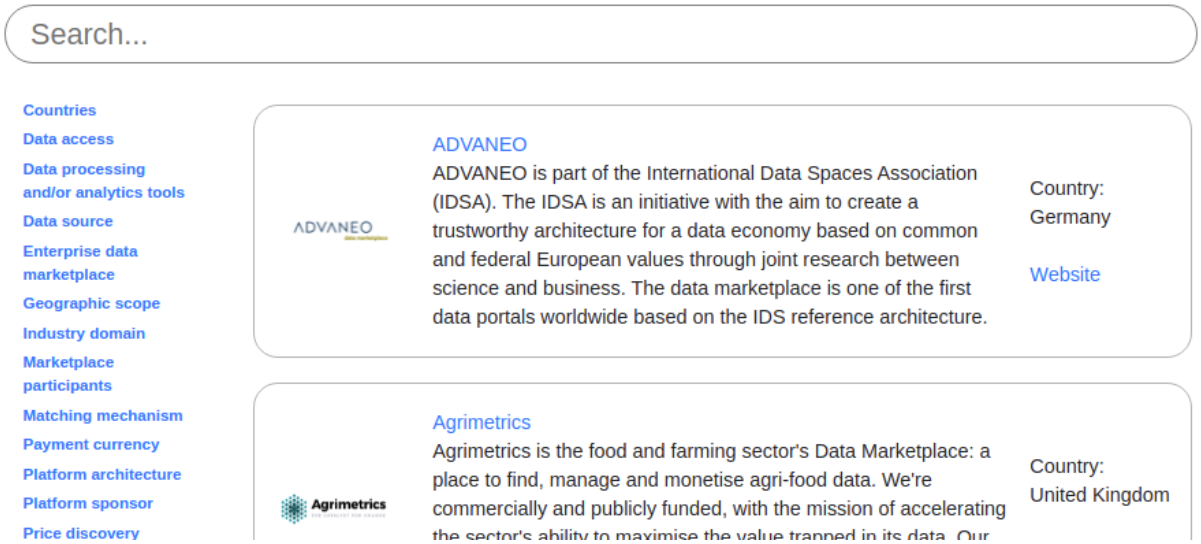

Figure 1 - Registry of Data markets (RoD)

The implementation of the RoD has been finished. Current work focuses on populating the registry with an initial critical mass of data markets. The RoD is open to any data market to use. The RoD is planned to exist beyond project lifetime and is supposed to help TRUSTS turn into a vibrant data ecosystem.

Data Exchange TRUSTS Component

This component resides within TRUSTS and harvests (EDMI compliant) metadata from external data markets and EOSC initiatives. Via its connection to the RoD it resolves their online location as well as their specified metadata characteristics. Harvesting is activated in predefined intervals and the respective data loaded into TRUSTS or updated. This component draws upon a metadata model compatible to both the needs of data markets while trying to ensure compatibility with relevant EOSC initiatives.

Data Exchange Client Component

This component resides on the premises of third-party data markets or EOSC initiatives. The interface exposed by it allows them to specify and transform their metadata into a format understood by TRUSTS. It communicates with the Data Exchange TRUSTS component, where the metadata specification is registered.

The Interoperability Metadata Model

The interoperability solution leverages a metadata model combining existing models: **IDS-IM**, a more extensive model established by the International Data Spaces Association[2] will get aligned with **EDMI**, the EOSC Datasets Minimum Information[3]. Additionally, similarity or open gaps with other established metadata models such as **DCAT**[4] are identified and analyzed. IDS-IM, through its extensiveness, is a solid backbone for interoperability with existing data markets and also from the commercial aspect. EDMI sets a focus on research and scientific data, thus providing the basis for interoperability with scientific initiatives such as EOSC. The merging of IDS-IM and EDMI was deemed necessary after an analysis showed that the IDS-IM cannot represent all required information.

Summarizing, interoperability in TRUSTS encompasses the establishment of a new metadata model as well as the implementation of additional components, i.e. the Registry of Data markets, the Data Exchange TRUSTS component, and the Data Exchange Client component.

3. Services and Improvements resulting from TRUSTS

The federated architecture of the TRUSTS platform provides the participants with several functionalities for the exchange of data, services and applications in manner that safeguards both the privacy of their data and their commercial interests. In particular, we highlight the following functionalities:

A. The ability to trade three types of assets: data, applications and access to services; directly from one participant to the other, without the possibility for third parties to eavesdrop, intercept of exfiltrate their data.
B. Holders of sensitive or private data can buy applications that are executed on their own premises and will process and extract value from it.
C. Creators of innovative processing technologies can offer them as services, thus guaranteeing that the source and machine code never leaves their premises.
D. Application and providers can offer their products in a way that can be billed according to usage, regardless of the computer infrastructure the product is deployed in.
E. All transactions are logged in a distributed, cryptographically signed, ledger to which both consumers and providers have access to, in order to verify compliance with contractual terms.
F. Optionally, every access operations to datasets, services or applications can also be logged in the distributed ledger and trigger events in smart contracts. The access mechanisms, in turn, consult the state of the smart contracts in order to grant or deny access, which means that contractual obligations can be automatically enforced.

