TheFSM | The Food Safety Market

The Food Safety Market: An SME-powered industrial data platform to boost the competitiveness of European food certification

D3.1 – TheFSM Open Reference Architecture

DELIVERABLE NUMBER	D3.1
DELIVERABLE TITLE	TheFSM Open Reference Architecture
RESPONSIBLE AUTHOR	Danai Vergeti (UBITECH)

Co-funded by the Horizon 2020
Framework Programme of the European Union

GRANT AGREEMENT N.	871703
PROJECT ACRONYM	TheFSM
PROJECT FULL NAME	The Food Safety Market: An SME-powered industrial data platform to boost the competitiveness of European food certification
STARTING DATE (DUR.)	01/01/2020 (36 months)
ENDING DATE	31/12/2023
PROJECT WEBSITE	www.foodsafetymarket.eu
COORDINATOR	Nikos Manouselis
ADDRESS	110 Pentelis Str., Marousi, GR15126, Greece
REPLY TO	nikosm@agroknow.com
PHONE	+30 210 6897 905
EU PROJECT OFFICER	Stefano Bertolo
WORKPACKAGE N. | TITLE	WP3 | Platform
WORKPACKAGE LEADER	UBITECH
DELIVERABLE N. | TITLE	D3.1 – TheFSM Open Reference Architecture
RESPONSIBLE AUTHOR	Danai Vergeti (UBITECH)
REPLY TO	vergetid@ubitech.eu
DOCUMENT URL	
DATE OF DELIVERY (CONTRACTUAL)	31 October 2020 (M9)
DATE OF DELIVERY (SUBMITTED)	31 October 2020 (M9)
VERSION | STATUS	1.0 | Final
NATURE	Report (R)
DISSEMINATION LEVEL	Public (P)
AUTHORS (PARTNER)	Danai Vergeti (UBITECH), Iosif Angelidis (UBITECH), Dimitris Ntalaperas (UBITECH)
CONTRIBUTORS	Giannis Stoitsis (AGROKNOW), Svetla Boytcheva (SAI), Pavlin Gyurov (SAI), Branimir Rakic (PROSPEH), Tanja Matosevic (AGRIVI)
REVIEWER	Giannis Stoitsis (AGROKNOW)

VERSION	MODIFICATION(S)	DATE	AUTHOR(S)
0.1	Table of contents	1-Sep-2020	Danai Vergeti (UBITECH), Dimitris Ntalaperas (UBITECH)
0.3	Incorporation of use cases and user stories	25-Sep-20	Danai Vergeti (UBITECH), Iosif Angelidis (UBITECH), Dimitris Ntalaperas (UBITECH), Braminir Rakic (PROSPEH), Giannis Stoitsis (AGROKNOW), Tanja Matosevic (AGRIVI)
0.4	Requirements extraction (functional, non-functional, technical)	27-Sep-20	Danai Vergeti (UBITECH), Iosif Angelidis (UBITECH), Dimitris Ntalaperas (UBITECH)
0.5	Section 5.3.6.1	8-Oct-20	Iosif Angelidis (UBITECH)
0.6	Contributions to sections 5.2.4 and 5.2.5.2, 6	9-Oct-20	Braminir Rakic (PROSPEH)
0.7	Contributions to sections 5.2.3.3, 5.2.8.1, 5.2.8.2, 6	16-Oct-20	Giannis Stoitsis (AGROKNOW), Tanja Matosevic (AGRIVI)
0.8	Contributions to sections 5.2.1, 5.2.2, 5.2.3.1, 5.2.3.2, 5.2.3.4 6	23-Oct-20	Svetla Boytcheva (SAI), Pavlin Gyurov (SAI)
0.9	Minor corrections and contributions to all sections	26-Oct-20	Danai Vergeti (UBITECH), Iosif Angelidis (UBITECH)
0.95	Internal review	29-Oct-20	Giannis Stoitsis (AGROKNOW)
1.0	Final version	30-Oct-20	Danai Vergeti (UBITECH)

PARTNERS		CONTACT
Agroknow IKE (Agroknow, Greece)	Agroknow	Nikos Manouselis (Agroknow) nikosm@agroknow.com
SIRMA AI EAD (SAI, Bulgaria)	ontotext	Svetla Boytcheva (SAI) svetla.boytcheva@ontotext.com
GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS (UBITECH, Greece)	UBITECH ubiquitous solutions	Danai Vergeti (UBITECH) vergetid@ubitech.eu
AGRIVI DOO ZA PROIZVODNJU, TRGOVINU I USLUGE (Agrivi d.o.o., Croatia)	AGRIVI	Tanja Matosevic (Agrivi d.o.o.) tanja.matosevic@agrivi.com
PROSPEH, POSLOVNE STORITVE IN DIGITALNE RESITVE DOO (PROSPEH DOO, Slovenia)	tracelabs originstrail Core Developers	Ana Bevc (PROSPEH DOO) ana@origin-trail.com
UNIVERSITAT WIEN (UNIVIE, Austria)	universität wien	Elizabeth Steindl (UNIVIE) elisabeth.steindl@univie.ac.at
STICHTING WAGENINGEN RESEARCH (WFSR, Netherlands)	WAGENINGEN UNIVERSITY & RESEARCH	Yamine Bouzembrak (WFSR) yamine.bouzembrak@wur.nl
TUV- AUSTRIA ELLAS MONOPROSOPI ETAIREIA PERIORISMENIS EUTHYNIS (TUV AU HELLAS, Greece)	TŪV AUSTRIA HELLAS	Kostas Mavropoulos (TUV AU HELLAS) konstantinos.mavropoulos@tuv.at
TUV AUSTRIA ROMANIA SRL (TUV AU ROMANIA, Romania)	TŪV AUSTRIA ROMANIA	George Gheorghiou (TUV AU Romania) george.gheorghiu@tuv.at
VALORITALIA SOCIETA PER LA CERTIFICAZIONE DELLE QUALITA'E DELLE PRODUZIONI VITIVINICOLE ITALIANE SRL (VALORITALIA, Italy)	VALORITALIA	Francesca Romero (Valoritalia) francesca.romero@valoritalia.it
TUV AUSTRIA CERT GMBH (TUV AU CERT, Austria)	TŪV AUSTRIA	Stefan Hackel (TUV AU CERT) stefan.hackel@tuv.at

ACRONYMS LIST

A2C	Advantage Actor Critic
ABAC	Attribute-Based Access Controller
ABE	Attribute-Based Encryption
ACL	Access Control Lists
API	Application Programming Interface
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DID	Decentralized Identifiers
DLT	Distributed Ledger Technologies
DoA	Description of Action
DSS	Decsision Support System
EPCIS	Electronic Product Code Information Services
ERP	Enterprise Resource Planning
ETL	Extract, Transform, Load
FSQA	Food Safety and Quality Assurance
IaaS	Infrastructure-as-a-Service
IoT	Internet of Things
JSON	Javascript Object Notation
LOD	Linked Open Data
LSSS	Linear Sharing Secret Schemes
OASIS	Organization for the Advancement of Structured Information Standards
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
RBAC	Role-Based Access Control
RDBMS	Relational Database Management System
RDF	Resource Description Framework
SME	Small & Medium Enterprises
SOML	Semantic Object Model Language
SSE	Symmetric Searchable Encryption
TEE	Trusted Execution Environment
TheFSM	The Food Safety Market
UID	Unique Identifier
UML	Unified Modeling Language
WoT	Web of Things
XACML	eXtensible Access Control Markup Language

Executive summary

The purpose of the deliverable D3.1 “TheFSM Open Reference Architecture” is to deliver the user requirements and the technical requirements of TheFSM, as well as to deliver the first version of the conceptual architecture of the TheFSM platform. In order to define the user and technical requirements in a solid manner, requirements identification and elicitation approach is adopted that is based on Agile development methodology.

The adopted agile development methodology describes the agile processes, instruments, roles and methods that are adopted in all the phases of the development of TheFSM platform. This methodology defines User Stories definition with the appropriate guidelines and the additional information included within these User Stories. Moreover, it dictates the requirements definition in terms of key characteristics and requirements classification. Additionally, the TheFSM stakeholders and their interactions with the platform is clearly defined.

Following this methodology, the User Stories, that are stemming directly from the domain experts and end users partners of the project, are generated from D1.1 and contain a high-level description of the excepted behaviour of all sub-systems of the platform from the end-user perspective. Following the User Stories collection, the user requirements are extracted ensuring their compliance with the requirements characteristics defined in the methodology. The extracted user requirements are classified into the functional and the non-functional requirements of the platform and are utilised in the technical requirements definition that will drive the design and implementation of the platform.

A comprehensive analysis of the user requirements provided the concrete and solid technical requirements which are provided as input in the design and specification definition of the components that will be integrated in TheFSM platform. The list of elicited requirements constitutes the complete requirements backlog of the platform that will be maintained during the project implementation in order to guide all development tasks.

These technical requirements are thoroughly analysed in order to provide the first version of the conceptual architecture of TheFSM platform. This architecture is designed in a modular manner and is composed by a set of key components with distinct roles and scope towards the aim of providing the envisioned platform features and that address the stakeholders’ needs as expressed into the identified technical requirements. For each component, a comprehensive description of the design and functionalities is documented ensuring that it addresses a specific set of technical requirements from the list of the technical requirements.

The current deliverable presents the first version of TheFSM conceptual architecture, as well as the user and technical requirements. However, the design of the architecture is a living and iterative process that will last until M36 as per the Description of Action. Thus, D3.1 constitutes a living document that will include the updates that will be based on further identified functional requirements translated into technical requirements, originating mainly from the evaluation and feedback received from the pilot partners, and that will introduce updates and refinements in TheFSM architecture and will be presented in the upcoming versions of this deliverable.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Scope

The scope of D3.1 is to document the preliminary efforts undertaken within the context of Tasks T3.1 "Architecture and Specifications". The deliverable D3.1 focuses on the following objectives: (a) the identification of the user requirements (functional, non-functional) deriving from D1.1, using an agile methodology, (b) identification of the preliminary version of the technical requirements of TheFSM platform that will be used as the basis for the design of the components of the platform, and (c) to document the first version of the conceptual architecture of the platform and the detailed specifications of the components that will be integrated.

Towards this end, the current deliverable presents TheFSM conceptual architecture as this is defined through a solid iterative methodology which ensures the coverage of the end user needs, as they are defined in Wp1 (D1.1). More specifically, D3.1 presents the User Stories collection and prioritization as they are derived from the business requirements of D1.1. Further analysis on the user stories, as well as, the D1.2 Development Roadmap, the technical, data, legal requirements of D1.1 provided the functional, non-functional and technical requirements of the platform that will build the basis for the design and the specifications definition of all the components that will be integrated in TheFSM platform. The architecture is composed of a set of modular components and addresses the needs of all the different stakeholders of the platform as expressed into the identified technical requirements. More specifically, the technical requirements are translated into specific platform features that are grouped under the modular components of the platform. The architecture is designed in a modular manner that will enable the desired scalability, interoperability and extensibility, while also preserving a considerable degree of implementation-platform-independence. Additionally, the current document will provide the initial requirements backlog, containing the functional, the non-functional and the technical requirements backlog, that will be maintained during the project implementation in order to guide all development tasks. It should be noted that the identification and analysis of the functional and non-functional requirements, as well as their translation into technical requirements is living iterative process that will last until M36 according to the Description of Action and as the project evolves it will be constantly updated and documented in the upcoming versions of this deliverable.

1.2. Audience

D3.1 targets the consortium members of the TheFSM project and especially the technical partners which participate in WP2, WP3, WP4 with the scope to provide the conceptual architecture of TheFSM Data Platform which will set the basis and guide the development and the integration of TheFSM Platform. Additionally, an audience outside the consortium, with technical background (s/w engineers, developers, architects etc.) can also follow and understand the methodology, the technical requirements and the architecture of TheFSM Data Platform as it is presented in the current document.

Nevertheless, the document can be easily read by the non-technical partners of the consortium, since it also presents a solid iterative methodology which ensures the translation of the end user needs, as they are defined in Wp1 (D1.1) to technical requirements and the relevant architectural components.

1.3. Structure

The current document is structured as follows:

- Section 1: Introduces the deliverable by presenting its scope, the relevant audience, the document structure and the relation to other deliverables.
- Section 2: The requirements identification and elicitation methodology is defined. At first, the agile development methodology is presented, providing an overview of the adopted development processes, instruments, roles and methods and how they were adapted to TheFSM needs. Moreover, in this section the User Stories definition process is presented, its prioritizations, as well as the requirements and use cases definition process.
- Section 3: The elicited user requirements of TheFSM platform are documented in functional and non-functional. The mapping to relevant architectural components, as well as, the relevant use cases which identified the main data flows among the components are presented.

  Section 4: This section is dedicated to the technical requirements we extracted by following the thoroughly documented agile methodology.
- Section 5: TheFSM conceptual architecture is presented and described. The section presents the functional view of the architecture (the architectural elements that deliver the system's functionality), as well as, the dynamic view (focusing on runtime behavior). The different architectural and technological layers are presented. Moreover, the functionalities of each architectural component are presented, as well as, the interactions of the internal subcomponents providing the dynamic view of the architecture.
- Section 6: Provides an initial integration plan for TheFSM Platform
- Section 7: Concludes the deliverable. It outlines the main findings of the deliverable which will guide the future research and technological efforts of the consortium.
- Annex I: Lists the final User Stories
- Annex II: Lists the final User Stories – End Users Ranking
- Annex III: Lists the final User Stories – Technical Partners Ranking
- Annex IV: Lists the functional requirements
- Annex V: Lists the business requirements from D1.1 for quick reference

1.4. Relation to other deliverables

The current deliverable documents the preliminary efforts undertaken within the context of Tasks T3.1 “Architecture and Specifications”. The main input of D3.1 is D1.1 - Report on Requirements for TheFSM and D1.2 - TheFSM Development Roadmap. D3.1 analyses the outcomes of the end user requirements performed in T1.1-T1.4, as they are documented in D1.1 and by adopting an agile methodology produces the User Stories, the functional, non-functional, technical requirements and use cases as a backlog of TheFSM platform, as presented in sections 2 and 3. Finally, D1.2 is also used in the definition of an initial integration plan, as well as, the definition of the architectural components of the architecture. It is expected that the next versions of TheFSM architecture will also make use of the outcomes of WP5 and WP6 in order to evaluate the platform architecture and implementation, as well as, to enrich and update the use requirements backlog with additional requirements stemming out from TheFSM pilots and legal aspects.

2. METHODOLOGY

2.1. Working methodology

TheFSM conceptual architecture is the main artefact which will guide the technical development, the integration and the successful delivery of the TheFSM platform. TheFSM platform, besides addressing the technical challenges of an **industrial data platform**, needs also to address the needs of the stakeholders of TheFSM value chain. Towards this, the consortium adopted an agile methodology which ensures that the user requirements are taken under consideration in the architectural design and throughout the implementation. This paragraph describes the methods and the instruments of the standard agile methodology and their adaptations to the needs for the development of TheFSM platform.

One characteristic of the agile development is the assignment of activities to precise specified roles, as was defined by Cohn [1]:

- **Product Owner** : The viewpoint of the product owner is the perspective of the customer. The product owner translates the product related interest of the customer into a functional description – so called User Stories - which will feed into the development process. By assigning a priority to a functionality, the product owner determines the sequence of functions development. Finally, the product owner checks during an acceptance if the functional requirement has been implemented completely and correctly.
- **System Architect:** A System Architect is a developer with special skills. A system architect designs the system architecture to ensure among other things reliability, availability and maintainability of the product during the development process.
- **Developer:** A developer executes a development task to realize the functional request defined by the product owner.
- **Quality Assurance:** The Quality Assurance ensures during the development that newly implemented functions are working as specified and that the rest of the product works still faultlessly.

Figure-1 describes the core parts of all agile development processes in which the recurring execution of a defined sequence of process phases is presented. The following table describes the typical activities of each phase for the software development process.

Phases	**Participants**	**Actions Taken**
Plan	Product Owner System Architect Developer Quality Assurance	Define and specify user features for the next product increment. Features are described by User Stories. To prepare the acceptance of a User Story by the Product Owner, special test criteria have to be defined and specified by the whole team. Only if all of these criteria are fulfilled, the user story will be accepted by the Product Owner.

Design	System Architect Developer	As architects and developers.
Build	Developer Quality Assurance	The software will be developed by consideration of predefined test criteria
Test	Quality Assurance	The predefined test criteria will be translated into test cases. The test cases will be applied to the product increment.
Review	Customer Product Owner System Architect Developer Quality Assurance	The development team presents the new features of the product increment to the customer. The customer checks if the requirements are fulfilled completely. In case of required changes new User Stories will be defined

Table-1Phases, Roles and Activities in an Agile Software Development Process

These phases can be varied by the certain requirements of the project. Nevertheless, each iteration creates a product increment with available features defined in the planning, designed, built and verified in the following phases. The product increment is the input for the next iteration.

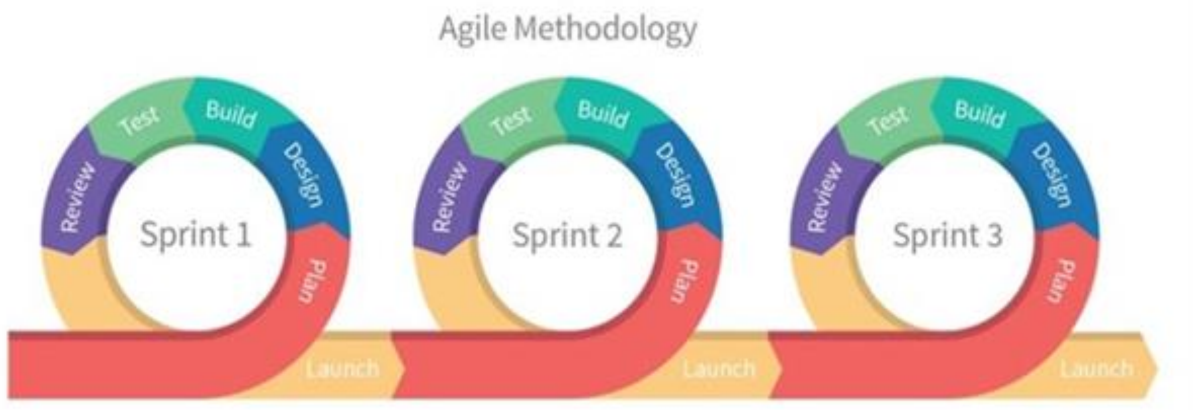


Figure-1 Sprint Based Agile Methodology (Source: http://www.illuminationworksllc.com/agile-enablement/)

The following picture (Figure-2) shows the agile development process in a more general manner. User feature requests for a new or the enhancement of an existing product are managed in a so-called backlog. For each iteration a set of these requests will be determined and brought into the development. The resulting release will be delivered to the stakeholders of the project, who will evaluate it and provide feedback. The TheFSM development process will embrace this process with the necessary adjustments to fit the needs of the project.

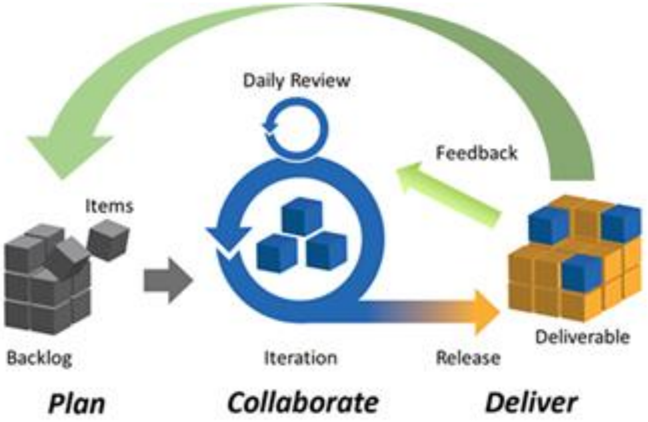


Figure-2 General Agile Development Process (Source: http://empireone.com.au/agile-iterative-lean-development-what-does-it-all-mean)

Backlog: The backlog manages user requested product features. In TheFSM, we will start with the collection of product features and translate them into the so called User Stories. Each User Story is constructed in a predefined schema, which is explained in section 2.2. A User Story contains a clearly separated product function that enables developers to give a rather good workload estimation. Finally, a priority is assigned to the User Stories. It will be used in the selection of User Stories for the next iteration and by the developer for the decision in which sequence the User Stories will be implemented.

Iteration: The iteration is the software development process for a predefined set of backlog items. Due to the earlier estimation and the knowledge about the capacity of the development team, a set of User Stories will be selected which fits into an iteration. Each User Story will run through the phases plan, design, build and test. Of particular importance during the development is the collaboration of all stakeholders in the process. Frequently, meetings between the relevant stakeholders of TheFSM are the chosen methodology.

Deliverables: At the end of each iteration an increment of the product is available for verification and validation conducted by the TheFSM pilots and stakeholders. This process step will create a first assessment of available product features which allow the acceptance or lead to a rejection or change request of the requirements as a first feedback to the development team.

According to the implementation efforts some changes can be implemented immediately, and others have to be translated to new User Stories and stored in the backlog again, waiting to be selected for a certain iteration.

The TheFSM agile method and the usage of User Stories, Requirements and Backlog allows a requirement engineering process as described in Figure-3.

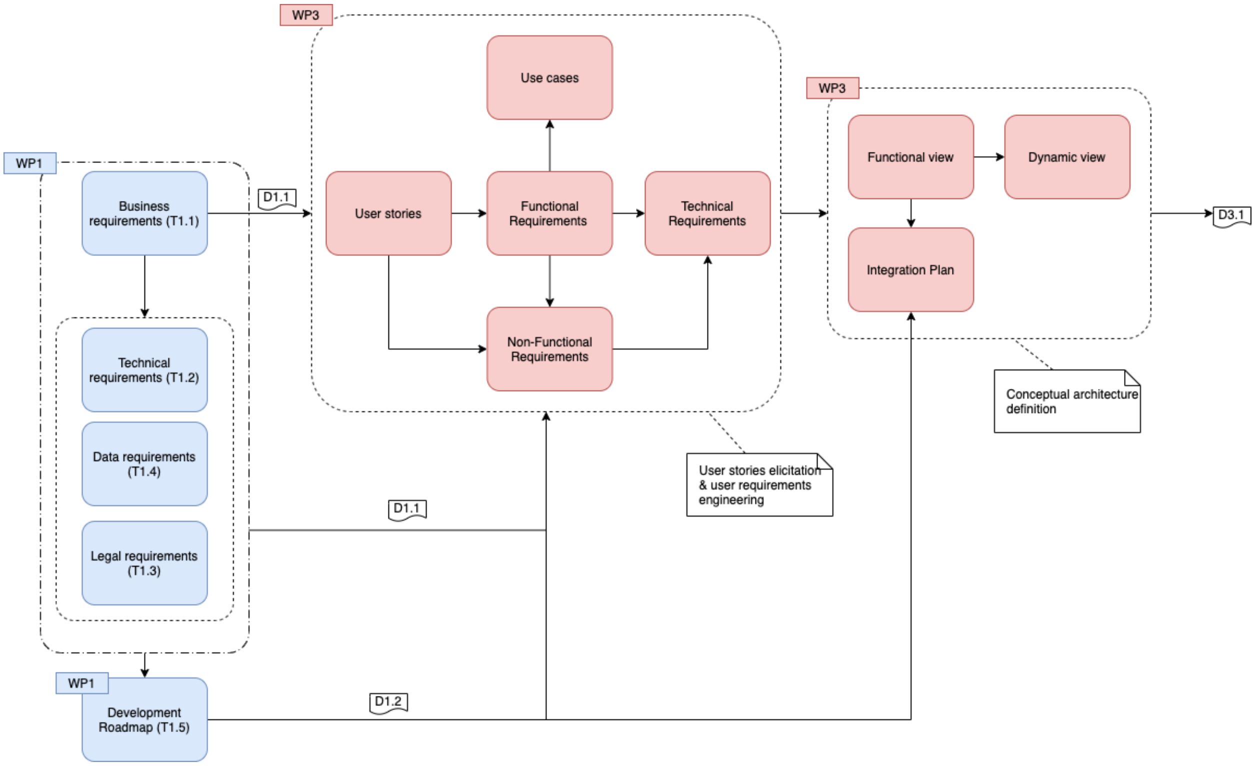

WP3
Use cases
WP3
Functional view
Dynamic view
WP1
Business requirements (T1.1)
D1.1
User stories
Functional Requirements
Technical Requirements
D3.1
Integration Plan
Non-Functional Requirements
Technical requirements (T1.2)
Conceptual architecture definition
Data requirements (T1.4)
User stories elicitation & user requirements engineering
D1.1
Legal requirements (T1.3)
WP1
Development Roadmap (T1.5)
D1.2

Figure-3 Requirements Engineering in TheFSM

The consortium adopted a collaborative and overlapping at workpackage level approach between WP1 and WP3. Initially, the **Business Requirements (T1.1)**, as well as, a subset of the **Technical Requirements (T1.2)**, the **Data Requirements (T1.4)** and **Legal Requirements (T1.3**) served as input to provide a natural set of **User stories**, when grouped together, in order to form specific scenarios covering all possible workflows. Additionally, all possible actors are defined.

The User Stories, as well as, the Business Requirements (T1.1), as well as, a subset of the Technical Requirements (T1.2), the Data Requirements (T1.4) and Legal Requirements (T1.3) serve as a valuable source of defining the **Use Cases**, the **Functional** and **Non-Functional** Requirements. The Use Cases group **common and complementary functional and non-functional requirements** and are used in order to define and understand the **data workflows** between the components. The **Technical Requirements** are derived directly from the last two. The technical requirements are **mapped to architectural components**, while, the Use Cases are used to identify the involved components and their interactions which enables the design of a **Functional Architecture** (T3.1). Based on the Functional Architecture, the Dynamic view is defined. The Functional Architecture in conjunction with the Development Roadmap (D1.2) provided the **Integration plan** which will guide the integration of the platform and its successful delivery. The aforementioned steps, will be repeated for all versions of the architecture.

The first version of the architecture is based on the analysis of the user requirements as they are defined in WP1. Regarding the user requirements, the next versions of the architecture will also take under consideration the pilot requirements (WP6), as well as, any additional updates regarding the legal requirements (WP5).

The following table assigns the agile instruments to the TheFSM adapted instruments, lists the activities and the responsible work packages and partners.

Agile Instrument	**Representation in TheFSM**	**Represented in WP by:**
Product Owner	The product owners are the partners responsible for building and extending the web applications in WP4. In TheFSM project, product owners are also considered the partners who are domain experts performing requirement analysis and pilots requirement analysis. Their input is the user requirements.	WP1, WP4, WP6: AGROKNOW, TUV, UNIVIE, WFSR, VALORITALIA, AGRIVI
System Architect, Developer	Represented in TheFSM by the partners who are designing and implementing the TheFSM platform and applications. Their activities are the derivation of technical requirements out of user requirements, the definition of User Stories and implementing the platform versions (M12, M24, M36).	WP2, WP3, WP4: SAI, UBITECH, PROSPEH, AGROKNOW, AGRIVI
Quality Assurance	Represented in TheFSM by the partners who are defining and performing the evaluation of the platform and the pilots	WP6: AGROKNOW, TUV, UNIVIE, WFSR, VALORITALIA, AGRIVI, UBITECH
Iterations	TheFSM platform versions (M12, M24, M36) including the applications versions (M12, M24, M36). After release, specific pilot scenarios will be applied to verify and validate each version by following the steps defined in the framework. Assigned User Stories will be checked and new or adapted requirements will be created	WP2, WP3, WP4: SAI, UBITECH, PROSPEH, AGROKNOW, AGRIVI

	and reported to WP1 and WP3, to be considered for the next release.	
User Stories	Defined by the partners who are domain experts performing requirement analysis, implementing pilots and using the platform features with help of the partners who are responsible for the implementation of all features and layers of TheFSM platform.	WP1 – WP6: AGROKNOW, TUV, UNIVIE, WFSR, VALORITALIA, AGRIVI (end user partners) SAI, UBITECH, PROSPEH, AGROKNOW, AGRIVI (technical partners)

Table-2 TheFSM agile process responsibilities

The procedures of User Stories, Functional, Non-Functional and Technical requirements definition are thoroughly described in the next sections, as well as the interactions between the project's stakeholders.

2.2. User stories definition

A User Story is an instrument used in Agile software development to capture a description of a software feature from an end-user perspective. The User Story describes the type of user, what they want and why. A User Story is very high level and helps to create a simplified description of a requirement.

Usually a User Story provides in one sentence enough information related to the described product feature, for which the development team can conduct a reasonable workload estimation. Furthermore, the User Story is used in planning meetings to enable the development team to design and implement the product features. A User Story typically owns a predefined structure:

As a <user-type (stakeholder)>, I want to <user-requirement> so that <reason>

Where each building block is defined as follows:

- As a <user-type (stakeholder)>: This is the type of the stakeholder of the story writing the user story.
- I want to <user-requirement>: the requested feature or functionality that will be included to the TheFSM platform.
- So that I can <reason>: a description of the benefit or the added value of the requested feature or functionality.

As aforementioned, the agile software development method allows the definition and adaption of User Stories during the whole project life cycle and the selection of them for implementation in the upcoming iteration. In TheFSM methodology, the User Stories are defined using the following information:

- **ID**: an unique identifier of the User Story.
- **Business Requirement ID**: a unique identifier linking the User Story with corresponding Business Requirement of D1.1.
- **Category**: is a generic term for grouping the required functionality. Categories generally represent a logical group of functions that exist within TheFSM and include functionality for the specific User Story and make use and extend the categories used in D1.2 TheFSM Development Roadmap.
- **Priority/value criteria**: a set of criteria in order to define the priority of each user story. They define the importance of the user story and usually how soon should this user story be included in the upcoming development iteration.

A sample of TheFSM user stories is provided below (Table-3).

ID	**Business requirement no**	**Category**	**User Story**		
			As a	**I want to <user>**	**So that**
US_1	BR_nr2_1	Analytics	Producer	Collect different data related to business characteristics and the final product	I can have a better view of products I am interested in / i can confirm (reveal) that my production process conforms with the certification requirements
US_2	BR_nr2_2	Analytics	Producer	Be able to manage and evaluate data from different heterogeneous sources	I can draw conclusions for analysis, legislative requirements, etc.
US_3	BR_nr2_3	Notifications	Producer	Be constantly updated about information shown to me	I can make valid decisions

Table-3 TheFSM user stories - Sample

The full list of the user Stories is provided in **ANNEX I.**

2.2.1. User stories prioritization in TheFSM

The identified User Stories will serve as **features** offered to the end-users and will have to be implemented from the development teams. While all of them add some value to the system, it might not be equally essential for the stakeholders. Thus, it is crucial to organise the user stories accordingly, for better development planning and delivery of all needed functionalities in time.

Nevertheless, another factor that has to be taken into consideration, is that a feature of little direct relevance to the end-users, might be **a prerequisite** for the proper function of the whole system and inevitably must be high in the prioritization list. Additionally, the **technical feasibility** is also of high importance for the successful delivery and prioritization. For the last two criteria, the technical side is responsible for deciding that. The applied prioritization process is based on the model proposed by Lant[1], which was adapted accordingly to fit our case. The Lant model introduces a two-dimensional approach to the user stories ranking, based on two assessment vectors (originally, time and business value). Following, the priority ranking value is the multiplication among the two factors of each user story and their final story ranking based on a priority range table.

Thus, in order for both, sometimes conflicting, perspectives on the features to be included, we defined two main assessment vectors: the end user side and the technical side. Two distinct voting processes were conducted, one by the end users and one by the technical partners, in order to accumulate the user stories values.

End-users ranking

The end users were requested to evaluate and rank the User Stories based on the two criteria:

- **Priority**: The priority (high, medium or low) defines the importance of the user story and usually how soon should this user story be included in the upcoming development iteration. As will be explained shortly, this has two dimensions, based on business maturity and time urgency.
- **Value**: The value (high, medium or low) defines the level of benefit or added value of the addition of the described feature or functionality to TheFSM platform from the point of view of the stakeholder.

In order to further investigate the priority in TheFSM, the consortium decided to define two sub-criteria: **business maturity/feasibility** and **time urgency**. The business maturity/feasibility expresses how feasible a story is from a business perspective, while the time urgency factor shows how soon the end users wish for the feature to be available. The end-users provided three possible values for each criteria: low, medium, high.

A sample of TheFSM user stories ranked by the end-users partners is provided below (Table-4). The full list of the user stories ranking from the end-users partners is provided in Annex II.

ID	AGROKNOW		
	Priority		Value
	business maturity/feasibility	time urgency	critical to business success/competitive advantage
US_1	Medium	Low	Low
US_2	Low	Low	Low
US_3	Low	Low	Low
US_4	Low	Low	Low
US_5	Low	Medium	Medium
US_6	Medium	Low	Medium

[1] https://michaellant.com/2010/05/21/how-to-easily-prioritize-your-agile-stories

Table-4 TheFSM user stories – End-users partners ranking - Sample

Technical partners ranking

Afterwards, we proceeded with the voting on the technical side. The technical partners were requested to rank the User Stories based on two assessment factors, which are both related to possible development constraints: the **technical feasibility** of a user story implementation and whether it is a **prerequisite** for other features of the platform. The guidelines as provided for the voting, are the following:

Feasibility	
Value	**Guidelines**
5	Extremely highly feasible
4	Highly feasible
3	Moderately feasible
2	Not easily feasible
1	Very difficult to be implemented

Table-5 Ranking Guidelines for Feasibility Factor

Prerequisite	
Value	**Guidelines**
5	Extreme level of dependency of other functionalities on this feature/ Most of other features are dependent on this feature
4	High level of dependency of other functionalities on this feature/ Many other features are dependent on this feature
3	Moderate level of dependency of other functionalities on this feature/ Moderate number of other features are dependent on this feature
2	Extreme level of dependency of other functionalities on this feature/ Few other features are dependent on this feature
1	This feature is not a prerequisite for other features

Table-6 Ranking Guidelines for Prerequisite Feature Factor

A sample of TheFSM user stories ranked by the technical partners is provided below (Table-7).

ID	**Agroknow**			**UBITECH**			**SAI**			**PROSPEH**			**Agrivi**			**Final**
	Feas	**Prer**	**Mean**	**Feas**	**Prer**	**Mean**	**Feas**	**Prer**	**Mean**	**Feas**	**Prer**	**Mean**	**Feas**	**Prer**	**Mean**	
US_1	2	4	3	2	3	3	5	1	3	4	3	4	3	3	3	**4**
US_2	3	4	4	3	4	4	5	1	3	4	3	4	3	4	4	**4**
US_3	3	4	4	3	4	4	2	4	3	3	4	4	3	4	4	**4**
US_4	3	3	3	3	3	3	4	2	3	4	2	3	3	4	4	**4**

Table-7 TheFSM user stories – Technical partners ranking - Sample

The full list of the user stories ranking from the technical partners is provided in ANNEX III.

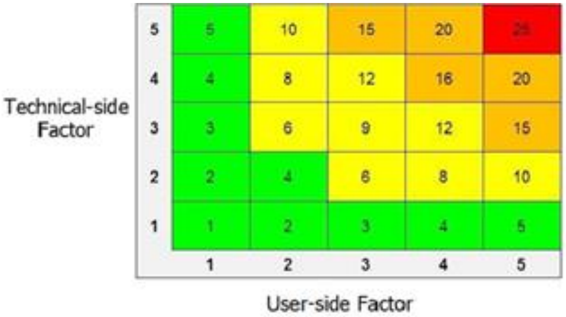
Final ranking

The final ranking is provided by the Lant prioritization guide which is adapted to the needs of TheFSM platform. More specifically, we processed the individual values for each user story and we proceeded with the extraction of the two main assessment vectors.

For the first vector (user-side): The user story ranking per end user partner was calculated as the mean value of the end-user value, time urgency and business feasibility. Subsequently, for every user story, the overall end-user ranking was calculated as the mean value of the individual end-user rankings. (In order to perform this calculations, the end-user values were converted to the Lant's values as follows: low = 1, medium = 3, high = 5).

For the second vector (technical-side): For each technical partner, the user story ranking was found as the mean value of the feasibility and the prerequisite factor. Afterwards, we calculated the overall technical ranking for every user story by finding the mean value of the individual technical rankings.

The last stage of this process contains the final assessment of the user stories by combining the two vectors. The Priority factor will be the product of the multiplication among the user-side and the technical-side factors and the ranking will be based on the following Figure-4:



5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Figure-4 Lant Prioritisation Guide

As shown in the figure, there are 4 areas – distinguished by different colors – dividing the prioritisation scale. At this stage of TheFSM platform design, the priorities assigned to the different user stories based on their ranking values can be translated as follows:

- 25: Critical & Highest Priority – to be included in the first 1-2 development sprints
- 15-20: Important to be implemented – to be included in the first round of sprints towards the 1st major release of the platform or in the initial sprints of the 2nd major release cycle
- 6-12: Moderately important – scheduled for later in order to be included in the sprints for the 2nd major release
- 1-5: Nice to have but low priority – to be scheduled at a later stage

Apparently, the highest total ranking value that a user story can get following Lant's model is 25, however due to the dual-dimensionality of the two main factors (end-user value and priority for the user side, feasibility and prerequisite for the technical side) and to the fact that the end users have different focus points and needs, it is expected that few or no user stories may achieve this maximum value. In any case user stories with a ranking value over 15 (within the orange range in the Figure) shall be considered as highly prioritised. The full Table of the User Stories final ranking is as follows:

ID	Vector value (end-user)	Vector value (technical)	Final ranking value
US_1	3	4	12
US_2	3	4	12
US_3	3	4	12
US_4	3	4	12
US_5	3	4	12
US_6	3	4	12
US_7	3	3	9
US_8	4	4	16
US_9	4	4	16
US_10	4	5	20
US_11	3	4	12
US_12	4	4	16
US_13	4	5	20
US_14	3	4	12
US_15	3	4	12
US_16	4	5	20
US_17	3	4	12
US_18	3	4	12
US_19	3	4	12
US_20	3	5	15
US_21	4	3	12
US_22	4	3	12
US_23	3	4	12
US_24	4	4	16
US_25	4	4	16
US_26	3	4	12
US_27	4	5	20
US_28	3	4	12
US_29	4	4	16
US_30	4	4	16
US_31	4	4	16
US_32	3	4	12
US_33	3	3	9

US_34	4	4	16
US_35	4	5	20
US_36	3	4	12
US_37	3	4	12
US_38	3	4	12
US_39	4	4	16
US_40	4	3	12
US_41	4	3	12
US_42	4	4	16
US_43	3	4	12
US_44	3	4	12
US_45	4	3	12
US_46	4	4	16
US_47	4	4	16
US_48	4	4	16
US_49	4	4	16
US_50	3	4	12
US_51	3	3	9

Figure-5 Final ranking and heatmap

2.3. Requirements definition

User Stories are a useful instrument to get well defined portions of system requirements in a language, users without technical background are able to use. User Stories are the input for the next action, where the technical partners are translating "user" requirements into more implementation-oriented requirements, which can be interpreted by system architects or developers.

Requirements do not have such a strong definition schema like User Stories but need to own a set of characteristics in order to be useful as an input for the design and development process, as proposed by Ericson [2]. These characteristics are listed in Table-8.

Characteristic	**Explanation**
Unitary (Cohesive)	The requirement addresses one and only one thing.
Complete	The requirement is fully stated in one place with no missing information.
Consistent	The requirement does not contradict any other requirement and is fully consistent with all authoritative external documentation.

Non-Conjugated (Atomic)	The requirement is atomic, i.e., it does not contain conjunctions. E.g., "The postal code field must validate American and Canadian postal codes" should be written as two separate requirements: (1) "The postal code field must validate American postal codes" and (2) "The postal code field must validate Canadian postal codes".
Traceable	The requirement meets all or part of a business need as stated by stakeholders and authoritatively documented.
Current	The requirement has not been made obsolete by the passage of time.
Unambiguous	The requirement is concisely stated without recourse to technical jargon, acronyms (unless defined elsewhere in the Requirements document), or other esoteric verbiage. It expresses objective facts, not subjective opinions. It is subject to one and only one interpretation. Vague subjects, adjectives, prepositions, verbs and subjective phrases are avoided. Negative statements and compound statements are avoided.
Specify Importance	Many requirements represent a stakeholder-defined characteristic the absence of which will result in a major or even fatal deficiency. Others represent features that may be implemented if time and budget permits. The requirement must specify a level of importance.
Verifiable	The implementation of the requirement can be determined through basic possible methods: inspection, demonstration, test (instrumented) or analysis (to include validated modeling & simulation).

Table-8 Requirements characteristics

The requirements can be classified in the two following main categories:

- **Functional**:

Functional requirement is the declaration of the intended functionality of a system and its components as reported by a hypothetical non-technical observer. The functional requirement is facilitating the development team to determine the expected behaviour or output of the system in the case of a certain input and in which a technical problem is addressed. Additionally, within the functional requirements the outputs of the envisioned product increment when receiving the described input is described. Depending on the degree of efficiency they can be split into “platform” and “pilot” oriented functional requirements.

- **Non-functional:**

As per ISO/IEC 25010:2011, the Non-functional requirements define system attributes such as security, reliability, performance, maintainability, scalability and usability. Also known as system qualities, they are just as critical as functional requirements, as they safeguard the usability and effectiveness of the entire system. Failing to meet any of them can result in systems that fail to satisfy business or markets or user needs, as explained in ScaledAgileFramework [3].

In some cases non-functional requirements cannot be resolved to one function or component or layer in the architecture. And in other cases, they cannot be tested directly. Nevertheless, they have to be kept in mind for choosing the right design and implementation of a system.

2.4. TheFSM Stakeholders and Interactions

Since TheFSM is an ambitious project, multiple stakeholders have been defined. However, a simple enumeration of them is far from sufficient, because of the complex interaction and multiple roles each stakeholder can have in different scenarios. In order to remedy this, multiple levels describing interactions have been defined.

The first classification refers to the actual taxonomy of the stakeholders based on the five user scenarios provided in D1.1. The User Stories and Use Cases define multiple stakeholder roles, but some are similar and generally refer to a higher-level role/stakeholder which can represent them all. To that end, the next table illustrates the proposed taxonomy of actors. The top level has all main stakeholders, while the next rows indicate secondary roles representing sub-classes derived from D1.1 and TheFSM pilots:

Stakeholder	**Subclasses derived from D1.1 and TheFSM pilots**
Certification Body	
Certification Scheme owners	
Public Authorities	
Inspector/auditor	
Lab expert	
Consultant	
Producer	*Growers, Farmers, Crop Traders, Winegrowers, Winemakers*
Food processor	*Bottler, Food processing company*
Supplier	
Distributor	
Retailer	

Table-9 Stakeholders taxonomy (as provided in D1.1).

(Bold indicates a primary stakeholder, while italics show a subclass)

Based on this classification, we define two stakeholder views. The first is the **Business View**, in which stakeholders are treated as parts of fundamental procedures in TheFSM value chain. The two main aspects in this classification are the **supply-chain procedures** (simply put, the entire process from food producing, processing, distribution etc. till it reaches the customer) and the **certification processes** (all steps required in order for a stakeholder to receive a certificate). Both aspects involve various stakeholders, however not all of them are equally vital to the procedures. This is addressed by further dividing the stakeholders participating in each aspect into primary and secondary (isPrimary column). Sub-categories of stakeholders are included here as well, for the sake of completeness.

Role	IsPrimary	Sub-roles	Description
Producer	Yes	Growers, Farmers, Crop traders, Winegrowers, Winemakers	Creates the product in raw form
Food processor	Yes	Bottlers, Food processing companies	Processes food to make it ready for consumption (e.g., bottler)
Supplier	Yes	-	Suppliers are at the top of the chain and give them products to distributors
Distributor	Yes	-	Distributors take products from suppliers and sell them to wholesalers and retailers
Retailer	Yes	-	Retailers get their products from wholesalers or from distributors
Consultant	No	-	Consultants offer advice to stakeholders for decision-making, during both supply chain and certification processes

Table-10 TheFSM stakeholders involved in supply-chain procedures

Role	IsPrimary	Description
Certification Body	Yes	Issues certifications and oversees supply chain for transparency
Certification Scheme owners	Yes	Issues certifications and oversees supply chain for transparency
Public Authorities	Yes	Supervises certification body and ensures its fair function
Inspector/auditor	Yes	Inspects and reports on findings via periodic checks of stakeholders upholding to standards
Lab expert	Yes	Conducts lab tests to issue certifications (with the permission of the certification body)
Consultant	No	Consultants offer advice to stakeholders for decision-making, during both supply chain and certification processes
Retailer	No	Retailers get their products from wholesalers or from distributors and produce their Private Label (PL) products from manufacturers

Table-11 TheFSM stakeholders involved in certification procedures

Finally, the second stakeholder view is from the **Data Market perspective**. In this view, we define the aspects each stakeholder should cover when participating in **data exchange**. Our study shows that all stakeholders are meant to have both **data producer** and **data consumer** stakeholders when exchanging data. This is derived from workflow coverage of all Use Cases which were defined throughout the above agile methodology. It also means that extra care must be taken when implementing the functionalities of the platform as the interaction graph is the most dense it can be. Additionally, the platform envisages the potential use of the exposed data services from **food tech companies** and other **ICT companies** which are interested to make use of the data of TheFSM platfrom and build on top of TheFSM data services additional added value services, which they could also be added into TheFSM platform. Thus, the following table of technological stakeholders is foreseen.

Role	**IsPrimary**	**Description**
Data consumer	Yes	All stakeholders mentioned above are data consumers in TheFSM Data platform
Data provider	Yes	All stakeholders mentioned above are data providers in TheFSM Data platform
External service providers	Yes	Developers and other ICT experts from the food tech domain and certification which to make use of the data of TheFSM platfrom and build on top of TheFSM data services additional added value services

Table-12 TheFSM Data market stakeholders

3. THEFSM USER REQUIREMENTS

In section 2.1 the TheFSM agile development methodology was presented. Within this methodology, all partners of the TheFSM project, especially the domain experts and end-users, were involved in the User Stories definition and prioritization following the instructions described in the previous section. In the current section we present the functional, non-functional requirements of TheFSM platform and the Use Cases.

3.1. Functional requirements

In the current section, we present the functional requirements of TheFSM platform as they are derived mainly from the business requirements of D1.1. For each functional requirement the following attributes are defined:

- **ID**: The unique identifier for each functional requirement.
- **Business scenario**: The relevant business scenario from D1.1 that the functional requirements refers to.
- **Business Requirement ID**: The relevant business requirement id that the functional requirement refers to. The list of the Business Requirements is provided in Annex XX.
- **Title**: A short description of the requirement.
- **Actors**: The stakeholders involved with the requirement. “All” indicates all stakeholders are involved.
- **Category**: An abstract thematic category expressing the relevant platform functionality that the requirement belongs to. The category is based and extends the category used in D1.2 Development Roadmap.

A sample table for the functional requirements is as follows. The full list is provided in ANNEX IV..

Reference ID	Business scenario	Business Requirement ID	Title	Actors	Category
FR_1	nr_1	BR_nr1_2, BR_nr1_1	Create user account	All	User account
FR_2	nr_1	BR_nr1_2, BR_nr1_1	Create company profile	All	Company profile
FR_3	nr_1	BR_nr1_2, BR_nr1_1	Upload certification info	Producer	Certification validation
FR_4	nr_1	BR_nr1_2, BR_nr1_1	Upload laboratory analysis test info	Producer	Certification validation
FR_5	nr_1	BR_nr1_2	Estimate risk	Retailer (FSQA expert)	Risk assessment

Table-13 TheFSM Functional Requirements - Sample

3.2. Non-functional requirements

In the current section, we present the non-functional requirements of TheFSM platform as they are derived mainly from the Business Requirements of D1.1. For each functional requirement the following attributes are defined:

- **ID**: The unique identifier for each non-functional requirement.
- **Relevant Requirement ID**: The relevant business/technical/data/legal/functional requirement id that the non-functional requirement is related
- **Title**: A short description of the requirement.
- **Category**: An abstract thematic category the requirement belongs to. The category is based and extends the category used in D1.2 Development Roadmap.