[2] https://internationaldataspaces.org/, last accessed June 24, 2021

[3] https://eosc-edmi.github.io/, last accessed June 24, 2021

[4] https://www.w3.org/TR/vocab-dcat-2/, last accessed June 24, 2021

G. Organisations can easily integrate services and applications acquired through TRUSTS into their existing processes, since these are made accessible using industry standards and best practices. Thus, the integration efforts need not occupy themselves with contractual procedures.
H. The combination of the above allows for privacy-preserving computations to be performed, in which different parties make use of each other's data without compromising the privacy of the data subjects, or the rights of the data holders.

For providing these functionalities, a set of key technologies are leveraged. From the operation point of view, **cloud-computing technologies** allow for an easy deployment of the different nodes of the network, and the easy configuration of different components. These cloud technologies also allow for easy packaging, distribution and installation of applications. From the access control point of view, **the Trusted Connector** developed by the IDS plays a central role of gatekeeper to every access. In this capacity, it uses asymmetrical key encryption to guarantee identity of participants, and consults every access operation with the distributed ledger to ensure compatibility with contract clauses. Finally, it provides an extra layer of isolation and security that keeps existing services isolated from the rest of the TRUSTS platform. From the usability point of view, **machine learning based recommendation**, as well as **search mechanisms based on semantic technologies** are used to increase discoverability and reusability of assets, thus multiplying their value. From the contracting point of view, **blockchain based distributed ledgers and smart contracts** are exploited in order to provide participants with live and tamperproof records of transactions, as well as the above-mentioned access control. The exchange of information necessary to coordinate these different functionalities is realized by using a **Knowledge Graph**, where metadata about the platform and the assets traded therein is described according to well-specified ontologies and using controlled vocabularies. This enables consistent interpretation both among the platform components, as well as interoperability with existing components developed by platform participants and third party initiatives.

One relevant example: Smart Contracts

The Smart Contract Demonstrator is being developed within the TRUSTS project in order to provide the technical foundations and support needed to realise smart contract usage within the TRUSTS platform. This demonstrator consists of a Hyperledger Fabric blockchain instance used for standard purposes such as verifying transactions and providing a ledger, which can be queried later. The smart contracts, or as Hyperledger calls them 'chanicodes', are loaded onto the blockchain and run as blockchain applications; their subsequent operations are logged to the blockchain as transactions. The blockchain can be communicated with by several means; via CLI (locally or remotely over SSH), by REST API or using a NODE JS application.

A fully containerized set of services comprises the demonstrator system; these services include tools, an orderer and peers (blockchain nodes) needed for the Hyperledger Fabric blockchain. The containerized services that comprise the Hyperledger Explorer user interface are; the explorer application itself and an attached database. A simple architecture diagram of the Smart Contract Demonstrator can be seen in *figure 2.*

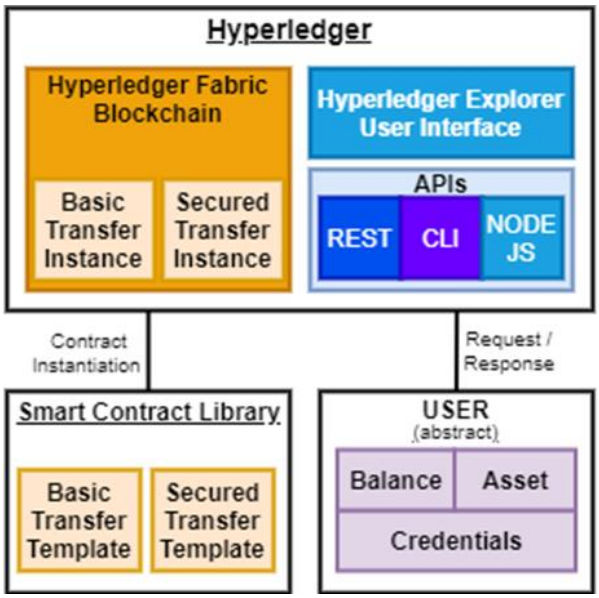

Figure 2 - Smart Contract Demonstrator

The demonstrator will not include an intrinsic payment system but will instead provide the ability to connect to an external payment system via API.

The Hyperledger Explorer web-application user-interface is integrated with the Hyperledger Fabric blockchain in order to enable viewing of on-chain data such as smart contracts, transactions performed, blocks on the chain and other associated data.

Presently the Smart Contract Demonstrator supports ledger query operations and asset transfer operations. The asset transfer smart contract is secured and authenticated - at the moment using SSH keys. The transfer operation requires agreement from the participants. Some controls are also included to mitigate fraudulent behavior, for example. If an owner of an asset sets a price and a purchaser attempts to procure the asset for less than the desired amount the transfer will not complete and the asset owner will receive a notification. Currently machine-generated SALT codes are being used as unique identifiers for this smart contract's operations.

The demonstrator will include a smart contract library; a set of smart contracts that address core operations needed by the TRUSTS platform, but are customizable in order to facilitate any partner who wishes to implement a modified version of a given smart contract or indeed create their own. Detailed documentation will also accompany the demonstrator to enable a seamless installation process for partners who wish to create their own instance.

4. Contact for further inquiries

Nina Popanton
Data Intelligence Offensive
TRUSTS Communication Lead
nina.popanton@dataintelligence.at
+43 664 20 45 965