The final table for the non-functional requirements is as follows:

Reference ID	Title	Category
NFR_1	Personal data pseudonymization & GDPR compliance	Anonymization
NFR_2	Data access control based on attributes/ensure different authorisation access to different datasets	Access control
NFR_3	Representation & coverage of the food supply chain	Core functionality
NFR_4	FSM should provide monitoring capabilities.	Monitoring
NFR_5	FSM should ensure reliable communication with labs and IoT devices (API communication)	Integration
NFR_6	FSM should scale well and handle notifications about actions, events, schedules.	Scalability
NFR_7	FSM should provide feedback utilities between actors.	Notifications
NFR_8	FSM should provide a multi-filtered and advanced search engine. Actors should be able to search products based on specific parameters, which certification body is related to issuing certifications they need, etc.	Search engine
NFR_9	FSM should provide agreement support.	Collaboration
NFR_10	FSM should provide support for risk estimation.	Risk assessment
NFR_11	FSM should have a DSS component.	DSS
NFR_12	FSM should be able to showcase custom views per product (based on prices, compliances, certifications, etc.).	Search engine
NFR_13	FSM should provide advanced profiles for companies and stakeholders.	Data views
NFR_14	Search engine should have past history, monitoring and traceability capabilities.	Search engine, traceability, monitoring
NFR_15	FSM should integrate data from various sources and databases	Integration
NFR_16	FSM should log important operations and transactions	Logging
NFR_17	FSM should provide online forms for actors to fill in, when needed (e.g., auditing reports, lab results).	Digital data input
NFR_18	FSM should periodically check and automatically notify actors in cases of	Notifications

	legal compliance issues, or actions involving other actors.	
NFR_19	TheFSM should be able to verify the identity of the user/subject performing any operation	Verification
NFR_20	TheFSM should be able to able to trace all user/subject operations	Traceability
NFR_21	TheFSM should support an extended list of analytic algorithms on a mixture of confidential and public data in order to perform big data analytics	Analytics
NFR_22	TheFSM should be able to execute (big) data analytics in a timely and efficient manner	Performance, Analytics
NFR_23	TheFSM should be able to handle and store large datasets	Scalability
NFR_24	TheFSM should enable the interconnection and exchange of information with other platforms or devices with appropriate secure mechanisms	Integration
NFR_25	TheFSM should be able to support the functional and flexible operation in a distributed cloud infrastructure	Integration, Cloud infrastructure
NFR_26	TheFSM should be able to consume and handle different datasets in various formats (e.g. CSV, JSON, XML files)	Integration
NFR_27	TheFSM should be able to handle simultaneous requests on a timely and efficient manner	Scalability
NFR_28	TheFSM should provide the mechanisms to recover after system failure conditions	Recovery
NFR_29	TheFSM should have high availability	Availability
NFR_30	TheFSM platform should offer security and transparency regarding IPR management	Access control
NFR_31	TheFSM platform should offer a trusted way for data exchange agreements between two parties	Access control
NFR_32	TheFSM platform should support data representation using well established standards	Integration

Table-14 TheFSM Non-functional Requirements

3.3. Use cases

As mentioned in section 2.1, the Use Cases group common and complementary functional and non-functional requirements and are used in order to define and understand the data workflows between the components. The Technical Requirements are derived directly from the last two and are mapped to architectural components, while, the Use Cases are used to identify the involved components and their interactions which enables the design of the architecture. The technical partners identified nine (9) general use cases which cover the main data flows in the platform. Each use case was assigned with a responsible technical partner, based on the background and the role each has in the technical implementation of the platform. Each use case scenario was elaborated in three main iterations. Each use case template includes the following information:

- **UC ID**: Unique identifier for the user case.
- **Use Case Title**: Short title for the use case.
- **Related Functional Requirement(s)**: List of functional requirements which are related to the use case.
- **Description**: A short description of the use case, written in a story format.

- **Involved Stakeholders**: List of stakeholders involved for this user story.
- **TheFSM components involved**: List of TheFSM components involved.
- **Pre-conditions**: Preconditions assumed to be valid before the use case workflow can run.
- **Use Case Path**: The workflow path the use case undergoes to run. Simply put, a description of the TheFSM components running the scenario and their interactions.
- **Post Condition**: The result of the use case, the output.
- **Leading Partner**: The partner leading this use case.
- **Contributing Partners**: Contributing partners to the use case.

The nine Use Case scenarios are provided below.

UC ID	UC-1
Use Case Title	**Share stream data** (from farm, production and other phases of the product life cycle) of a specific product with public and/or specific stakeholders
Related Functional Requirement(s)	FR_13 - View IoT data (from farm, production) of a specific product FR_14 - Provide IoT data (from farm, production) of a specific product FR_26 - Access to retail-entered data (production plans, progress, practices, risks, deliveries) FR_27 - View real-time data related to cultivation conditions FR_28 - View additional data related to cultivation conditions
Description	**As a producer/manufacturer/food processing company** I want to feed relevant production stream and/or IoT data about a specific product/a batch of products into the system and be able to monetize it. **As a supplier** I want to feed relevant product storage stream and/or IoT data about a specific product/a batch of products into the system and be able to monetize it. **As a supplier** I want to get a report from the system with relevant IoT data from producers and processing companies about a specific product/a batch of products to check production and storage conditions with regards to food safety compliance. **As a FSQA expert** I want to get a report from the system with relevant combined IoT & retail data about a specific product or a batch of products to check production and storage conditions with regards to food safety compliance.
Involved Stakeholders	**Producers/Growers/Farmers** - providing IoT sensor data about the products they are producing **Manufacturers/Food Processing Companies** - providing IoT sensor data about the products they are manufacturing/processing **Suppliers** - providing IoT sensor data about the products they are selling to the retailer; reading IoT sensor data from food producers/processors about the products they are selling **Food Safety and Quality Assurance (FSQA) experts at retailers** - reading/analyzing IoT data provided by the suppliers and producers
TheFSM components involved	Data sources: ● IoT devices ● Farm management system ● ERP/WMS systems Security Layer: ● A2C components

	● E2E security components Data processing: ● Licence and agreement management ● Query explorer Data curation and Semantic enrichment ● Semantic mapper ● Secure storage & indexing Identity management & blockchain ● Decentralized identifiers & DIF Universal hub ● Transaction Validation Engine ● Underlying DLT Resource management: ● **Data flow management (data pipeline)** ● Message brokerage service ● Resource orchestrator Data brokerage model & engine ● Data brokerage model ● Data brokerage engine ● Micro-contracts auth ● Micro-contracts drafting, validation & execution engine
Pre-conditions	- IoT device data should be accessible either directly from the device or through a proxy service - Appropriate semantic mappers & standards need to be incorporated into the system to produce standardized semantic data - Product & batch identification should conform to industry standards such as GS1 ID Keys
Use Case Path	**User perspective:** End users (FSQA experts, retailers, producers etc) search for relevant data on the FSM by performing data queries using specific product batch identifiers or unique product identifiers. The queries are sent via a secure channel and the appropriate A2C system is in place. The FSM performs queries across the participating systems, of data indexed in their secure storage modules. Responses from the systems (identified by their DIDs) are handled by the query explorer and presented as Verifiable claims or data feeds. Each is verifiable by utilization of DLTs (using the DIF Identity hub, Universal Resolver and OriginTrail Verification mechanisms). A stack of contract management data brokerage modules allows for data monetization - purchase by the interested parties directly from data owners. **Data sourcing perspective:** Originating systems provide data through standardized interfaces into the FSM for mapping. Data is being ingested, prepared and parsed using a data flow manager (Apache Nifi or similar), while streams are being handled by the Message Broker service (Apache Kafka or similar). Relevant data is being timestamped, organized according to access policies and attributes, and wrapped into verifiable credential form for later proof verification (so that the data verifier can verify the data issuer identity and data integrity). The cryptographic data proofs and indexes are being stored in such a way that they can be queried by the FSM systems.

	Relevant resources utilized in the integration are managed by the resource orchestration module. Failures and errors are communicated to system administrators using a system specific messaging module.
Post Condition	The stakeholders are able to view and analyze cultivation, production and retail enriched data coming from IoT Devices and retail processes, by searching for and downloading relevant datasets, verifying their integrity to obtain actionable knowledge based on trusted data.
Leading Partner	Prospeh
Contributing Partners	-

Table-15 UC-1: Share stream data

UC ID	UC-2
Use Case Title	**Share traceability information** of a specific product (covering all the phases of the product life cycle) with the public and/or specific stakeholders
Related Functional Requirement(s)	FR_17 - Show product history based on traceability unit id (LOT number) FR_20 - View traceability history for cultivation FR_34 - Share measurement of the concentration (residues) of Plant Protection Substances in the final product FR_36 - Share data from all correlation stages with the food processor FR_37 - Share certificate history of a specific product FR_40 - Share directly production data related to the traceability units with processor FR_42 - Correlate the certification with tracking batches FR_54 - View/access farm data on the traceability of a particular batch from producer FR_55 - View/access product safety verification data from producer FR_56 - View/access food recall data from producer FR_57 - View/access retailer's requirements data from retailer FR_61 - Access to certificates generated in previous phases FR_64 - View supplementary product data FR_66 - Share final product safety verification data to retailer FR_67 - Share compliance data, which evidently reveal conformity of the packaging process against the requirements of the food safety standards (FSSC22000, IFS) to the certification body
Description	**As a producer/grower/farmer** I want to feed my own traceability information about a specific product/batch of products into the system. The information should also include all the certification and compliance data relevant for that product and its packaging. **As a manufacturer/food processing company** I want to feed my own traceability information about a specific product/batch of products into the system. The information should also include all the certification and compliance data relevant for that product and its packaging. **As a manufacturer/food processing company** I also want to get a traceability report for all the stages of production from primary producer to food processing company about a product/batch of products. The report should include production traceability history as well as all the certification and compliance data relevant for that product. **As a supplier** I want to get a traceability report for all the stages of production from farm to supplier about a product/batch of products. The report should include production

	traceability history from primary producers and food processors as well as all the certification and compliance data relevant for that product. **As a supplier** I also want to feed my own traceability information about a specific product/batch of products into the system before the products are supplied further to the retailer. **As a FSQA expert** I want to get a traceability report for all stages of production from farm to retail about a specific product/batch of products. The report should include traceability production history from primary producers and food processors as well as all the certification and compliance data relevant for that product. **As a certification body** I want to feed certification and compliance information about products, packaging, producers, processors, suppliers, and retailers into the system. **As a food safety authority** I want to get a traceability report for all stages of production from farm to retail about a specific product/batch of products. The report should include traceability production history from primary producers and food processors as well as all the certification and compliance data relevant for that product. **As a food safety authority** I want to feed information about recalls for a specific product/a batch of products into the system and alert all relevant supply chain stakeholders. **As a laboratory** I want to feed laboratory test results about a product/a batch of products relevant for food safety and quality into the system.
Involved Stakeholders	**Producers/Growers/Farmers** - providing their traceability data and certification and compliance data for a product/a batch of products **Manufacturers/Food Processing Companies/Abattoirs** - providing their traceability data and certification and compliance data for a product/a batch of products; reading traceability report on previous production stages **Suppliers** - providing their traceability data and certification and compliance data for a product/a batch of products; reading traceability report on previous production stages **Food Safety and Quality Assurance (FSQA) experts at retailers** - reading/analyzing traceability report about a specific product or a batch of products **Certification bodies** - providing certification and compliance information **Food safety authorities** - providing information on audits, recalls **Laboratories** - providing laboratory analysis results
TheFSM components involved	Data sources: ● Farm management systems ● ERP/WMS systems ● Legacy systems Security Layer: ● A2C components ● E2E security components Data processing: ● License and agreement management ● Query explorer Data curation and Semantic enrichment ● Semantic mapper ● Secure storage & indexing Identity management & blockchain ● Decentralized identifiers & DIF Universal hub ● Transaction Validation Engine ● Underlying DLT Resource management: ● **Data flow management (data pipeline)** ● Message brokerage service ● Resource orchestrator

	Data brokerage model & engine ● Data brokerage model ● Data brokerage engine ● Micro-contracts auth ● Micro-contracts drafting, validation & execution engine
Pre-conditions	- Product & batch identification, as well as stakeholder identification should conform to industry standards such as GS1 ID Keys (GTIN, GLN etc) - Traceability data should conform to globally utilized standards, particularly GS1 EPCIS for event based tracking - Appropriate semantic mappers & standards need to be incorporated into the system to produce standardized semantic data
Use Case Path	**User perspective (read side):** End users search for relevant data on the FSM by performing traceability data queries using specific product batch identifiers or unique product identifiers, such as GTIN numbers, LOT numbers or any combination of those. The user can be unaware of such identifiers in case of using a system such as a GS1 Digital Link, resolving to the appropriate resource in the FSM by having the knowledge of appropriate identifiers in the GS1 Digital Link itself. The queries are performed via a secure channel and the appropriate A2C system is in place. The data storage system should conform to the GS1 EPCIS Repository specifications. The FSM performs queries across the participating systems, of product traceability data indexed in their secure storage modules (individual EPCIS repositories). Responses from the systems (identified by their DIDs) are handled by the query explorer and presented as Verifiable claims or data feeds in standardized GS1 EPCIS data structure. Each received document is verifiable by utilization of DLTs (using the DIF Identity hub, Universal Resolver and OriginTrail Verification mechanisms). A stack of contract management data brokerage modules allows for data monetization - purchase by the interested parties directly from data owners. **Data sourcing perspective:** Originating systems provide data through standardized interfaces into the FSM for mapping. Data is being ingested, prepared and parsed using a data flow manager (Apache Nifi or similar), while streams are being handled by the Message Broker service (Apache Kafka or similar). Data structuring according to GS1 EPCIS is performed partially at Data Flow Management modules and partially with Data curation and Semantic enrichment modules. Relevant data is being timestamped, organized according to access policies and attributes, and wrapped into verifiable credential form for later proof verification (so that the data verifier can verify the data issuer identity and data integrity). The cryptographic data proofs and indexes are being stored in such a way that they can be queried by the FSM systems. Relevant resources utilized in the integration are managed by the resource orchestration module. Failures and errors are communicated to system administrators using a system specific messaging module.
Post Condition	Stakeholders of FSM are able to obtain traceability information based on their queries using product and batch identifiers, to access the connected traceability information from all the supply chain partners sharing information on that specific product. The users are able to verify the data issuer of each data point (by using the verifiable credentials data standard) and it's integrity.
Leading Partner	Prospeh
Contributing Partners	UBITECH, PROSPEH

Table-16 UC-2: Share traceability information of a specific product

UC ID	UC-3
Use Case Title	Share **certification data** of a specific product (covering all the phases of the product life cycle) with public and/or specific stakeholders
Related Functional Requirement(s)	FR_3, FR_4, FR_19, FR_37, FR_49, FR_61, FR_66, FR_67, FR_68, FR_70, FR_72
Description	This use case covers user/system interactions needed for sharing specific certification related data. The users – food producers, food processors and packers share their company certifications like ISO 9001 and specific Global Gap certificates and lot information. On the other hand certification bodies are able to enter information about issued certificates such as verification. They all use a specific UI in the Data Publish service. In cases when we are dealing with images or handwritten forms, there will be additional fields with metadata about the document to be fulfilled and to be used instead of the document itself. Various Natural Language Processing tools will be used for extraction of semantic categories from plain texts. The field values and categories are mapped to the FSM Semantic Model in order for a unification to be achieved. The entry process ends with storing the document representation in the Semantic Storage. Each separate data source will require its corresponding customization of the processing pipeline. Additionally information from external public data sources will be accessed and ingested into the semantic storage. Once processed, the data can be retrieved by authorized users via specially designed Query Explorer service offering various parameterized queries.
Involved Stakeholders	Data providers: Producers, Processors, Packaging Companies, Certification Bodies Data consumers: All
TheFSM components involved	The FSM Semantic Model and all Data Curation and Semantic Enrichment modules. Data processing and Analysis module. Identity management, Anonymization Framework, Encryption/Decryption services
Pre-conditions	All data sources are identified, access to them is assured, and entry points are defined. Corresponding data ingestion service and Data publishing service entries for each data source and type are defined and customized.
Use Case Path	Data provider (user) registers in the system and using Data publishing service via Security Layer provides a document or database records of some predefined type. In case of a raw document – text, scanned image, etc. the valued fields of the document are replaced with their metadata equivalents and they must be filled manually. This functionality is implemented as a part of the publishing service. Preprocessing is performed, fields are identified. Sensitive data is anonymized and/or pseudonymized by Anonymization Framework. The corresponding data ingestion service pipeline is called. Data curation and semantic mapping are performed and the input data is transformed to the corresponding RDF triples set regarding the FSM Semantic Model. The set is stored via Apolo Federation service in GraphDB and the original document (depending on the need to be displayed further) is stored in the corresponding storage – RDBMS, Json storage or document storage. The same process could be performed periodically or on demand by Data Ingestion Service for querying data from other external sources like LOD, External Farm Management Systems, Certification Authorities and Certificate registers, etc. When some user needs access to certification information, he registers in the platform using Identity Management Systems and depending on his obtained access permissions calls the

	Query Explorer and retrieves the needed data from the Semantic Storage and connected data storages via Apolo Federation service. The platform-wide tools for orchestration and messaging are also used
Post Condition	The data inputs: ● Certification data of existing certificates, ● laboratory measurement results related to specific food production/packaging/processing lots, ● data records about used food lots for delivering of each food processing/packaging lot, ● other required documents are transformed into RDF format with regards to the Semantic Objects Model. Extracted and generalized data objects are persisted in the Semantic Repository. The original documents are loaded in the additional data storages depending on their type. All data transfer and persistence and is in conformance with GDPR requirements.
Leading Partner	SAI
Contributing Partners	Ubitech, Agroknow, Prospeh

Table-17 UC-3: Share certification data of a specific product

UC ID	UC-4
Use Case Title	**View list of potential collaborators, products etc.** based on specific criteria and access details
Related Functional Requirement(s)	FR_62, FR_21, FR_22, FR_23, FR_24, FR_25, FR_26, FR_76, FR_85, FR_86, FR_87, FR_88, FR_97, FR_98, FR_99, FR_102, FR_136
Description	Story-like description of the events, interactions between actors and systems A retailer that has thousands of suppliers can use the TheFSM empowered FOODAKAI module to search for a supplier (collaborator) which can be a producer, a manufacturer or food processor. The catalogue of all the collaborators can be accessed by FOODAKAI through an API of the data platform and any user of FOODAKAI can access this information. The information (details) of the supplier that is presented to the retailer depends on the visibility preferences that the supplier has selected. Each field of the supplier entity has a visibility option. The retailer may see the list of the Certification Bodies and Certification Schema owners that the supplier (producer, processor) is working with.
Involved Stakeholders	Roles that people have in relation to the certification process ● Quality assurance and Food Safety Experts working in the retailer ● Food producer, food processor or food manufacturer
TheFSM components involved	TheFSM tools/components/modules. ● Data sources: FOODAKAI will invoke an API of the data sources layer to get the list of all collaborators (already supported by the FOODAKAI data platform) ● Identify management: an API to get a unique identifier (UID) for each collaborator or to retrieve the UID based on the company name, location, etc.

Pre-conditions	The conditions that must be met before the scenario described in this use case can be implemented. ● The retailer needs to create a company profile and a user account in FOODAKAI ● The supplier (producer, processor) should create a profile and a user account in FOODAKAI
Use Case Path	A short description of the workflow followed in the use case, based on TheFSM modules, defining the architecture. ● FOODAKAI system invokes an API of the data sources layer to get a catalogue of all the collaborators or to search a collaborator based on specific criteria (e.g. using the collaborator name) ● TheFSM platform's indexer provides a response with an agreed schema that is compliant with the data standards that will be followed in the project. The data in the response provides enriched data for the collaborator. ● FOODAKAI system gets the response and presents the data in the supplier profile
Post Condition	What is achieved if this use case is successfully completed ● The retailer can find his suppliers and through suppliers the Certification Organizations, Auditors and Certification Schema owners that the supplier is collaborating with ● The food producer or processor is able to find the Certification Bodies, Owners Schemas and Auditors that is collaborating with.
Leading Partner	Consortium partner(s) highly involved in the development of the systems components and functionalities associated with the UC ● Agroknow (leader) ● Ubitech ● Prospech ● Agrivi (to retrieve producer and farming data)
Contributing Partners	Consortium partners with supporting roles ● TUV Austria ● GlobalGap

Table-18 UC-4: View list of datasets (potential collaborators, products etc.) based on specific criteria and access details

UC ID	UC-5
Use Case Title	**Monitor status (profile**) of a specific collaborator (producer, retailer, food processor etc.)
Related Functional Requirement(s)	FR_11, FR_16, FR_19, FR_62, FR_72, FR_96, FR_120, FR_128, FR_130, FR_131, FR_132, FR_141, FR_142, FR_143, FR_144, FR_145, FR_146, FR_147, FR_148, FR_151, FR_153
Description	Story-like description of the events, interactions between actors and systems The retailer has purchased a subscription to the FOODAKAI Premium Package. The Quality Assurance and Food Safety Experts of the retailer are the end users of the FOODAKAI platform. The expert is using the FOODAKAI to monitor a supplier (may be a producer, grower or food processor) by using the TheFSM-powered FOODAKAI. Monitor means that he can store the name of the supplier that he wants to monitor and he gets a profile with live data about the supplier, a risk score for the supplier and alerts every time that there is a new event for the supplier (incident, audit, laboratory data, risk increase).

	The monitoring starts with an invitation that is sent by the retailer to the supplier. The latter needs to accept the invitation and to add all the required information that is needed for the monitoring. The profile of the supplier that the experts monitor includes information about incidents that he was involved in, audits, audit reports, laboratory testing results, food safety plan mainly OPRPs and CCPs, mitigation actions, certificates, certification bodies, subsidiaries and parent organizations.
Involved Stakeholders	Roles that people have in relation to the certification process
TheFSM components involved	TheFSM tools/components/modules. ● Security layer to securely transfer data provided by the supplier ● Identity management to assign and get a unique ID for the supplier ● A2C Engine to check the access rights for the specific data ● Anonymization layer to anonymize the information that can be used for generic analytics and open data layer ● Data sources layer to check for a new event for the specific supplier
Pre-conditions	The conditions that must be met before the scenario described in this use case can be implemented. ● Retailer needs to purchase a FOODAKAI subscription ● Retailer's experts need to invite the supplier to the system ● Supplier (producer, processor, manufacturer) needs to accept the invitation, create an account in FOODAKAI and add all the information that is needed for monitoring.
Use Case Path	A short description of the workflow followed in the use case, based on TheFSM modules, defining the architecture. ● FOODAKAI System invokes the API of the data sources to get information about a specific supplier including his UID ● Data sources connects to farm managements, ERPs/CRMs (of retailers, certification body, certificate schema owner) and open data sources to provide information and new events about the supplier ● FOODAKAI uses the A2C to check if the retailer has access to the data of the specific supplier ● FOODAKAI uses the anonymization service to anonymize data of the supplier that can be used for generating analytics ● FOODAKAI uses the security layer to transfer business sensitive information (audit results, laboratory tests) of the supplier ● FOODAKAI uses the alerting mechanism to send an alert to retailer if there a new event for the supplier
Post Condition	What is achieved if this use case is successfully completed The retailer is able to continuously monitor a supplier, he can study the profile of the supplier at any point and is informed every time that a new event is announced about the supplier. The FOODAKAI system is able to provide a live risk score for the supplier.
Leading Partner	Consortium partner(s) highly involved in the development of the systems components and functionalities associated with the UC ● Agroknow is responsible for the development of the end user application ● Ubitech for developing the data platform mechanisms for secure data exchange ● SAI responsible for semantic services
Contributing Partners	Consortium partners with supporting roles ● TUV AUSTRIA ● Agrivi

	● PROSPEH ● (GlobalGap)

Table-19 UC-5: Monitor status (profile) of a specific collaborator (producer, retailer, food processor etc.)

UC ID	UC-6
Use Case Title	**Share (and monitor) own data** (production plans, progress, practices, risks, deliveries, business resources)
Related Functional Requirement(s)	FR_21, FR_29, FR_33, FR_64, FR_67, FR_69
Description	This user case covers activities and functionality allowing food suppliers (producers, processors, packers) to share certain information to their customers and certification bodies. There are two main groups of data objects: static and real-time data. The first one includes company identification data, facilities, equipment (if necessary), production capacity, financial state, production plans, investment plans, plots, used technology, certifications, etc. The second group is real time data – measured values from some IoT sensors or broadcasted by company ERP systems: lots, production and storage temperatures, some sensor values, etc. The purpose of this use case is to allow the customer or the certification body to assess the supplier capacity and to perform real time quality control for negotiated deliveries and certification audit. The static data is possible to be entered and modified by the user via some UI as a part of Data publish service or extracts from customers in-house ERP system to be uploaded. In that case some ETL pipeline will be applied in order the data to be transformed and stored in the Semantic Storage (GraphDB) and lateral data storages: RDBMS, Json store or Document Store. The real-time data will come automatically by receiving messages from the supplier's ERP system or from some IoT sensors. In the latter case there will also be some aggregation filter which will reduce the stored data volume. An ETL will also be applied in order the information to be stored. The users – supplier, customer and certification body, provided they were authorized by the supplier, will be able to read and probably validate its data via Query Explorer The authorization aspect is important. Except the data provider, only authorized parties are allowed to receive his data.
Involved Stakeholders	Data providers: Producers, Processors, Packaging Companies Data consumers: Processors, Packaging companies, Retailers, Certification bodies Technological partners: Agroknow, Ubitech, Prospeh
TheFSM components involved	The FSM Semantic Model and all Data Curation and Semantic Enrichment module. Data processing and Analysis module. Identity management, Anonymization Framework, Encryption/Decryption services, Data Brokerage Engine
Pre-conditions	Data supplier is registered. His company data model is known, a corresponding ETL pipeline is customized. The real-time incoming data aggregation filters are instantiated and customized
Use Case Path	Data provider (user) registers in the system and provides his company static data: company name, identifier, company location, offices, facilities, equipment, production capacity and plans, certification (there is an overlap with UC-3) etc. using the UI, or uploads some xls or csv files with this information. In case of upload, a field names mapping must be defined in advance. When a modification/addition is needed, he is using the UI or uploads the new data.

	If the supplier provides a real-time streaming of sensor data, the corresponding income filter must be customized and the data input will be performed automatically. The filter generalizes the input data and using the Data Ingestion Service stores them in the system. It could be also possible the supplier to upload some measurement data time-to-time in a manual or semi-manual manner as an alternative to automatic ingestion. It the suppliers likes to share some data to other party, using Data Brokerage Service and Identity Management Service he grant the access to its own data or some parts of it – e.g, for a specific product only. The data consumer queries the suppliers data using Query Explorer All communication of sensitive data is going to be performed using End to end encryption/decryption (between Query Explorer and the receiving user) The platform-wide tools for orchestration and messaging are also used
Post Condition	The suppliers own data are stored in the Semantic Repository.in compliance with TheFSM Semantic Model. Time series from IoT sensors are stored in RDBMS. All data transfer and persistence is in conformance with GDPR requirements.
Leading Partner	SAI
Contributing Partners	Agroknow, Ubitech, Prospeh

Table-20 UC-6: Share (and monitor) own data

UC ID	UC-7
Use Case Title	**Support audit and certification data exchange** between the certification body and the agri-food stakeholders
Related Business Requirement(s)	BR_nr1_2, BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_5, BR_nr2_6, BR_nr2_8, BR_nr2_9, BR_nr2_10, BR_nr2_14, BR_nr2_16, BR_nr2_35, BR_nr2_36, BR_nr2_37, BR_nr2_38, BR_nr2_39, BR_nr2_46, BR_nr3_1, BR_nr3_2, BR_nr3_3, BR_nr3_5, BR_nr3_6, BR_nr3_7, BR_nr3_25, BR_nr3_28, BR_nr3_33, BR_nr3_34, BR_nr3_36, BR_nr4_1, BR_nr4_2, BR_nr4_3, BR_nr4_4, BR_nr4_6, BR_nr4_7, BR_nr4_8, BR_nr5_2, BR_nr5_3, BR_nr5_4, BR_nr5_10, BR_nr5_12
Description	An actor requests an audit report in order to obtain a certificate for upholding certain standards. The auditor submits their findings, so that the Certification Body can decide whether the actor fits the qualifications for the certificate. Monetization procedures take place before issuing the certificate, if necessary and the actor eventually obtains the certificate. Now, they can share this and other data involving them to an interested third party for a potential collaboration.
Involved Stakeholders	At least an auditor, the Certification Body and two parties/actors (one for which the auditor writes their report for and one which is interested in data exchange)
TheFSM components involved	Security Layer, Smart Contracting Layer, Alerting component, Traceability component, Resource Management Layer, Automated Contract Negotiation and Monetization components
Pre-conditions	Involved parties must be already registered to the platform with their respective roles and they must also be aware of each other’s existence.
Use Case Path	Certification data exchange: ● Parties log in to the platform. ● Security Layer authenticates and authorizes them (working together with Traceability component).

	● Each party interacts with the Security Layer so that they authorize access to their certificates to the other partner. ● The Smart Contracting Layer compares the certificates to their signatures to verify immutability status. Audit report submission and certification issuing: ● Auditor login in to the platform. ● Security Layer authenticates and authorizes them (working together with Traceability component). ● Auditor submits a digital form with their findings, which is processed by the Resource Management component. ● Auditor defines via rules who is authorized to view the report (actors of and for whom the auditor wrote the report are automatically authorized). ● Smart Contract Layer generates the report's signature for immutability checking and then, in cooperation with the Security Layer, encrypts and stores the report. ● All parties involved are notified by the Alerting component. ● User from Certification Body logs in to the platform. ● Security Layer authenticates and authorizes them (working together with Traceability component). ● The user obtains the audit report, decrypts it by interacting with the Security Layer and, after interacting with the Smart Contracting Layer, checks its signature to verify its immutability for transparency. ● The Alert component will undertake the task of notifying the involved parties on which actions they need to take, if necessary, or notify them of the success of the process. ● If monetization is involved for the certificate, the Automated Contract Negotiation and Monetization components also need to be involved. If so, additional access constraints are imposed on the certificate, until the corresponding actor pays off the debt. ● The Resource Management Layer then stores all information in a proper uniform and standardized structure, so that the certificate can be easily handled by all other components as needed. ● The Smart Contract Layer also generates the certificate's signature and, working with the Security Layer (ABE's mechanism to be more specific), stores both the certificate and the signature.
Data sources	-
Post Condition	Audit reports are submitted, processed and the interested parties are notified/Parties exchange data with authorization.
Leading Partner	UBITECH, PROSPEH
Contributing Partners	-

Table-21 UC-7: Support audit and certification data exchange

UC ID	**UC-8**
Use Case Title	**Support agreements on product specifications** between the stakeholders
Related Business Requirement(s)	BR_nr2_7, BR_nr2_8, BR_nr2_9, BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33, BR_nr3_1, BR_nr3_2, BR_nr3_3, BR_nr3_5, BR_nr3_6, BR_nr4_19, BR_nr4_20, BR_nr4_21, BR_nr5_10, BR_nr5_12

Description	Two actors wish to form an agreement. They first login to the platform and verify each other's identities. Then, they compose the document of the agreement, using draft versions and getting assisted in addressing any legal constraints which may be imposed on a specific kind of agreement. After finalizing it, the agreement is stored to the platform and all interested parties are notified (depending on the nature of the agreement, the Certification Body may also be notified).
Involved Stakeholders	Two actors interacting in order to reach an agreement on product specifications.
TheFSM components involved	Security Layer, Smart Contracting Layer, Traceability component, Resource Manager, Automated Contract Negotiation and Monetization components, Alerting component.
Pre-conditions	The actors must already be registered to the platform and they also need to have filled their respective information.
Use Case Path	Parties log in to the platform. The Security Layer authenticates and authorizes them (working together with Traceability component). The Security Layer verifies their identities to each other. Resource Manager offer legal constraints which are related to the agreement. The participants will interact with the Smart Contracting Layer and the Automated Contract Negotiation and Monetization components to generate a smart contract with a structured format, while the Security Layer will ensure they are authorized to take any action that they do. The Automated Contract Negotiation component will provide functions like automatic draft versions of the contract as the partners work on it till they reach a final version, while the Monetization component will handle any monetary transactions and conditions involving the document. The agreement is processed by the Smart Contracting Layer and enters the blockchain. The participants specify the attributes the agreement should have for access. The agreement document is encrypted and stored to the platform. Any intermediate information required by the Traceability component will be forwarded to it, since the contract is semantically related to the two participants now. If the contract requires the interference of a legal entity such as the Certification Body, or if the Certification Body requires to be automatically notified about a newly finalized contract, the involved legal entities will also be notified.
Data sources	-
Post Condition	A 100% legal agreement is established between interested parties. The Certification Body may or may not be notified about this.
Leading Partner	UBITECH
Contributing Partners	PROSPEH

Table-22 UC-8: Support agreements on product specifications

UC ID	**UC-9**

Use Case Title	**Generate alerts** when new data are provided for a product
Related Business Requirement(s)	BR_nr1_1, BR_nr1_2, BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_8, BR_nr2_9, BR_nr2_10, BR_nr2_14, BR_nr2_20, BR_nr2_24, BR_nr2_31, BR_nr2_32, BR_nr2_33, BR_nr2_34, BR_nr3_1, BR_nr3_2, BR_nr3_3, BR_nr3_6, BR_nr3_7, BR_nr3_9, BR_nr3_12, BR_nr3_14, BR_nr3_34, BR_nr3_35, BR_nr3_36, BR_nr4_6, BR_nr4_7, BR_nr4_8, BR_nr4_19, BR_nr4_20, BR_nr4_21, BR_nr5_2, BR_nr5_3, BR_nr5_4, BR_nr5_6
Description	Actor related to a product and, more specifically, wishing to update the product's information logs in to the platform, updates the information, (optionally) sets fine-grained access to the product's information and submits the data via digital forms. All subscribers to the product's information immediately receive a notification reflecting the latest status.
Involved Stakeholders	All (for each kind of alert, only related actors are notified but they can be of any type)
TheFSM components involved	Traceability component, Security Layer, Smart Contracting Layer, Data Processing Layer, Alerting component.
Pre-conditions	Actor must be already registered, related to the product and the product's initial information and access policies must be already filled.
Use Case Path	Actor related to a product and more specifically its updated information logs in to the platform. The Security Layer authenticates and authorizes them (working together with Traceability component). The Security Layer must enable them to update the product's information, provided they are authorized to do so. The actor can optionally adjust the rules indicating who is authorized to access the product's information. The actor submits everything via digital forms, which are then processed by the Data Processing Layer. The product's info is encrypted and stored to the platform via the Security Layer. All subscribers to the resource (in this case, the product's information) are immediately notified by the Alerting component.
Data sources	-
Post Condition	When new data is produced involving a product, all interested parties (subscribers) are immediately notified.
Leading Partner	UBITECH
Contributing Partners	PROSPEH

Table-23 UC-9: Generate alerts when new data are provided

UC ID	**UC-10**
Use Case Title	**Extract of insights and analytics**

Related Functional Requirement(s)	FR_5, FR_18, FR_31, FR_94, FR_96
Description	Story-like description of the events, interactions between actors and systems The retailer has purchased a subscription to the FOODAKAI Premium Package. The Quality Assurance and Food Safety Experts of the retailer are the end users of the FOODAKAI platform. The expert is using the FOODAKAI and has access to a suppliers dashboard that highlights which are the suppliers at high risk and they need to take actions. The expert clicks on the supplier that is at high risk and can study the profile of the supplier and he can understand why he is at high risk e.g. there is an increasing micro trend for one of his key ingredients. He can see analytics about the ingredients trends, about previous incidents and he can see the estimated risk score for the supplier. Using the analytics, the insights and the risk score he is taking a decision about the mitigation actions e.g. notifying the supplier to do extra lab tests or request an extra audit.
Involved Stakeholders	Roles that people have in relation to the certification process ● Food safety and quality assurance expert on the side of the retailer ● Food safety and quality assurance expert on the side of the supplier (producer, processor, manufacturer) ● Auditor working in a Certification Body ● Laboratory that is working with retailer or supplier to perform tests
TheFSM components involved	TheFSM tools/components/modules. ● Security layer to securely transfer data provided by the supplier ● A2C Engine to check the access rights for the specific data ● Anonymization layer to anonymize the information that can be used for generic analytics and open data layer ● Data sources layer to check for a new event for the specific supplier
Pre-conditions	The conditions that must be met before the scenario described in this use case can be implemented. ● Retailer needs to purchase a FOODAKAI subscription ● Retailer's experts need to invite the supplier to the system ● Supplier (producer, processor, manufacturer) needs to accept the invitation, create an account in FOODAKAI and add all the information that is needed for monitoring. ● Auditor needs to be registered in the data sources
Use Case Path	A short description of the workflow followed in the use case, based on TheFSM modules, defining the architecture. ● FOODAKAI systems invokes the API of the Data Sources layer using the UID of the company to get the latest update of the supplier's data ● FOODAKAI system calls the analytics API and the risk API for the supplier ● FOODAKAI system presents the results in the supplier profile ● FOODAKAI system send an notification to the supplier ● FOODAKAI system sends a request to the catalogue of collaborators to get the names of auditors ● FOODAKAI system sends the invitation to the auditor to perform an extra audit ● FOODAKAI system invokes the API of the automated contracts for generating a contract with the Certification Body (start date, end date, agreed report) ● Auditor uses the Auditor Application to submit the report ● FOODAKAI system uses the data sources API to get the report for the specific supplier (UID) and auditor (UID) ● FOODAKAI system presents the report on the supplier profile page

Post Condition	What is achieved if this use case is successfully completed ● The Food Safety and Quality Assurance experts working in the retailer have access to a suppliers dashboard with analytics and insights for all the suppliers ● The Food Safety and Quality Assurance experts working in the retailer have access to a rich supplier profile with all the required information to mitigate the risk
Leading Partner	Consortium partner(s) highly involved in the development of the systems components and functionalities associated with the UC ● Agroknow is responsible for the development of the end user application ● Ubitech for developing the data platform mechanisms for secure data exchange
Contributing Partners	Consortium partners with supporting roles ● TUV AUSTRIA ● PROSPEH

Table-24 UC-10: Extract of insights and analytics

UC ID	**UC-11**
Use Case Title	**Access various data sources related to production to support decision making**
Related Functional Requirement(s)	FR_30, FR_35, FR_61, FR_63, FR_64, FR_75, FR_79, FR_94, FR_107, FR_119, FR_136
Description	Collection of farm data from external farm management systems and AGRIVI where collection of data includes: agricultural plots information, soil information, meteorological information, field records information etc., relevant to food processor's requirements together with the safety and quality certification requirements. The connection between farm producer and food processor happens through different stages of time, as it requires the availability and access to different types of information.
Involved Stakeholders	Producers (farm producers), food processors (food processing companies), consultants and Global G.A.P. approved certification bodies who conduct Global G.A.P. audits (auditors)
TheFSM components involved	Data Source: Third-party Farm Management System & AGRIVI
Pre-conditions	- Food Processing company together with farm producers from which the company sources the produce need to become users of a Farm Management System (Agrivi) - Farm producers need to enter their growing practices within farm management system during the growing season - Food processing company needs to have traceability insight into farm producer growing practises within the farm management system - Consultants need to have access to farm management system in order to collect data and perform internal audits - Global G.A.P. auditors need to have the possibility to view farm reports for certification purpose
Use Case Path	Farm producer has an access to a farm management system where he keeps records regarding the farm production.

	A farm producer manages its farm data within the farm management system where during the crop vegetation season he keeps track over the required plot (geographical location, agricultural ID information, plot name, utilization), soil (chemical analysis information, soil type) and field records data (planting, fertilization, protection, irrigation, harvesting and other field activities data that include information regarding the applied farm material name and amount, location and date of application,..).Farm producer shares the required information with the food processor, for the purpose of positioning and selling his product, directly through a farm management system where a food processor has access or has an insight through required report/s detailing the required production information that is required for the food processor. Farm producer can enable the consultant to view data within the farm management system or export his farm data from the farm management system for the Global G.A.P. certification process that contains the required production traceability information. Farm producers need to be able to find all necessary data related to the production process. Farm management system (Agrivi 2.0) will expose data via API to third party systems but will not consume data from other systems.
Post Condition	Seamless interaction of farm producers and food processors over different stages in time through a farm management system. Seamless Global G.A.P. required record keeping for the producer within the farm management system. Efficient interaction of the farm producer with consultants and /or auditors for the Global G.A.P. certification process.
Leading Partner	● Agrivi for developing the Agrivi 2.0 application which will provide farm management data to TheFSM platform to facilitate the data exchange between the food producer and food processor
Contributing Partners	Consortium partners with supporting roles: ● UBITECH ● TUV Austria ● PROSPEH ● Global G.A.P. ● Agroknow

Table-25 UC-11: Access various data sources related to production to support decision making

4. THEFSM TECHNICAL REQUIREMENTS

This section is dedicated to the technical requirements we extracted by following the thoroughly documented agile methodology. Since all other requirements need to be defined before reaching the technical requirements, they also serve as a way to verify the entire procedure, as any inconsistencies, duplicates, circular dependencies etc will become immediately obvious here. In this section we illustrate both the list of technical requirements we defined and their mapping to functional components.

4.1. List of Technical Requirements

In this section we provide the list of TheFSM Technical Requirements. The columns shown contain information as described here:

- **Reference** ID: The unique identifier defining a technical requirement.
- **Functional Requirement ID**: The unique identifier of the corresponding functional requirement(s) which justify the existence of the respective technical.
- **Technical Requirement**: A small description of the requirement.
- **Functional Components needed**: A list of functional components which are involved in this technical requirement.

Category	Sub-category	ID	Title	Related non-functional requirement	Related functional requirement
Data curation	Data collection, integration	TR_1	TheFSM platform shall allow data to be imported from external sources and systems	NFR_26	FR_14,FR_25,FR_26,FR_36,FR_40,FR_43,FR_47,FR_50,FR_64,FR_65,FR_66
	Data collection, integration	TR_2	TheFSM platform shall allow the user to upload and download files	NFR_26	FR_3,FR_4,FR_8,FR_9,FR_14,FR_25,FR_26,FR_36,FR_40,FR_43,FR_47,FR_50,FR_64,FR_65,FR_66
	Data collection, integration	TR_3	TheFSM platfrom shall allow the data ingestion of stream data	NFR_15,NFR_17,NFR_24,NFR_25,NFR_26	FR_14,FR_25,FR_26,FR_36,FR_40,FR_43,FR_47,FR_50,FR_64,FR_65,FR_66
	Data collection, integration	TR_4	TheFSM platfrom shall allow the data ingestion of batched data	NFR_15,NFR_17,NFR_24,NFR_25,NFR_26	FR_14,FR_25,FR_26,FR_36,FR_40,FR_43,FR_47,FR_50,FR_64,FR_65,FR_66
	Data management, intergration	TR_5	TheFSM platfrom should provide data curation services	NFR_15,NFR_17,NFR_24,NFR_25,NFR_26	FR_76,FR_83,FR_84,FR_95,FR_96
	Data enrichment, integration	TR_6	TheFSM platfrom should provide data enrichment services for data deriving from internal and external datasources using a RESTful API	NFR_15,NFR_17,NFR_24,NFR_25,NFR_26	FR_7,FR_68,FR_69,FR_88,FR_89,FR_99,FR_102,FR_110,FR_123,FR_133,FR_135,FR_149
	Data management, intergration	TR_7	TheFSM platfrom should should offer a well-defined API for data export	NFR_15,NFR_17,NFR_24,NFR_25,NFR_26	FR_7,FR_68,FR_69,FR_88,FR_89,FR_99,FR_102,FR_110,FR_123,FR_133,FR_135,FR_149

	Data enrichment, integration	TR_8	TheFSM platfrom should develop and maintain a semantic model for food safety and certification	NFR_15	FR_34,FR_35,FR_37,FR_38,FR_47,FR_73,FR_119
	Data management, integation, cloud infrastructure	TR_9	TheFSM platfrom should support updating and maintaining uploaded datasets	NFR_3,NFR_15, NFR_17,NFR_25	FR_3,FR_4,FR_8,FR_9,FR_34,FR_35,FR_37,FR_38,FR_47,FR_73,FR_119
	Data management, Integration	TR_10	TheFSM platform should support data representation using well established standards (GS1, EPCIS, WoT)	NFR_26, NFR_32	FR_12, FR_17, FR_20, FR_21, FR_36, FR_39, FR_40, FR_42, FR_52, FR_53, FR_54,FR_65,FR_75,FR_78,FR_79,FR_94, FR_106,FR_112, FR_126, FR_133,FR_150
	Scalability, integration	TR_11	TheFSM platfrom should offer a secure big data infrastructure	NFR_6,NFR_19, NFR_23,NFR_27	FR_82
Security and privacy	Access control, Search engine	TR_12	TheFSM platfrom should offer access control to data based specific parameters	NFR_8,NFR_14	FR_86,FR_100,FR_109
	Anonymization	TR_13	TheFSM platfrom should offer anonymization/pseudonymization services	NFR_1	
	Encryption, Access control	TR_14	TheFSM platfrom should encrypt data files	NFR_1, NFR_31	
	Authorization	TR_15	TheFSM platfrom should provide a controlled and secure way to decrypt data files	NFR_2	
	Authorization	TR_16	TheFSM platfrom should provide robust identity management for user authorization	NFR_1, NFR_2	
	Authorization	TR_17	TheFSM platform shall provide a secure and controlled registration process for new users	NFR_1, NFR_2	FR_1,FR_2
Licencing	Access control	TR_18	TheFSM platfrom should offer an IPR management service to data providers	NFR_30	FR_50,FR_73,FR_137
	Access control	TR_19	TheFSM platform shall store the data sharing contracts in a DLT-based repository for non-repudiation purposes.	NFR_30, NFR_31	FR_12, FR_17, FR_20, FR_21, FR_36, FR_39, FR_40, FR_42, FR_52, FR_53, FR_54, FR_55,FR_56,FR_57,FR_58, FR_94, FR_112, FR_126, FR_133

Traceability	Integration	TR_20	TheFSM platform shall use widely established standards (EPCIS) for traceability data	NFR_32	FR_12, FR_17, FR_20, FR_21, FR_36, FR_39, FR_40, FR_42, FR_52, FR_53, FR_54,FR_55,FR_56,FR_57,FR_58,FR_65,FR_75,FR_78,FR_79,FR_94, FR_106,FR_112, FR_126, FR_133,FR_150
	Traceability, monitoring, notifications	TR_21	TheFSM platform should capture the certification and auditing event in tracebility data	NFR_14,NFR_16,NFR_20	FR_6,FR_7,FR_8,FR_12, FR_17, FR_20, FR_21, FR_22,FR_23,FR_24,FR_36, FR_39, FR_40, FR_42, FR_44,FR_45,FR_46,FR_47,FR_48,FR_49,FR_50,FR_52, FR_53, FR_54, FR_55,FR_56,FR_57,FR_58,FR_91,FR_92,FR_94,FR_101,FR_104,FR_107,FR_111, FR_112, FR_114,FR_117,FR_126, FR_130,FR_133,FR_140,FR_148
	Access control, Traceability	TR_22	TheFSM platform should use DLT for trust and transparency in traceability	NFR_30, NFR_31	FR_12, FR_17, FR_20, FR_21, FR_36, FR_39, FR_40, FR_42, FR_52, FR_53, FR_54,FR_55,FR_56,FR_57,FR_58, FR_94, FR_112, FR_126, FR_133
Data processing	Decision Support, Risk assessment	TR_23	TheFSM platform should offer services for risk assessment and prediction	NFR_10, NFR_11,NFR_21	FR_5,FR_18,FR_115
	Search engine, asset exporation	TR_24	TheFSM platform should offer query services for data asset exploration	NFR_8,NFR_12, NFR_14	FR_77,FR_86,FR_100,FR_109
	Search engine, asset exporation	TR_25	TheFSM platform shall retrieve and show the datasets that are relevant to a dataset that is returned as a query result.	NFR_8,NFR_12, NFR_14	FR_86,FR_100,FR_109
	Decision Support, Risk assessment	TR_26	TheFSM platform shall enable the integration and combined analysis over multiple datasets	NFR_8,NFR_10, NFR_11, NFR_12, NFR_14,NFR_21	FR_5,FR_18,FR_115
	Decision Support, Risk assessment	TR_27	TheFSM platform shall enable the application of predefined data analysis algorithms on datasets	NFR_10, NFR_11,NFR_21	FR_5,FR_18,FR_115
	Decision Support, Risk assessment	TR_28	TheFSM platform shall provide tools and services to apply machine learning algorithms	NFR_10, NFR_11,NFR_21	FR_5,FR_18,FR_115

	Decision Support, Risk assessment	TR_29	TheFSM platform shall provide tools and services to apply deep learning algorithms	NFR_10, NFR_11,NFR_21	FR_5,FR_18,FR_115
	Decision Support, Risk assessment	TR_30	TheFSM platform shall provide tools and services to apply basic analytics and statistics	NFR_10, NFR_11,NFR_21	FR_5,FR_18,FR_115
Added value services	Notifications	TR_31	TheFSM platform should inform users with active contracts on a dataset that the dataset has been updated	NFR_4,NFR_7, NFR_16,NFR_18	FR_10,FR_11,FR_32,FR_80,FR_128,FR_141
	Monitoring	TR_32	TheFSM platform should provide data usage analytics to the users for the datasets they own.	NFR_4, NFR_16	FR_16,FR_27,FR_28,FR_29,FR_30,FR_31,FR_33,FR_67,FR_138
	Access control, authorization, authentication	TR_33	TheFSM platform shall ensure that access control over datasets is applied according to the data provider's policies and the terms of relevant active valid data sharing contracts	NFR_2	FR_94,FR_146,FR_148
Applications	Data views	TR_34	TheFSM platform shall enable the certification data exchange among the parties through intuitive UIs	NFR_9,NFR_13, NFR_31	FR_13,FR_19,FR_21,FR_41,FR_59,FR_60,FR_61,FR_62,FR_63,FR_71,FR_77, FR_81
	Data views	TR_35	TheFSM platform shall provide certification data to food safety stakeholders through intuitive UIs	NFR_9,NFR_13, NFR_31	FR_13,FR_19,FR_21,FR_41,FR_59,FR_60,FR_61,FR_62,FR_63,FR_71,FR_77, FR_81
	API integration, data processing	TR_36	TheFSM platfrom shall integrate with the application using RESTful APIs exchnaging data in json format	NFR_9,NFR_13, NFR_17,NFR_24,NFR_25,NFR_26,NFR_31	FR_34,FR_35,FR_37,FR_38,FR_47,FR_73,FR_119

Table-26 TheFSM Technical Requirements

4.2. Mapping Technical Requirements to functional components

The technical requirements (and the related functional and non-functional requirements) are grouped and mapped under the relevant functional components which will be used in order to define the architectural components of TheFSM architecture.

Functional component needed	**Technical Requirement Reference ID**
DID descriptor objects	TR_11, TR_17, TR_21, TR_31, TR_32
A2C engine	TR_17, TR_8, TR_32, TR_34, TR_35, TR_21, TR_31, TR_32, TR_9, TR_21, TR_12, TR_21, TR_24, TR_25, TR_26
DLT Data management	TR_8, TR_32, TR_34, TR_35
Data Brokerage Engine	TR_8, TR_32, TR_34, TR_35, TR_34, TR_35
Food Inspector	TR_8, TR_32, TR_34, TR_35, TR_9, TR_21
Secure storage and indexing	TR_8, TR_32, TR_34, TR_35, TR_2, TR_7, TR_9, TR_34, TR_35, TR_4, TR_14, TR_1, TR_3, TR_4, TR_5, TR_6, TR_8, TR_10, TR_36, TR_12, TR_21, TR_24, TR_25, TR_26

Data Handler	TR_8, TR_32, TR_34, TR_35, TR_2, TR_7, TR_9, TR_34, TR_35, TR_4, TR_14, TR_1, TR_3, TR_4, TR_5, TR_6, TR_8, TR_10, TR_36, TR_12, TR_21, TR_24, TR_25, TR_26
Data Staging	TR_8, TR_32, TR_34, TR_35, TR_2, TR_7, TR_9, TR_34, TR_35, TR_4, TR_14, TR_1, TR_3, TR_4, TR_5, TR_6, TR_8, TR_10, TR_36, TR_12, TR_21, TR_24, TR_25, TR_26
ABE	TR_2, TR_7, TR_9, TR_34, TR_35, TR_4, TR_14, TR_1, TR_3, TR_4, TR_5, TR_6, TR_8, TR_10, TR_36, TR_34, TR_35, TR_12, TR_21, TR_24, TR_25, TR_26
Foodakai 2.0	TR_4, TR_14
Agrivi 2.0	TR_4, TR_14, TR_9, TR_21
Semantic Mapper	TR_1, TR_3, TR_4, TR_5, TR_6, TR_8, TR_10, TR_36, TR_3, TR_4
Message Brokerage	TR_9, TR_31
VC Repository	TR_9, TR_21, TR_21, TR_22, TR_32
AI Models	TR_10, TR_23, TR_26, TR_27, TR_28, TR_29, TR_30
Data Licence and Agreement management	TR_34, TR_35
Identity management	TR_21, TR_22, TR_32
Query explorer	TR_12, TR_21, TR_24, TR_25, TR_26
Data sources and application catalogue (data publish)	TR_12, TR_21, TR_24, TR_25, TR_26
Legal	TR_13, TR_14, TR_16, TR_17

Table-27 Technical requirements and functional components mapping

5. THEFSM PLATFROM ARCHITECTURE

5.1. Conceptual Architecture

The conceptual architecture of TheFSM has been designed by conducting a thorough analysis of the technical requirements documented in section 4 that were later translated into technological, beyond the state of the art, software modules that will be implemented in the context of WP2, WP3 and WP4. The conceptual architecture of TheFSM is supporting the smooth and effective integration of the several software modules that will be implemented with the aim of maximising the benefits of combining multiple technologies and tools from different partners and organisations. During the design process, concerns and decisions were weighted, and the stakeholder requirements were constantly validated against the design.

TheFSM architecture is a loosely-coupled modular architecture that provides enhanced flexibility in order to adapt and connect the various components that will be implemented as software modules. The major focus was on the functional decomposition, the strict separation of concerns, the dependencies identification and especially the data flow. As such, each component has been designed with the aim of delivering specific business services with a clear context, scope and set of features. Components were assigned to the different technical partners that were involved in the analysis of the requirements, the shaping of the conceptual architecture and the design of the individual components. The technical requirements and the functional specifications were carefully analysed and facilitated the evolution of a mature concept architecture design that is aiming to address the ambition of TheFSM to deliver a novel big data platform for the food safety data value chain.

The main challenge of the TheFSM architecture is to provide the scalable and flexible environment that is enabling the interoperability of the various components that are facilitating the execution of analytics, data monetization and sharing through secure, transparent and advanced functionalities and features. To achieve this, all components of the TheFSM architecture will provide well-defined interfaces to ensure the seamless integration and operation of the integrated platform.

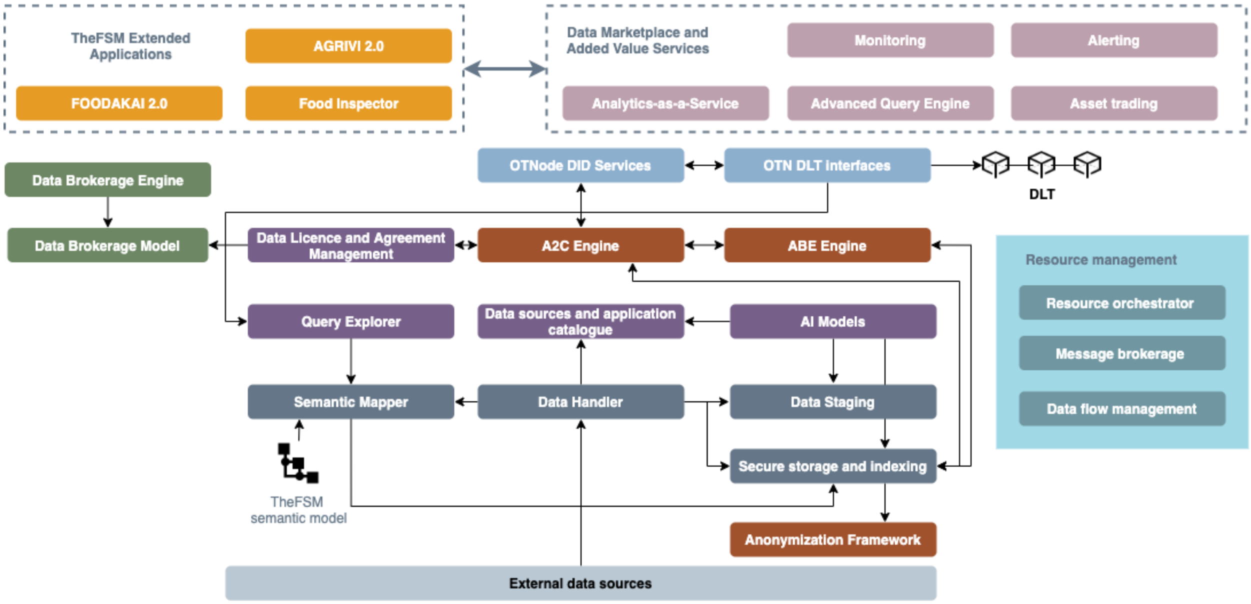


Figure-6 TheFSM Reference Architecture

TheFSM reference architecture consists of a set of loosely coupled architectural components which are organizes in three logical architectural layers: **Data curation and enrichment**, **core services and backend data Platform** and the **applications and marketplace** layer. The data curation and enrichment layer includes all the components which participate mainly in data ingestion, preparation, semantic enrichment and maintenance processes (and are mainly developed under the implementation tasks of WP2). The core services and backend data platform are the components which make use of the data stored and exchanged into TheFSM platform and perform the main data processing, encryption-decryption, analysis, identity and monetization services. Finally, the applications and marketplace layer includes the final offered services of TheFSM platform as they are implemented and provided by the lower architectural layers. These components include the three main applications which will support the end users (developed in WP4), as well as, the API of the services provided by TheFSM data platform consisting TheFSM data market (developed in WP2 and WP3). These services are provided to external applications for integration and other data consumers/providers for data asset trading.

Supporting the everyday transactions as well as the data asset trading in food safety and certification requires the harmonization of multidisciplinary data deriving from a number of heterogenous data sources (see section 5.2.1), while at the same time there's the need to enable the interoperability among different systems and support real-time data exchange. Towards this, the **Data Handler** ingests the data and performs data ingestion functionalities for collecting and storing (aggregated) data from various data streams. Data Handler performs ETL processes and implements a first lever of data transformation regarding a set of supported standards (WoT, GS1). The collected data will be summarized, preprocessed and stored in the **Data Staging.** Data staging is a collection of data storage systems (OntoText, Mongo, Postgres) for storing user data for sharing which is provided on batches or collected and ingested by the Data Handler and are ready for semantic enrichment by the Semantic Mapper. The **Semantic Mapper** provides semantic enrichment of the data using **TheFSM Semantic Model** and generates the relevant RDF representation of the data which is stored in the **Secure storage and Indexing**. The Secure storage and indexing consists of (big-data enabled) storage solutions, capable of storing and managing large amount of data in structured or unstructured format, as well as, semantic repositories (GraphDB) for the storage of the knowledge graphs generated and used in TheFSM platform. Indexing tools like Elasticsearch are used for better text search performance. TheFSM storage solution provides a set of key characteristics such as horizontal scalability, high availability, high performance and advanced security. Additionally, it provides the indexing capabilities of the platform over multiple complex datasets with flexibility and efficiency.

The enriched data are accessed from the **Query Explorer** which implements complex semantic queries based on a set of parameters in order to access and retrieve information from the Secure storage and Indexing. All data sources, as well as, data services build on top of the data are published to **Data Sources and Application Catalogue** which implements a repository of the TheFSM data applications created in the platform. As such, TheFSM applications can be stored, retrieved, modified and loaded in TheFSM Data Marketplace any time they are required. The purpose of the catalogue is to enable the reuse the designed datasets and applications through a defined license provided by the **Data License and Agreement Manager**. The component is responsible for handling all processes related to the data licenses and IPR attributes, as well as enabling the drafting, signing, and enforcing the smart data contracts that correspond to data sharing agreements between platform users. The component defines the **Data Brokerage Model** which is used by the **Data Brokerage Engine** which is responsible for generic brokering of datasets in TheFSM platform between different parties and for possible financial compensation. Regarding the authorization of the platform, attribute-based control on the data is implemented by the **A2C Engine** based on the access policies defined by the data provider in the Data License and Agreement Manager. Apart from the access on the data, **ABE Engine** implements attribute-based encryption (and decryption) of the data files stored in the Secure storage and Indexing. Both engines ensure that only authorized users with specific attributes which fulfil the defined access policies can a) access and b) decrypt the data that they want to access. The **Anonymization Framework** complements the secure attribute-based handling of the data by providing anonymization and pseudonymization of the data. The data access and brokerage mechanisms are supported by state-of-the-art decentralized identity management provided by the **OTNode DID Services**. This component ensures provision and resolution of the Decentralized Identifier Descriptor (DID) and the relevant Verifiable Credentials (VC) of each organization that wants to perform any action on the data (provision, request, update) using DLT. The **OTNode DLT Interfaces** offers an abstraction and data management layer over DLT and facilitates the communication among the OTNode DID Services, the A2C Engine, and the Secure Storage and Indexing in order to manage traceability data exchanges through the platform, as well as, transparency and immutability of the data transactions. **TheFSM Data Marketplace and Added Value Services** provide through APIs a set of added value services to empower the food safety and certification industry which address: a) Provision of data to stakeholders through intelligent query engine, b) Data sharing and monetization services, c) Traceability data services, d) support the analytics algorithms workflow design and execution. These services are used by **TheFSM Extended Applications** which implement a set of intuitive tools and UIs for the stakeholders of TheFSM value chain.

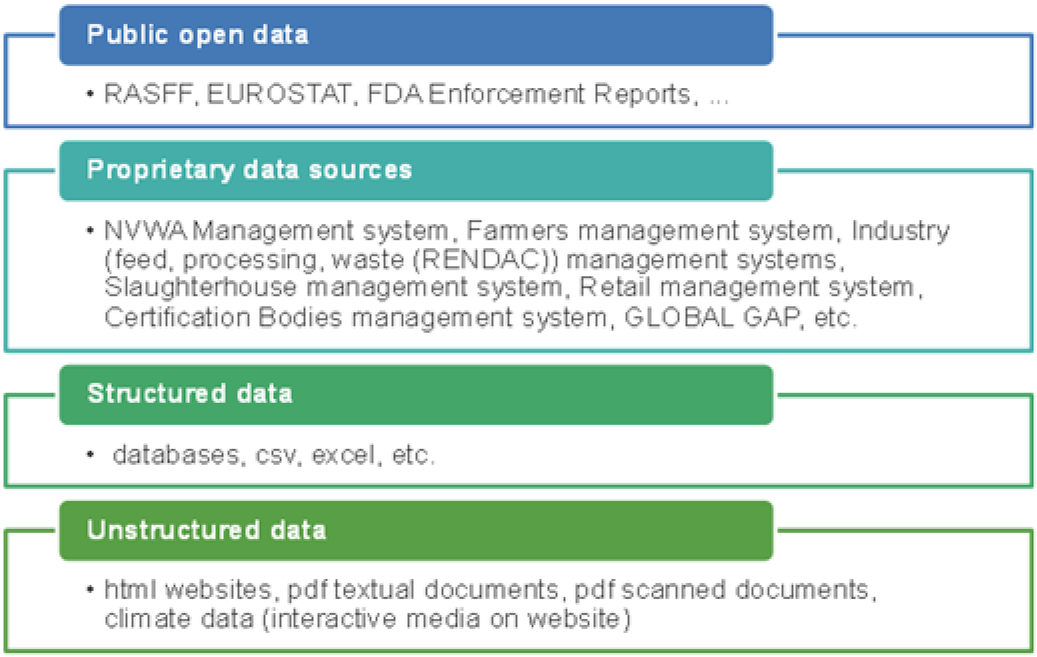
Regarding the resource management of the underlying technical infrastructure of the platform, the resource orchestrator is responsible for distributing tasks, load balancing, creation and setup of VM's for independent, isolated tasks etc. by utilizing state-of-the-art solutions like Kubernetes as part of its infrastructure. The message broker will be responsible for forwarding notifications to required users, depending on settings and nature of data updates. Existing solutions such as Apache Kafka are under consideration for the core of this functionality. Last, the dataflow management is responsible for integrating data, converting them in different formats, storing etc. Further details on the technical architecture will be provided in the second version of TheFSM Architecture.

5.2. TheFSM Architectural Components

5.2.1. Data Sources

Supporting the everyday transactions as well as the data asset trading in food safety and certification requires the harmonization of multidisciplinary data deriving from a number of heterogenous data sources. Each of them has its specifics and sometimes access restrictions and requires individual effort before getting accessible by the platform. They are intended to be used on demand, in real time, when necessary for execution of customer queries and taking into account the access privileges (if required) of the initiating user.

Most data sources are expected to be accessed as APIs providing REST interface over http protocol or as SparQL/GraphQL entry points. A detailed list of external data sources will be presented in D2.1 (M12). Nevertheless, below a list with the core data sources which affect the design of the architecture is presented. TheFSM platform is provisioned as a framework where the data exchange and semantic enrichment is provided as a common functionality even though adding each new specific data source will require its definition and likely development of a specific microservice to deal with it. However, the proposed approach facilitates dynamic addition of new data sources.



Public open data

- RASFF, EUROSTAT, FDA Enforcement Reports, ...

Proprietary data sources

- NVWA Management system, Farmers management system, Industry (feed, processing, waste (RENDAC)) management systems, Slaughterhouse management system, Retail management system, Certification Bodies management system, GLOBAL GAP, etc.

Structured data

- databases, csv, excel, etc.

Unstructured data

- html websites, pdf textual documents, pdf scanned documents, climate data (interactive media on website)

Figure-7 TheFSM Platform Data sources

The following data types are identified to be the input to the platform software:

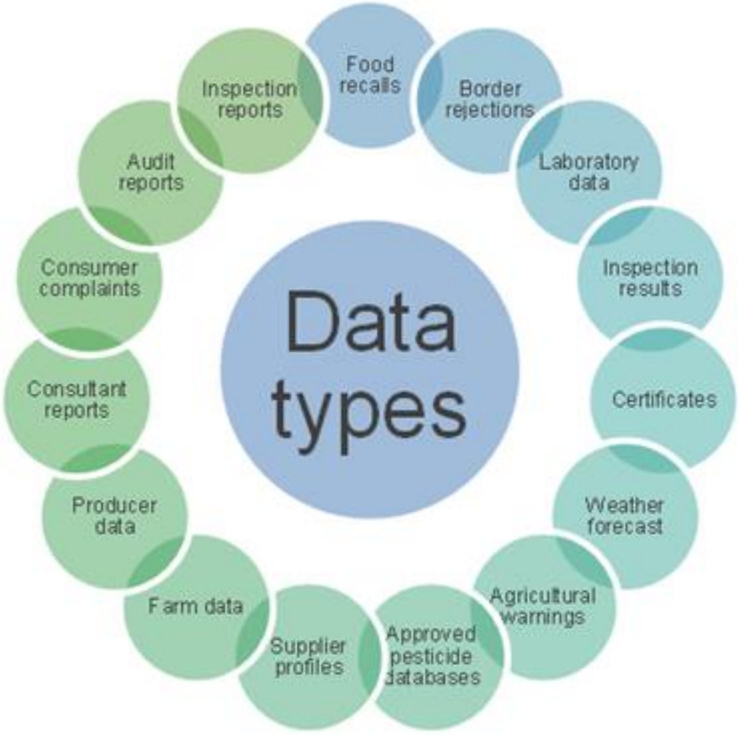


Figure-8 T Data types supported by TheFSM

5.2.2. Data Curation and Semantic Enrichment

This architectural layer provides data ingestion, preparation, semantic enrichment and maintenance processes (and are mainly developed under the implementation tasks of WP2). The layer mainly performs semantic transformation of input data and extracted metadata from the input documents, solving the problem of ambiguity. It also provides semantic enrichment by linking data to various ontologies and external data sources. The layer makes use and extends on the Ontotext Platform[2].

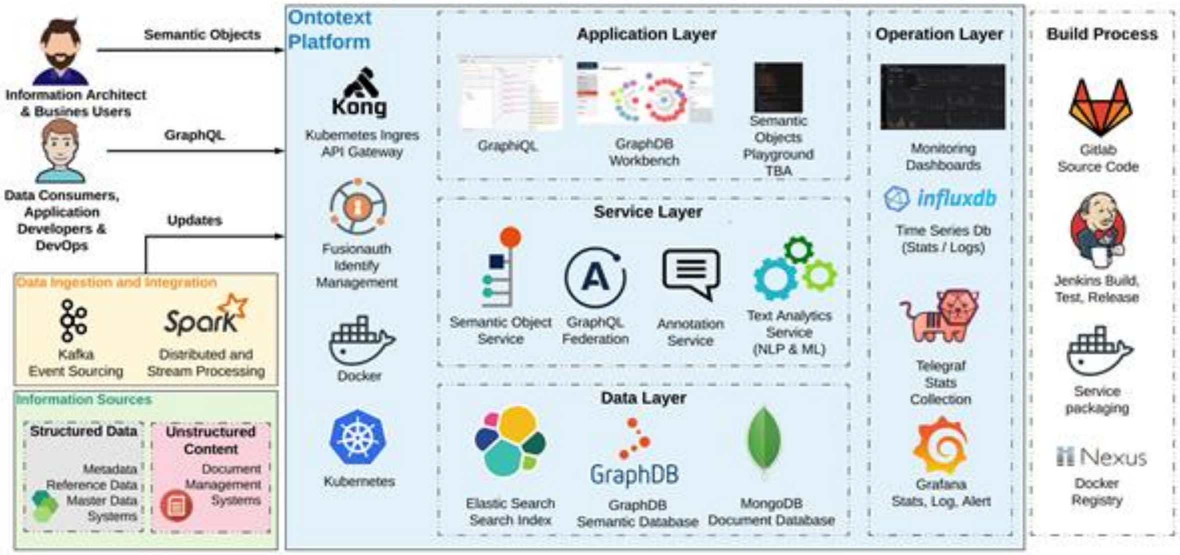

Information Architect & Busines Users
Semantic Objects
GraphQL
Data Consumers, Application Developers & DevOps
Updates
Data Ingestion and Integration
Kafka Event Sourcing
Spark
Distributed and Stream Processing
Information Sources
Structured Data
Metadata
Reference Data
Master Data Systems
Unstructured Content
Document Management Systems
Ontotext Platform
Kong
Kubernetes Ingres API Gateway
Fusionauth Identify Management
Docker
Kubernetes
Application Layer
GraphiQL
GraphDB Workbench
Semantic Objects Playground TBA
Service Layer
Semantic Object Service
GraphQL Federation
Annotation Service
Text Analytics Service (NLP & ML)
Data Layer
Elastic Search Search Index
GraphDB
GraphDB Semantic Database
MongoDB Document Database
Operation Layer
Monitoring Dashboards
influxdb
Time Series Db (Stats / Logs)
Telegraf Stats Collection
Grafana Stats, Log, Alert
Build Process
Gitlab Source Code
Jenkins Build, Test, Release
Service packaging
Nexus
Docker Registry

Figure-9 High-level architecture of Data Curation and Enrichment

5.2.2.1. TheFSM Semantic Model

TheFSM Semantic Model is a set of ontologies and class interrelations featuring the semantic representations of the incoming data objects, received from Data Processing and Analyzing component modules and the other data sources. There is also going to be a set of definitions of the specific input data fields mapping into semantic categories in RDF format as well as the ways of retrieving the corresponding objects' data from their data sources - as API calls, SparQL/GraphQL endpoints or stored data.

5.2.2.1.1. Design and Functionalities Overview

TheFSM Semantic Model will be defined using Semantic Object Model Language (SOML) [4] and functioning via the Semantic Objects Service part of the Ontotext Platform, where the data objects used in Use Case Scenarios are represented semantically. TheFSM Semantic Model will provide an ontology which will be defined on top of some common ontologies used in LOD data sources in regards of data needs from business requirements and use cases workflows. It will also include definitions of the other data classes, retrieved from the Data sources and their semantic mappings

[2] http://platform.ontotext.com/index.html

into the terms of the ontology. The data fields (objects) from different data sources which will be used for enrichment in the use cases will be identified and the ways of their retrieval to be included in Data Sources and application catalogue.

5.2.2.2. Semantic Mapper

The Semantic Mapper is a service providing functionality for mapping of input data to semantic categories and resulting in their RDF representation.

5.2.2.2.1. Design and Functionalities Overview

This service is based on the Ontotext platform[3] components **OntoRefine tool** and **Apollo Federation** service providing functionality for data mapping from textual data and relational database records to semantic representation in RDF format. To resolve any ambiguity problems in the input data, the Onto Refine service will be used to solve them based on the values of the other properties (fields) and the specific context.

The Federation service will be used to combine the data from the various data sources, retrieved by using the functionality of the Data Handler subcomponent and in regards with the mapping definitions in TheFSM Semantic Model and data retrieval descriptions in Data Sources and application catalogue.

The service is going to receive queries from the Query Explorer and using the mapping definitions in the Semantic Data Model to transform the provided data (query parameters) and extract the needed data from data sources via Data Handler functionality, map them again to semantic categories and via Federation Service to construct the query responses.

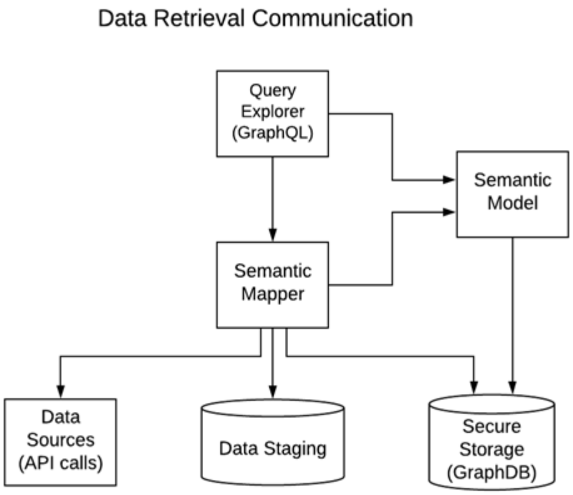


Figure-10 High level architecture of semantic mapper

5.2.2.3. Data Handler

[3] http://platform.ontotext.com/index.html

The Data Handler is a component providing data ingestion functionalities for collecting and storing (aggregated) data from various data streams. The collected data will be summarized, preprocessed and stored in the Data Staging.

5.2.2.3.1. Design and Functionalities Overview

The Data Handler is a set of streaming entry points for receiving WoT and transactional data from third party systems.

It will include WoT parsers, EPCIS parsers and other ETL pipelines for incorporating data from streams from third parties. ETL pipeline is a software service performing data transformation from one format to another. It is very case specific and is usually implemented case by case for transforming parsers output into RDF and storing, if necessary. They will be implemented and deployed as microservices.

If a data provider will share static data which to be stored in the system, a corresponding ETL pipeline must be developed for data transformations and storing in the Data Stage component.

Each datasource type and even the specific data fields/properties/classes which are to be retrieved, as well as the corresponding ETL pipelines to be used for intermediate processing will be defined in the **Data Sources and Application Catalogue**. When a new data source is added, the corresponding definitions of the data it provides must be added there. If the new source requires development of ETL pipelines, they must be implemented and the corresponding records must also be added to Data Sources and application catalogue.

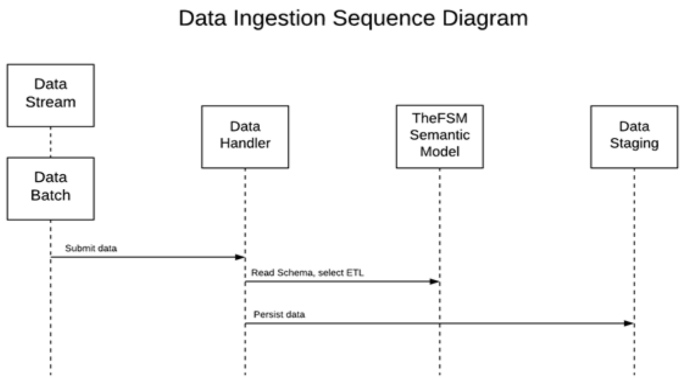


Figure-11 Data ingestion sequence diagram

5.2.2.4. Data Staging

Data Staging is a collection of data storage systems for storing user data for sharing which is provided on batches or collected and ingested by the Data Handler functionality.

5.2.2.4.1. Design and Functionalities Overview

In terms of TheFSM architecture, the Data Staging component consists of data management systems in regards to the stored data types. It will include Ontotext Platform and maybe some other types of storages like JSON storage (MongoDB), and RDBMS (Postgres).

All the data classes in the Data Staging must be included in TheFSM Semantic model SOML schema. The corresponding extensions and reading microservices must be included in the Data Sources and Applications Catalogue. The access restrictions if any must be defined as described further in Data Licensing and Agreement Service.

5.2.2.5. Secure Storage and Indexing

This component contains the semantic repository of the project where all necessary knowledge for running the platform is persisted. Here is the project specific ontology and downloaded and ingested external static ontologies and dictionaries.

5.2.2.5.1. Design and Functionalities Overview

The Ontotext platform featuring GraphDB is expected to be used as a semantic data repository in combination with Elasticsearch for better text search performance. MongoDB could be used as a separate json-data storage, if necessary and some RDBMS like PostgreSQL for local, offline storing of relational data, e.g. if some end user likes to share his static dataset.

All data storage functionality is going to be compliant with GDPR requirements and defined user-object access privileges from Data Licensing and Agreement and Access Management Service. This implies that no sensitive data is stored in the database and most of the data points are retrieved from the data sources when necessary for a specific query from a specific user taking into account his access rights. In cases where some sensitive data is stored, it must be encrypted. The emphasis, however is on dynamic retrieval of up-to-date information from its native sources, so that dataset copies are not going to be stored in the platform only as an exception, However, ontologies and other metadata, as well as data sources descriptions willare going to be persisted in the system.

The above also means that the functionality of the platform is going to depend on third party API versions and any change in the API and/or available data formats could result in malfunction of the data retrieval from the corresponding source, at least until the necessary changes in DSD and the corresponding ETL are done. This also means that some measures of early detection of API changes should be taken and that the partners must share information about planned changes of API call formats and/or data accessibility in advance in order the corresponding updates to be performed on time without interruption of the functionality.

5.2.3. Data Processing

5.2.3.1. Data Sources and application catalogue (data publish)

One of the main objectives of the data semantic processing in TheFSM project platform, is the enrichment of the consumed data with links to external valid data sources so that the data consumers can be provided with up-to-date and valuable data. This enrichment has to be performed real time, at the stage of data consumption, so that only up-to-date information is provided as an output. This approach requires creating an inventory of data sources to be used for the various data objects types and their prioritization in order to solve possible ambiguity problems if the same data object can be obtained from different sources but they also provide different values. So that all the necessary online data sources are identified and rated and their entry-points, API-calls, etc. are collected.

The Data Sources and Applications catalogue is a set of extensions to the platform SOML schema Each data object which can be retrieved from an external source and more specifically the data type is declared as such an extension as well as the service which must be called to retrieve it. If the source is not an SparQL/GraphQL endpoint a specific service which wraps the external source is implemented in order the two-directional data transformation to be achieved. The Semantic Mapper uses these definitions and additionally implemented service to retrieve the needed data. This approach creates a layer between data consumers and actual data sources, allowing all the data accessible within the FSM paltform to be considered as a whole. The only thing the consumer will see is that such data (types) exist, they are accessible and can be used for querying. The actual data sources and all communication details remain hidden to the consumer and he doesn't need to be aware about them.This means that the functionality of the platform will depend on third party API versions and any change in the API and/or available data formats could result in malfunction of the data retrieval from the corresponding source, at least until the necessary changes in the catalogue and the corresponding ETL are done. This also means that some measures of early detection of API changes should be taken and that the partners must share information about planned changes of API call formats and/or data accessibility in advance in order the corresponding updates to be performed on time without interruption of the functionality.

5.2.3.1.1. Design and Functionalities Overview

The Data Sources and Application Catalogue consists of two parts:

- Set of microservices (API calls) wrapping the external data sources and providing the Semantic Mapper (Apollo Federations Service) with all the needed data. If any data preprocessing is needed, it will be implemented in the corresponding microservice.
- Set of definitions – extensions to the SOML representing the structure of data pieces retrievable from the corresponding (remote) data source and their mapping to semantic objects.

The access to the collected and ingested data in the Data Stage component will be performed in the same manner resulting in a single data model. The data transformation to RDF will be performed by the corresponding microservice.

The data from applications and prototypes, parts of TheFSM platform, will be accessed by their provided API and will not be stored (doubled) in other places in the system. This allows using the same approach as in connection to the external data sources.

5.2.3.2. Data License and Agreement Management

The Data License and Agreement Manager is the component responsible for handling all processes related to the data licenses and IPR attributes, as well as enabling the drafting, signing, and enforcing the smart data contracts that correspond to data sharing agreements between platform users. This component is provisioned to handle the data exchange and data transformation between the Data Curation and Semantic Enrichment layer (Data staging), the Automated Contract Negotiation and Monetization layer and the Access and Authorization Control Engine.

5.2.3.2.1. Design and Functionalities Overview

The component has the following main functionalities:

a. Assist and perform a first level of collection of the environmental attributes need from the A2C Engine.
b. Handle any requests from the Automated Contract Negotiation and Monetization layer to the Data staging regarding the definition and review of the data licenses attached to datasets using all license-related metadata information. The information defined here will be stored in the core platform's storage and will be made available to all other components that need to query it.
c. It interacts with the platform's blockchain node to report on the validity of smart contracts for asset monetization. Furthermore, it handles all processes required to prepare a smart contract for each (paid) asset transaction and, finally, upload it to the blockchain.
d. Enable users to define their IPRs, terms of use of data (price, duration of access etc.)
e. Offer predefined data licence templates that the users can review and assign to the datasets they own in the platform
f. Enables the users to draft their own custom data licenses and assign them to the datasets they own in the platform

5.2.3.3. AI Models

In the context of the project Agroknow will build a number of AI-powered models and algorithms that will enhance the processing, forecasting and predictive capabilities of the platform, so that its users may generate more value from the data assets they use. The predictive services will be available through the Intelligence API of the data platform that will be hosted, operated and maintained by Agroknow. The deployment of the API will enable the integration with the TheFSM data platform and the applications that will be developed in the context of the project.
More specifically the predictive services will include:

- **Supplier & Product Risk Assessment Models**: we will integrate, train and test prediction models and algorithms that will be used for the estimation of risks associated with products, suppliers and critical control points (Task 2.3.1)

- **Incident Prediction Models**: we will integrate, train and test prediction models that will be used for the calculation of incident trends and estimations on upcoming threats (Task 2.3.2).
- **Risk prediction models:** we will integrate models and algorithms for the prediction of risk for ingredients and finished products.
- **Supplier risk prediction models:** we will develop, test and integrate models that will provide the ability to predict the risk of a supplier.

The predictive services will be used by the FOODAKAI 2.0 and the Food Inspector application which will be developed in the context of the TheFSM project. In addition to that any other application and third party system will be able to use the services by gaining access to the Intelligence API. The prediction models will be developed using Python and Deep Learning frameworks and libraries like Keras and Prophet.
A first version of the intelligence API was developed during the first year of the project to support the FOODAKAI 2.0 application.

5.2.3.4. Query Explorer catalogue

The query explorer catalogue provides various interfaces for accessing the users' stored data in the platform, their semantic representation and linking to various ontologies and data sources in a consistent and unified manner. It interacts with services in Data Curation and Semantic Enrichment components helping the users to focus on the semantic instead of struggling with various data sources specifics. It also provides a way for interchanging data between platform users featuring data market functionality and allowing data consumers to use the platform in a data source independent manner.

5.2.3.4.1. Design and Functionalities Overview

The query explorer catalogue provides various interfaces for accessing the users' stored data in the platform, their semantic representation and linking to various ontologies and data sources in a consistent and unified manner. It interacts with services in Data Curation and Semantic Enrichment components helping the users to focus on the semantic instead of struggling with various data sources specifics. It also provides a way for interchanging data between platform users featuring data market functionality and allowing data consumers to use the platform in a data source independent manner.

One of possible implementations of Query Explorer is the Ontotext Platform GraphQL Playground where skilled users are able to define their own GraphQL queries in a flexible and convenient way and also to explore the Semantic Object Model Language schema of the project.

Most commonly used queries in regards with identified use case scenarios are going to be provided as predefined parameterized queries where the data consumer users will be able to retrieve the required data in an implementation- and schema-independent way.

All the queries will be run with respect to the calling user access privileges and the results will be filtered (reduced) to those objects the user has rights to see.

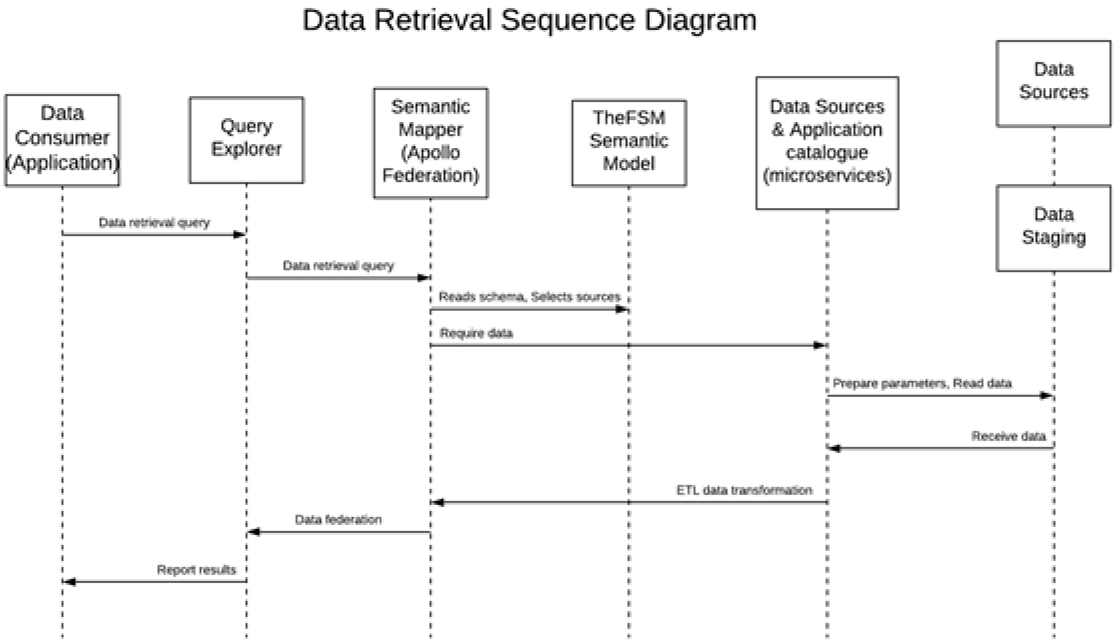

Data Retrieval Sequence Diagram
Data Consumer (Application)
Query Explorer
Semantic Mapper (Apollo Federation)
TheFSM Semantic Model
Data Sources & Application catalogue (microservices)
Data Sources
Data Staging
Data retrieval query
Data retrieval query
Reads schema, Selects sources
Require data
Prepare parameters, Read data
Receive data
ETL data transformation
Data federation
Report results

Figure-12 Data retrieval sequence diagram

5.2.4. Identity Management

5.2.4.1. OTNode DID Services

The **Decentralized Identifiers** (**DIDs**) are globally unique identifiers designed to enable individuals and organizations to generate self-sovereign identifiers using systems they trust, and to prove control of those identifiers (authenticate) using cryptographic proofs (for example, digital signatures, privacy-preserving biometric protocols, and so on).

A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides that it identifies. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party.

DIDs are URLs that **associate a DID subject with a DID document** allowing trustable interactions associated with that subject. Each DID document can express cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Service endpoints enable trusted interactions associated with the DID subject. A DID document might contain semantics about the subject that it identifies. A DID document might contain the DID subject itself (e.g. a data model).

A simple example of a decentralized identifier (DID):

did:example:123456789abcdefghi

A DID is a simple text string consisting of three parts, the:

- URI scheme identifier (did)
- Identifier for the DID method (the string "example" in above DID)
- DID method-specific identifier (the string "123456789abcdefghi" in above example**)**

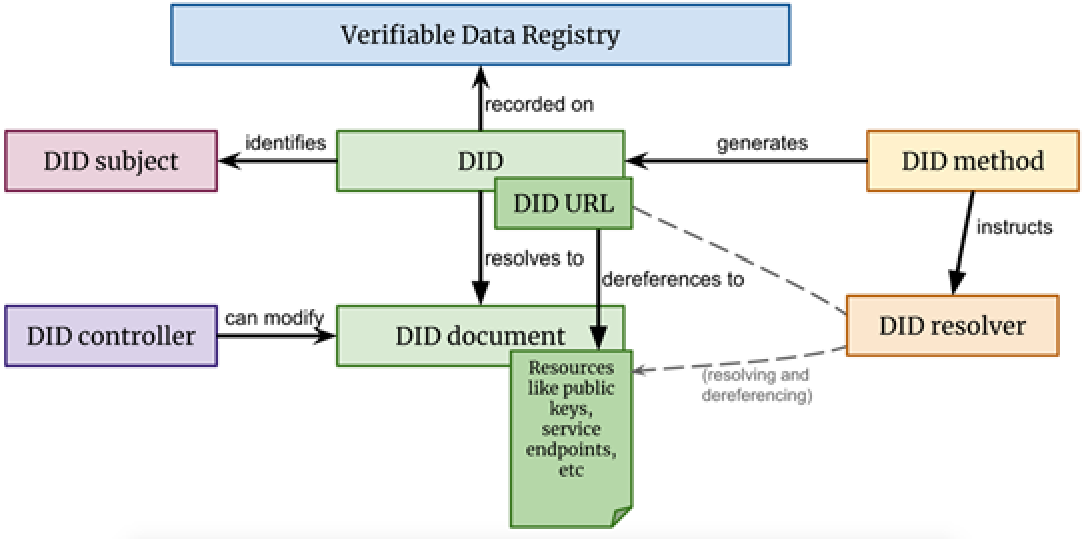


Figure-13 DID Architecture

DIDs and DID URLs

A DID, or Decentralized Identifier, is a fully qualified URI composed of three parts: the scheme "did:", a method identifier, and a unique, method-specific identifier generated by the DID method. DIDs are resolvable to DID documents. A DID URL extends the syntax of a basic DID to incorporate other standard URI components (path, query, fragment) in order to locate a particular resource.

DID Subjects

The subject of a DID is the entity identified by the DID. The DID subject may also be the DID controller. Anything can be the subject of a DID: person, group, organization, physical thing, logical thing, etc.

DID Controllers

The controller of a DID is the entity (person, organization, or autonomous software) that has the capability—as defined by a DID method—to make changes to a DID document. This capability is typically asserted by the control of a set of cryptographic keys used by software acting on behalf of the controller, though it may also be asserted via other mechanisms.

Verifiable Data Registries

In order to be resolvable to DID documents, DIDs are typically recorded on an underlying distributed system or network of some kind. Examples include distributed ledgers, decentralized file systems, databases of any kind, peer-to-peer networks, and other forms of trusted data storage.

DID documents

DID Documents describe the public keys, authentication protocols, and service endpoints necessary to initiate trustworthy interactions with the identified entity. A DID Document is a JSON-LD document that contain the following six, optional components:

- The DID that points to the DID Document, identified by the key id.
- A list of public keys identified by the key publicKey.
- Lists of protocols for authenticating control of the DID and delegated capabilities identified by the key authentication.
- A set of service endpoints, usually URLs, that allow discovery of a way to interact with the entity that the DID identifies by the key service.
- Timestamp indicating when the DID Document was created and updated for auditing the DID Document identified, respectively, by the keys created and updated.
- A digital signature for verifying the integrity of the DID Document identified by the key proof.

The DID Document is the root record for a decentralized identifier that can reference not only what's in the DID Document itself, but also any information from the service endpoints. This is accomplished by adding selectors, paths, query parameters, and fragments to the DID.

DID Methods

DID methods are the mechanism by which a particular type of DID and its associated DID document are created, resolved, updated, and deactivated using a particular verifiable data registry. DID methods are defined using separate DID method specifications.

DID Actions

DIDs are typically used between DID Controllers and relying parties (also called verifiers). The following groups of functionalities are possible with DIDs:

- **Create features** – provisioning DIDs and corresponding DID documents (done exclusively by the DID controller and according to DID method specification)
- **Delete features** – deleting DID material, performed exclusively by the DID controller
- **Update features** – the features for updating DID documents, such as rotating keys, modifying service endpoints, migration and recovery, performed by the **DID controller**
- **"Use" features** – enable presentation, authentication and cryptographic signing by the controller, and verification and auditing by the relying party (the verifier)
- **"Read" features –** corresponding to DID resolution and dereferencing, by definition performed by the relying party

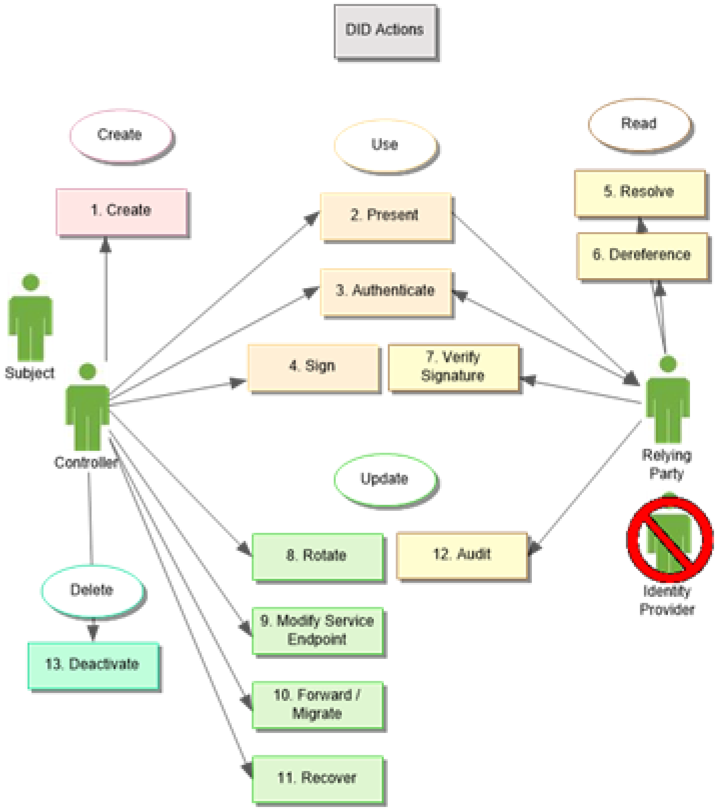


Figure-14 DID actions overview

DIDs features within TheFSM architecture are implemented through the **OTNode DID Services**: **Identity Hub**, **DID resolver** and **DLT system** components, explained further below. DIDs may be used according to the DID Auth protocol.

DIDs are utilized in conjunction with the Verifiable Credentials data model, which enable utilization of DIDs in provisioning, sharing and verification of generic verifiable claims in the below illustrated ecosystem. Verifiable credentials are cryptographically secure, privacy respecting and machine verifiable. The recommendation is to implement a verifiable credential scheme for datasets exchanged via TheFSM platform.

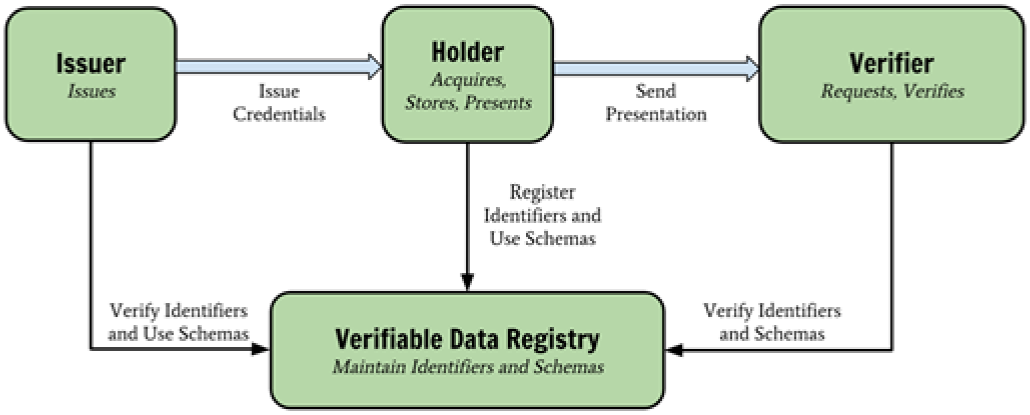

Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas

Figure-15 Verifiable Credentials ecosystem

Identifiers Registry (DIF Identity Hub)

The identity hub is used to securely store verifiable credentials. It is a datastore containing semantic data objects at well-known locations. Each object in a Hub is signed by an identity and accessible via a globally recognized API format that explicitly maps to semantic data objects. Identity hubs are addressable via unique identifiers maintained in a global namespace and are associated with the Decentralized Identifier standard described previously in the document.

A single entity (DID subject) may have one or more instances of a Hub, all of which are addressable via a URI routing mechanism linked to the entity's identifier. Hub instances sync state changes, ensuring the owner can access data and attestations from anywhere, even when offline.

DID Descriptor Objects (DIF Universal Resolver)

The DID resolver component is responsible to resolve the conforming DID documents based on the specific DID method and to verify the resolution result. By specification the DID resolver methods are implementation specific (based on the specific DLT). The DID resolution functions resolve a DID into a DID document by using the "Read" operation of the applicable DID method. DIF's Universal Resolver provides a unified interface which can be used to resolve any kind of decentralized identifier.

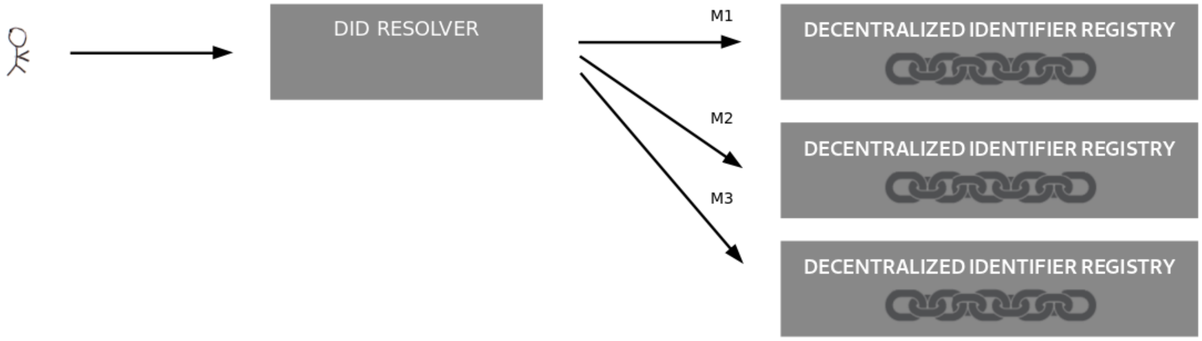

DID RESOLVER
M1
M2
M3
DECENTRALIZED IDENTIFIER REGISTRY
DECENTRALIZED IDENTIFIER REGISTRY
DECENTRALIZED IDENTIFIER REGISTRY

Figure-16 DID resolution

5.2.4.1.1. Design and Functionalities Overview

The relevant sequence diagrams for the DID provisioning and resolution are provided below:

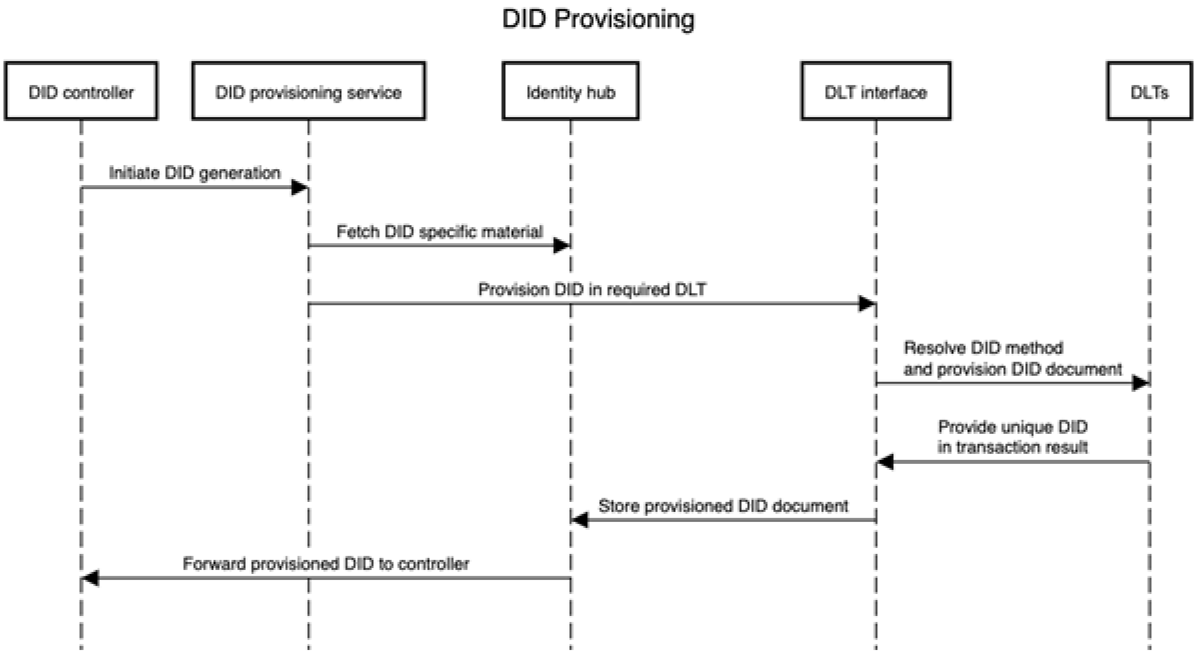

DID Provisioning
DID controller
DID provisioning service
Identity hub
DLT interface
DLTs
Initiate DID generation
Fetch DID specific material
Provision DID in required DLT
Resolve DID method and provision DID document
Provide unique DID in transaction result
Store provisioned DID document
Forward provisioned DID to controller

Figure-17 DID provisioning

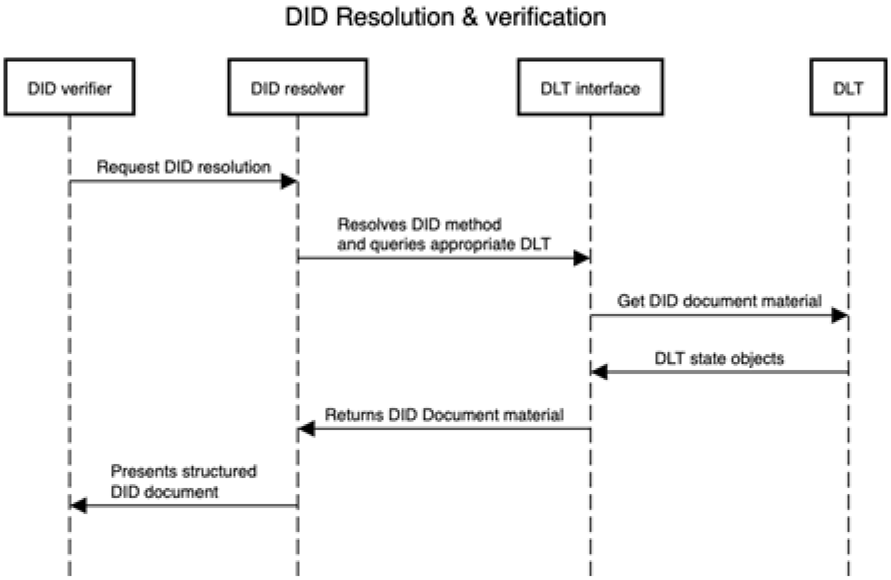

DID Resolution & verification
DID verifier
DID resolver
DLT interface
DLT
Request DID resolution
Resolves DID method and queries appropriate DLT
Get DID document material
DLT state objects
Returns DID Document material
Presents structured DID document

Figure-18 DID resolution and verification

5.2.4.2. OTNode DLT interfaces

The DLT data management interface is used to abstract the details of underlying specific DLT implementation in order to provide common functionality for the Identity hub and resolver components. It implements two generic functionalities – querying DLT state and publishing transactions, which include interactions with DLT smart contracts if the DLT implementation supports it.

The OriginTrail Network node presents an implementation of a multi-DLT interface (ODN, Ethereum, Hyperledger, and other blockchains in the future such as Polkadot) together with a supply chain data specific identity hub, storing semantic data in the standardized supply chain form (according to GS1 standards mostly). TheFSM platform will utilize OriginTrail as is for the DLT, DLT interface and Identity hub components.

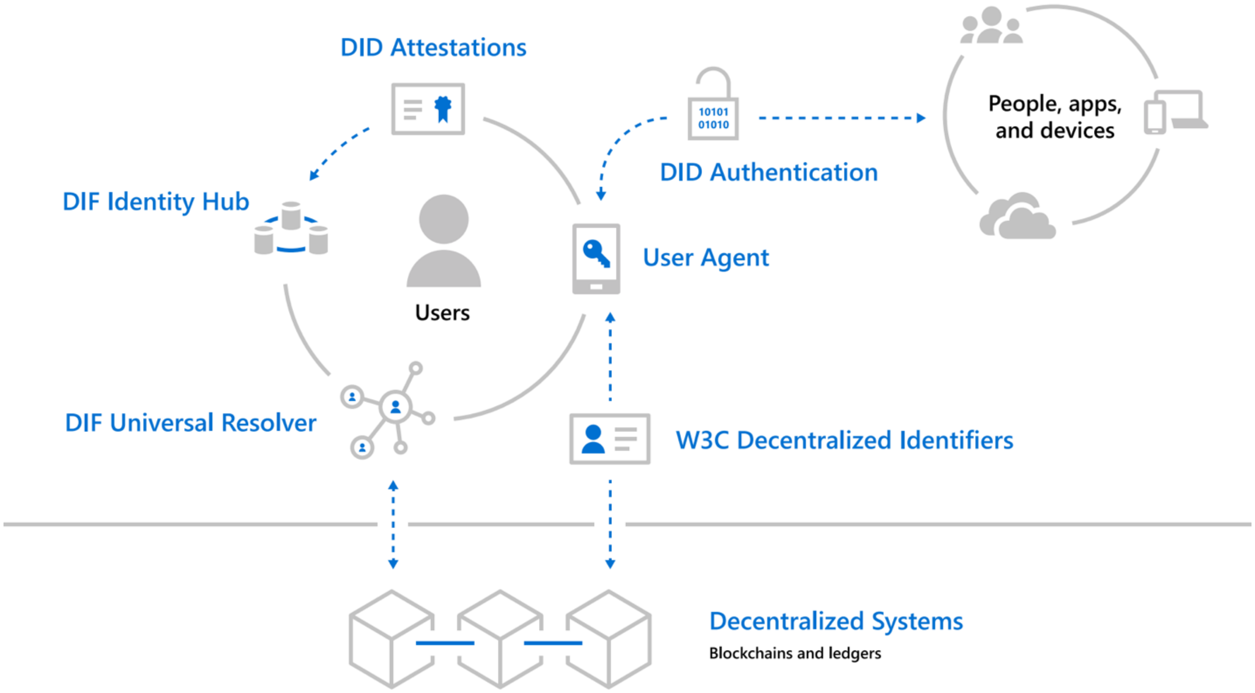


Figure-19 High level presentation of OriginTrail.

DLT

A distributed ledger (DLT stands for distributed ledger technology) is a replicated database that is consensually shared and synchronized with a specific protocol across multiple sites, institutions, or geographies, components of which are typically owned and accessible by multiple entities. The key property of DLT technology is that it is “decentralized”, meaning being maintained in such a way that no central service or authority is needed to operate the system and broker transactions between participants.

One type of DLT technology is blockchain, named by the specifics of the protocol by which data is replicated and shared between DLT stakeholders (as a series of linked, cryptographically verifiable blocks of data, hence block-chain). DLTs key characteristics are achieving high resilience and increased data integrity, which is why it has been utilized in many enterprise use cases such as supply chain visibility and trade finance.

OriginTrail is a purpose-built, open network for cross-organizational data sharing in supply chains, supported by blockchain. The OriginTrail protocol has been designed to support and grow the global linked-data-first decentralized knowledge graph (DKG) to enable interoperable, trusted data exchanges. The OriginTrail DKG is therefore growing according to emerging W3C and GS1 standards to support multiple functionalities for DIDs, verifiable credentials and enterprise data sharing, supported by consensus-enabling protocols as the trust foundation in data exchange. As such, the design of OriginTrail is based on a blockchain-agnostic approach for the long-term evolution of the technology, being able to leverage the progress of blockchain ecosystems.

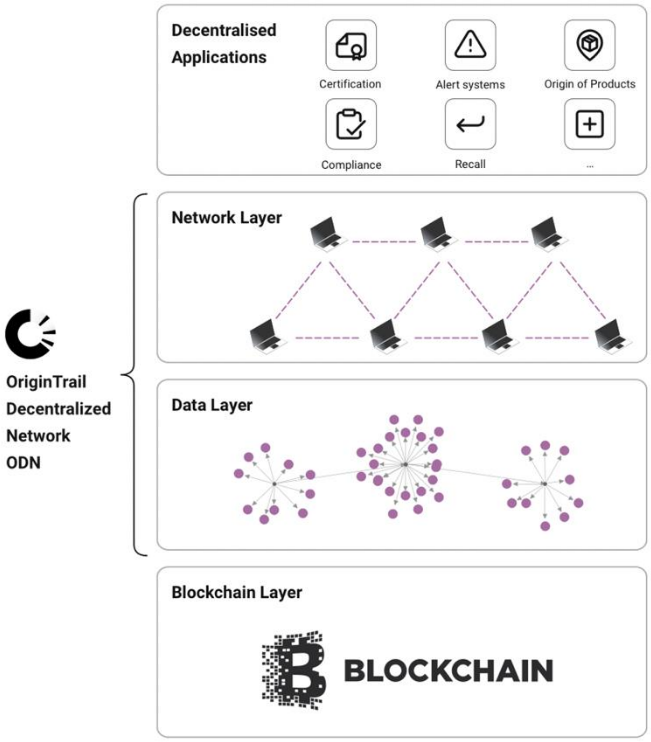


Figure-20 High level architecture of OriginTrail

5.2.4.2.1. Design and Functionalities Overview

The workflows for publishing traceability data as events and querying traceability info are presented in the next Sequence Diagrams:

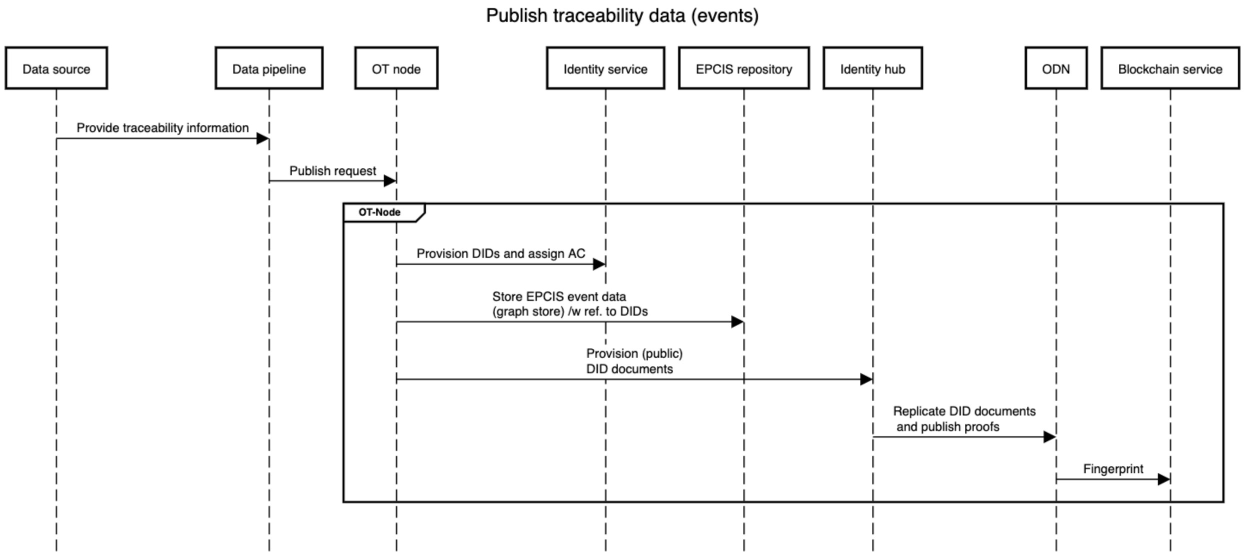

Publish traceability data (events)
Data source
Data pipeline
OT node
Identity service
EPCIS repository
Identity hub
ODN
Blockchain service
Provide traceability information
Publish request
OT-Node
Provision DIDs and assign AC
Store EPCIS event data (graph store) /w ref. to DIDs
Provision (public) DID documents
Replicate DID documents and publish proofs
Fingerprint

Figure-21 Sequence diagram illustrating the workflow for publishing traceability events.

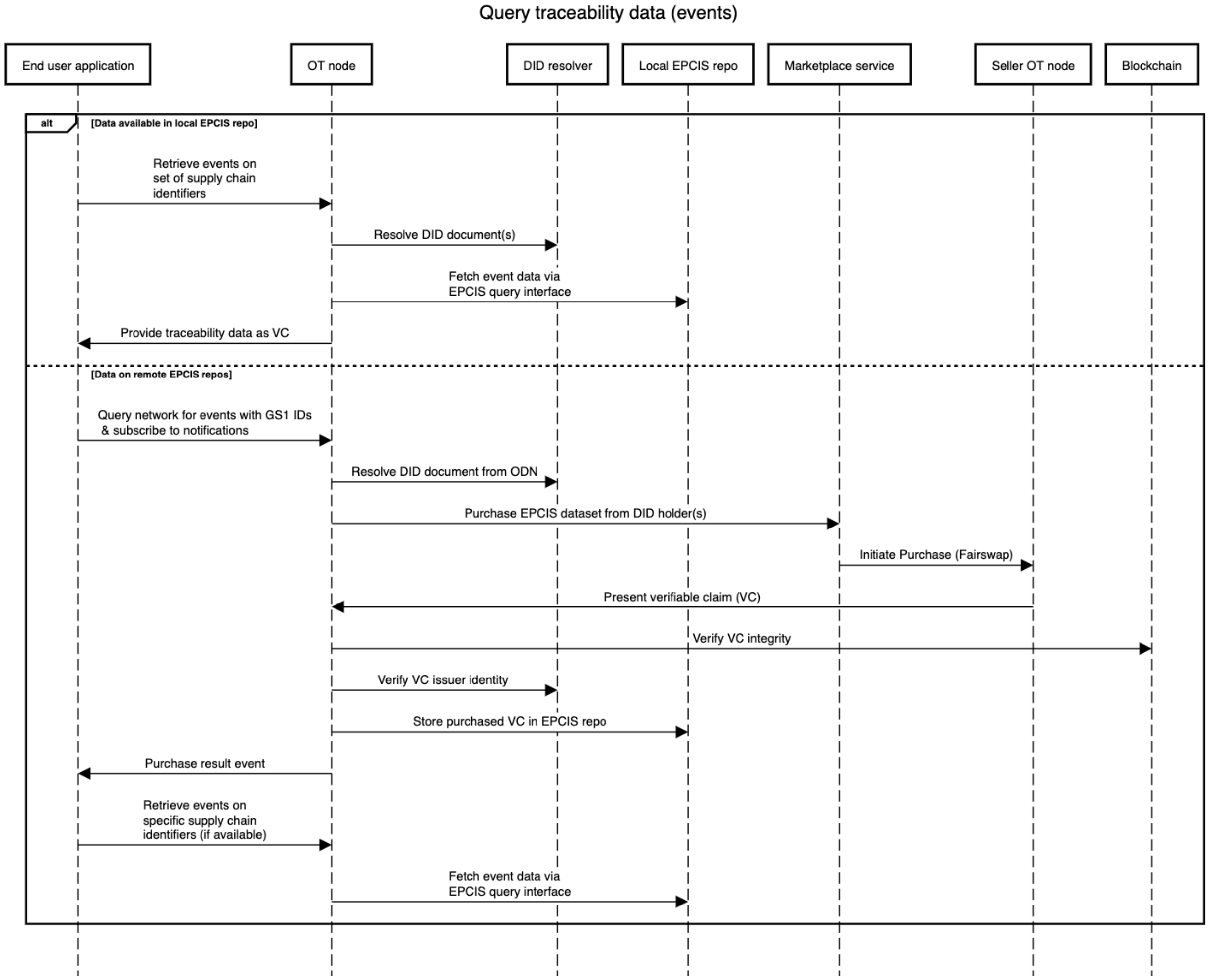

Query traceability data (events)
End user application
OT node
DID resolver
Local EPCIS repo
Marketplace service
Seller OT node
Blockchain
alt
[Data available in local EPCIS repo]
Retrieve events on set of supply chain identifiers
Resolve DID document(s)
Fetch event data via EPCIS query interface
Provide traceability data as VC
[Data on remote EPCIS repos]
Query network for events with GS1 IDs & subscribe to notifications
Resolve DID document from ODN
Purchase EPCIS dataset from DID holder(s)
Initiate Purchase (Fairswap)
Present verifiable claim (VC)
Verify VC integrity
Verify VC issuer identity
Store purchased VC in EPCIS repo
Purchase result event
Retrieve events on specific supply chain identifiers (if available)
Fetch event data via EPCIS query interface

Figure-22 Sequence diagram illustrating the workflow of querying traceability data.

5.2.5. Automated Contract Negotiation and Monetization

5.2.5.1. Data Brokerage Model

Based on the initially identified requirements, the Framework will be built on top of three core entities, namely the **Data Asset**, the **Policy** and the **Contract** and two supporting entities, namely Attributes and Terms, TheFSM defines a specific dataset from a data provider. A Data Asset, at least in the Framework's first version, corresponds to a single file which will either be already in or be easily formatted in a tabular form, i.e. comprising rows and columns or text. There is no separate entity to express the concept of DaaS, as these will be offered through sharing agreements that foresee updates and not through real-time data streams.

A Policy is the way all legal, IPR, license, quality etc. terms are expressed. Each Data Asset specifies a number of Policies which control how it can be shared and accessed. A Policy comprises a group of terms and/or attribute guarantees. Terms are specific prohibitions, permissions or obligations stemming from the above-mentioned aspects, whereas Attributes are expressions of certain facts and/or qualities, e.g. the date a Data Asset was created.

Finally, contracts represent the official data sharing agreements between a data provider and a data consumer in regard to one single Data Asset under specific Policies.

The Data Brokerage Model will be used by the Data Brokerage Engine to execute the data exchange between the two parties and will be instantiated by the Data Licence and Agreement component.

The component will be further analyzed in the second version of the architecture, as soon as, the design and the technical architecture of the security components, Data License and Agreement and identity management will be further elaborated.

Data Brokerage Engine

The data brokerage engine component is responsible for generic brokering of datasets in TheFSM platform between different parties and for possible financial compensation. The implementation of the Data brokerage engine will be based on OriginTrail protocol for data exchange, having OriginTrail nodes perform the function of the semantic store and data marketplace validation operations, interacting on the basis of smart contracts which solve the problem of fair data exchange between the dataset seller and the dataset buyer. This process is performed without reliance on a third party in between to guarantee the fair result of the transaction. The Data brokerage engine will enable the following two guarantees:

- The data seller can be **guaranteed to receive compensation** for a sold dataset
- The data buyer can be **guaranteed to receive a verifiable dataset** requested in the purchase

The OriginTrail data brokerage component implements the *FairSwap protocol*[4] with formally proven security, defined and specified by the researchers at TU Darmstadt and the University of

[4] https://eprint.iacr.org/2018/740.pdf

Warsaw. The protocol ensures a fair exchange of data for tokens, enabling a data seller to sell a digital commodity for a fixed price of tokens to the buyer.

The Marketplace FairSwap protocol is currently implemented in the form of Ethereum smart contracts, integrated together with the Ethereum identity smart contracts (conforming to the ERC725 standard, conformant to W3C DID standard) and OriginTrail protocol data replication incentivisation smart contracts. The dataset exchange is at the moment partially based on the *W3C Verifiable Credentials* framework, focusing on the broad use case of Verifiable Claims - enabling public viewing of the dataset **metadata** and **proofs**, and private storage of **data claims** which are offered for sale for a specific compensation in tokens.

5.2.5.1.1. Design and Functionalities Overview

The workflow of the FairSwap protocol which enables fair data exchange for tokens is presented in the next Sequence Diagram:

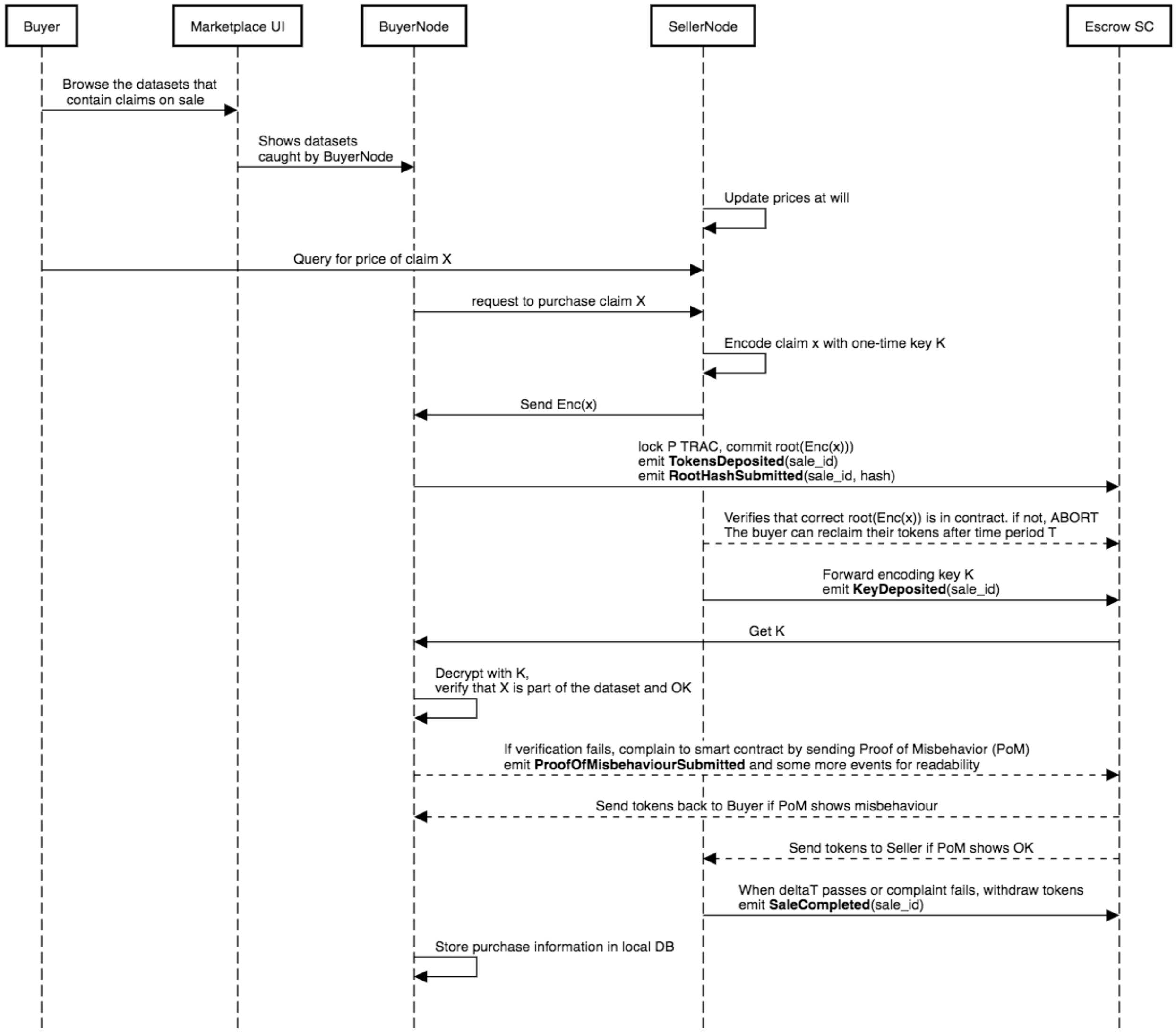

Buyer
Marketplace UI
BuyerNode
SellerNode
Escrow SC
Browse the datasets that contain claims on sale
Shows datasets caught by BuyerNode
Update prices at will
Query for price of claim X
request to purchase claim X
Encode claim x with one-time key K
Send Enc(x)
lock P TRAC, commit root(Enc(x)))
emit TokensDeposited(sale_id)
emit RootHashSubmitted(sale_id, hash)
Verifies that correct root(Enc(x)) is in contract. if not, ABORT
The buyer can reclaim their tokens after time period T
Forward encoding key K
emit KeyDeposited(sale_id)
Get K
Decrypt with K,
verify that X is part of the dataset and OK
If verification fails, complain to smart contract by sending Proof of Misbehavior (PoM)
emit ProofOfMisbehaviourSubmitted and some more events for readability
Send tokens back to Buyer if PoM shows misbehaviour
Send tokens to Seller if PoM shows OK
When deltaT passes or complaint fails, withdraw tokens
emit SaleCompleted(sale_id)
Store purchase information in local DB

Figure-23 Sequence diagram illustrating the FairSwap protocol.

5.2.6. Security and Access Control

This subsection is dedicated towards describing two important technologies which are utilized in unison, in order to ensure proper authentication and authorization when accessing resources throughout TheFSM platform. The first, ABE (Attribute based encryption) addresses the issue of encrypting documents and data according to a set of attributes, while ABAC (Attribute-Based Access Controller) addresses the authorization aspect of accessing resources, based on both environmental and user-specific attributes. The two technologies will be integrated with each other in the future and we will thoroughly document this process.

5.2.6.1. Attribute Based Encryption

ABE (Attribute-Based Encryption) is basically a promising new technique to encrypt data *without having to know the users beforehand*. The idea is that it encrypts a file using an access policy which specifies the attributes a user should be entitled to before being able to decrypt a file. A great advantage of this approach is that the owner can encrypt data based on desired attributes set, therefore allowing more fine-grained control. However, it should be noted that ABE is only applicable for data sources which are persisted in an encrypted form; it cannot work on dynamic data.

Ideally, an ABE mechanism should be scalable and offer symmetric key encryption. Also, it is important to allow multiple independent authorities to issue attributes, a necessary trait to have for a platform such as TheFSM which involves multiple sources. Another key aspect ABE should provide is scalability, which is yet another very desirable trait for the purposes of this project. Many ABE schemes have been proposed, such as FAME[5], DAC-MACS [6], RD-ABE [7] yet it is hard to guarantee all these conditions in a single implementation. Our approach will be based on a hybrid of CP-ABE and SSE (Symmetric Searchable Encryption), aiming to offer a good compromise between the strengths and weaknesses of all approaches and trying to cover all aspects as much as possible.

The protocol works as follows: A farmer ui wants to encrypt a message m containing sensor data so that it can only be read by a lab expert or read by an inspector belonging to the Certification Body. The so-called policy $\mathcal{P}$ that will be used to encrypt the file is therefore: *isLabExpert*() OR (*isPartOfCertificationBody*() AND *isInspector*()).

ABE allows a data owner u_{i} to encrypt a message m into encrypted message ct. User ui should now be able to share ct with anyone, as ABE only allows authorized users to recover the original message m by decrypting ct. Therefore, if encrypted using ABE, ct can be sent to the users who should receive it, but it can just as easily be hosted somewhere online using a CSP (Cloud Service Provider).

In general, in ABE schemes there is no need for u_i to stay online during the decryption phase, which can be quite useful in certain use cases. Such a use case might, for example, be that the Certification Body suspects foul play in some food data and wants to immediately inspect them. Someone who is entitled these two attributes (isCertificationBody(), isUnderSuspicionForFoulPlay()) is able to retrieve the secret key which it can use to decrypt ct to obtain message m. ABE does not specify, when encrypting a message, which users should be able to decrypt the ciphertext and instead specifies which attributes a user should have before being able to decrypt a ciphertext. This means that data can also be decrypted by users that will become entitled to those attributes after the original message was encrypted.

ABE was mentioned for the first time in [8], although more formal definitions were given by Goyal et al. [9] KP-ABE and Bethencourt et al. [10] CP-ABE. Basically, every CP-ABE scheme at least consists of four algorithms (which are similar to the algorithms used in Fuzzy Identity-Based Encryption), namely .Setup(), .Encryption(), .Key Generation() and .Decryption(). The following descriptions of the different sub algorithms were inspired by the descriptions in the paper by Bethencourt et al. [9] and some notations are changed for the sake of consistency:

- **.Setup()** - This algorithm takes no input other than the implicit security parameter. It outputs the public parameters PP and a master key MK.
- **.Encryption()** - This algorithm takes as input the public parameters PP, a message m and an access policy $\mathcal{P}$ over the universe of attributes. A ciphertext ct is generated from m and the access policy $\mathcal{P}$ is embedded into ct.
- **.Key Generation()** - This algorithm takes as input the master key MK and a set of attributes Sα. It outputs a private key SK.
- **.Decrypt()** - This algorithm takes as input PP, ct and SK. If Sα satisfies access policy $\mathcal{P}$ the algorithm is able to decrypt ct and returns message m.

Access policies in ABE are usually expressed as Boolean formulas, for example $\mathcal{P}$ = (α_1 OR α_2 AND α_3), where α_i denotes a specific attribute. The example formula describes an access policy ($\mathcal{P}$) where a user should be able to decrypt data, encrypted with policy $\mathcal{P}$, if it is entitled to α1 or if it is entitled to α2 and α3. Any Boolean formula can be transformed into a binary Boolean formula in an easy manner. For example, $\mathcal{P}$ can be transformed into $\mathcal{P}$ = (α_1 OR (α_2 AND α_3)) (if binary operators are assumed right associative). $\mathcal{P}$ can now be expressed as a graph (shown in Figure-24). A more tangible example might be where α_1 denotes someone being a lab expert (*isLabExpert* ()) and α_2 and α_3 denote someone being in the Certification Body (*isPartOfCertificationBody* ()) and being an inspector (*isInspector* ()). The farmer's data now is encrypted using these attributes and only lab experts or inspectors who are part of the Certification body. If the attributes of a user or a subset of them together adhere to the policy, meaning that the Boolean formula evaluates to true, the combination of those attributes is called 'accepting'. Current ABE schemes make use of a LSSS (Linear Secret Sharing Scheme) to reconstruct a secret based on a certain amount of shares a user holds, but the details of this process will be omitted to keep the description in a higher level. In a nutshell, it can be thought of as a transformation from/to a linear matrix which encodes the entire tree and Boolean operators.

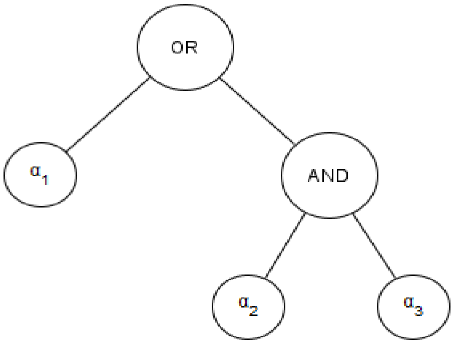


Figure-24 Boolean representation of an example access policy.

In its core functionality for TheFSM, ABE should allow a user to upload data, encrypt it using a hybrid ABE/SSE scheme, and then another user with proper attributes should be able to decrypt the data. This is of particular interest to TheFSM, as food data of importance can be properly encrypted and safely stored in the cloud (which can be untrusted and the data will still be secure), while data with the intention to be solved can also be protected that way.

Design and Functionalities Overview

Having covered the basics, we can now begin describing a high level of the proposed architecture for ABE. The key components are the following:

- **Cloud Service Provider (CSP)**: One of the common models of a cloud computing platform is Infrastructure-as-a-Service (IaaS). In its simplest form, such a platform consists of cloud hosts which operate virtual machine guests and communicate through a network. Often a cloud middleware manages the cloud hosts, virtual machine guests, network communication, storage resources, a public key infrastructure and other resources. Cloud middleware creates the cloud infrastructure abstraction by weaving the available resources into a single platform. In our system model we consider a cloud computing environment based on a trusted IaaS provider. The IaaS platform consists of cloud hosts which operate virtual machine guests and communicate through a network. In addition to that, we assume a Platform-as-a-Service (PaaS) provider that is built on top of the IaaS platform and can host multiple outsourced databases. Furthermore, the cloud service provider is responsible for storing users' data. Finally, the CSP must be TEE (Trusted Execution Environment) enabled since core entities of the protocol will be running in a trusted execution environment offered by SGX.
- **Master Authority (MS)**: MS is responsible for setting up all the necessary public parameters that are needed for the proper run of the underlying protocols. Furthermore, MS is responsible for generating and distributing ABE keys to the registered users. Finally, MS is considered as a single trusted authority. Thus, we assume that MS is TEE-enabled and is running in an enclave called the Master Enclave.
- **Key Tray (KeyTray)**: KeyTray is a key storage that exists in the CSP and stores ciphertexts of all the symmetric keys that have been generated by various data owners and are needed

in order to decrypt data. Every registered user can contact the KeyTray directly and request access to the stored ciphertexts. Furthermore, the symmetric keys are encrypted with a CPABE scheme. Thus, a single symmetric key is encrypted only once and users with certain access rights and different keys are able to access it (i.e. decrypt it). Moreover, similar to MS, KeyTray is also TEE-enabled and is running in an enclave called the KeyTray Enclave.

- **Revocation Authority (REV)**: REV is responsible for maintaining a revocation list (rl) with the unique identifier of the users that have been revoked. At this point it is worth mentioning that a single user might own more than one CP-ABE secret key. Therefore, rl maintains a mapping of users with the CP-ABE keys they own. Every time that a key of a user is revoked, REV needs to update rl. This, as we will see later, will prevent revoked users from accessing ciphertexts that are not authorized anymore. Similar to MS and KeyTray, REV is also TEEenabled and is running in an enclave called the Revocation Enclave.
- **Registration Authority (RA)**: RA is responsible for the registration of users in the CSP. Additionally, RA has a public/private key pair denoted as pkRA/skRA. RA can run as a separate third party but can be also implemented as part of the CSP. The registration process is out of the scope of this paper. Thus, we will not describe how the registration of a new user takes place. Instead, we will assume that a user has already registered and has access to the remote storage and the services offered by the CSP.

Putting all the components together, the architecture can be summarized in the figure below (Figure-25):

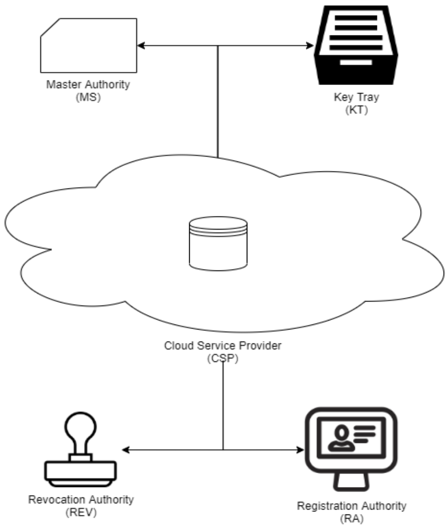


Figure-25 ABE architecture components

Finally, we describe the proposed protocol:

- **.Setup()**: Each entity from the described system model obtains a public/private key pair (pk, sk) for a CCA2 secure public cryptosystem and publishes its public key while it keeps the private key secret. Apart from that, all three entities that are running in an enclave generate a signing and a verification key. Furthermore, MS runs CPABE.Setup and generates a master public and private key. The following key pairs are generated:

  - (pk_{CSP}, sk_{CSP})- public/private key pair for the cloud service provider.
  - (pk_{MS}, sk_{MS}), (sig_{MS}, ver_{MS}), (MPK, MSK)-public/private, verification/signing and master key pairs for the Master Authority.
  - (pk_{KT}, sk_{KT}), (sig_{KT}, ver_{KT})- public/private and verification/signing key pairs for the KeyTray.
  - (pk_{REV}, sk_{REV}), (sig_{REV}, ver_{REV})- public/private and verification/signing key pairs for the Revocation Authority.
- **.ABEUserKey()**: This phase is taking place between a registered user u_i that wishes to obtain a CP-ABE key and MS who is responsible for generating such keys. This is a probabilistic key-generation algorithm that runs in the master enclave and takes as input MSK, the identity of the user that is requesting a key and a list of attributes A that is derived from user's registered information. More precisely, u_i contacts MS and proves that she is a registered user. Then, attests MS and requests a new CP-ABE key. MS then runs CPABE.Gen and generates $_{skA,}$. This is then sent back to the user over a secure channel.
- **.Store()**: After a successful registration, we assume that u_i has received a valid credential ($cred_i$) that can be used to login to a cloud service offered by the CSP. Additionally, u_i is now able to store data to the cloud storage. The user u_i communicates with CSP so that they both verify the integrity of each other, then the user uploads the encrypted data to CSP, an operation which also yields a collection of ciphertexts and an encrypted index.
- **.KeyTrayStore()**: A key storage algorithm that allows an already logged-in user to safely store a symmetric secret key K_i, that generated earlier, in the Key-Tray. This is a probabilistic algorithm that takes as input a symmetric key K_i, MPK and a policy P and outputs an encrypted version of K_i which is associated with P. Also, the KeyTray generates a random number pK_i encrypts it with r_{ki} and stores it next to c_r^{Ki} which is needed to later prove ownership when revoking.
- **.KeyShare()**: Enable user to share a key they stored to other users (let's say u_j for the example). Note that the original user needs not be involved during this operation. If user u_j has not been revoked, they are then checked for validity against the KeyTrayStore. If they are still valid, u_j's private key is used to obtain K_i.
- **.Search()**: Allow search over the ciphertexts that have been encrypted with K_i, for a specific keyword *w*. Upon verifying time of request *t* and user u_j's identity, a search token is issued, with which the user will obtain a sequence of file identifiers I_w. Using the sequence and K_i , the user can then obtain the files which contain keyword *w*.
- **.Update()**: This operation updates existing files, *without requiring to reupload the newer version* (which would be a bad idea). User u_j generates a token and sends it to CSP, which in turn returns the updated encrypted index and an updated sequence of ciphertexts.
- **.Delete()**: User issues a delete token. If they have not been revoked, their timestamp is valid and they have the proper attributes for the operation, the file is deleted and the encrypted index and sequence of ciphertexts are updated.

- **.Revoke()**: After validating data owner u_i, REV recovers r_{ki} (from KeyTray), then forwards it to u_i, who in turn signs r_{ki} and sends it back to KeyTray. After validating u_i, KeyTray notifies REV to proceed. REV adds u_j in rl (revocation list), denying them further access to the file.

The interactions between the subcomponents in order for a (new) user to upload a new file are presented in the sequence diagram, below (Figure-26):

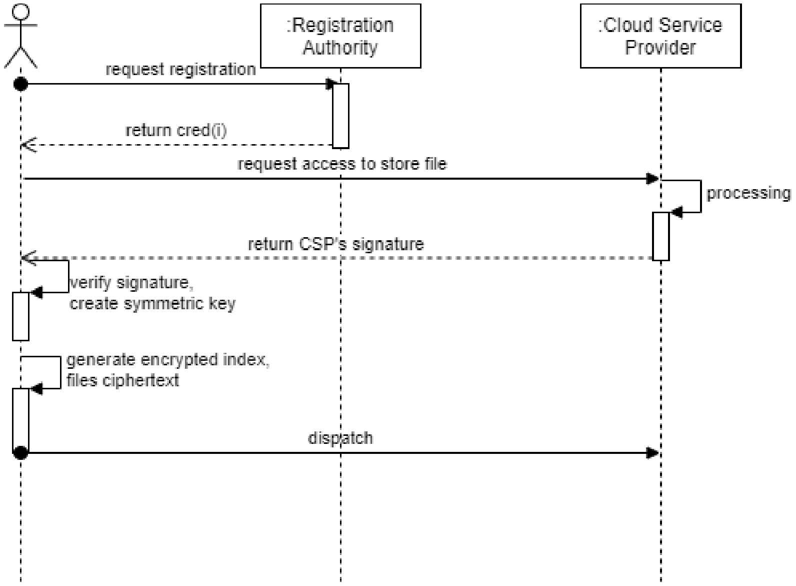


Figure-26 File upload

The interactions between the subcomponents in order for a user to request a new key are presented in the sequence diagram, below:

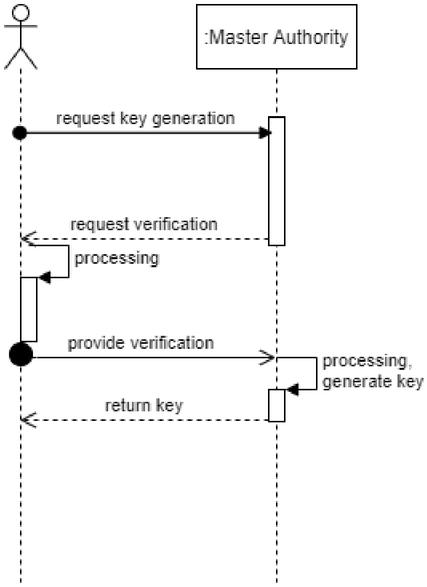


Figure-27 Request new key

5.2.6.2. *Authorization & Access Control Engine*

The Authorization & Access Control Engine is the component providing the authorisation engine that implements the access control mechanisms within the TheFSM platform. The purpose of the Authorization & Access Control Engine is to provide the logical access control that prevents the unauthorised access of any type of resource of the TheFSM platform such as data, services, tools, any kind of system resources, as well as all other relevant objects.

In general, access to resources refers to discovering, reading, creating, editing, deleting, reserving and executing resources (NIST, 2014). The realisation of the access control is performed by a set of access control policies. An access control policy describes the list of operations that can be performed on the resources, by whom and in which context. As such, the access to a specific resource depends on the condition if the subject requesting access on this specific resource is satisfying the corresponding policy or not. If the policy is satisfied, the access to the specific resource is granted for the subject, otherwise the access is denied.

In order to perform access control a variety of Access Control Mechanisms (ACM) are available with aim of the realization of the various logical access control models that exist. Each model proposes a security framework along with a set of conditions that define how the objects, subjects, operations and rules can be combined in order to form the access control decision that will either grant or deny the access to the requestor. The most widely-used ACMs are the Discretionary Access Control (DAC) (Lathan, 1986), the Mandatory Access Control (MAC) (Lathan, 1986), the Identity Based Access Control (IBAC), the Role Based Access Control (RBAC) (Ferraiolo et al, 2013) and the Attributed Based Access Control (ABAC) (Hu et al, 2015). Within the context of TheFSM, the ABAC model will be adopted and implemented by the Policy Manager.

The ABAC model defines an access control mechanism in which access rights are granted to users through the use of policies in which attributes are combined together. While IBAC is based on the attribute of "identity" with access control lists (ACLs) and RBAC is based on the attribute "role" in order to form an access control decision, the differentiation of the ABAC is the concept of policies in which multiple different attributes are evaluated through a complex Boolean rule set. As such, the model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request (subject), the resource (object) and the action (operation).

According to (NIST, 2014), the ABAC is defined as "*an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.*"

Following this definition (NIST, 2014), in the ABAC model:

- **Attributes** are characteristics of the subject, object, or environment conditions. Attributes contain information given by a name-value pair.
- A **Subject** is a human user or a systemic entity, such as a device, that issues access requests to perform operations on objects. Subjects are assigned one or more attributes.
- An **Object** is a system resource for which access is managed by the ABAC system, such as devices, files, records, tables, processes, programs, networks, or domains containing or

receiving information. Anything upon which an operation may be performed by a subject can referred as an object.

- An **Operation** is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, copy, execute or modify.
- **Policy** is the representation of rules that makes it possible to determine if a requested access should be allowed, given the values of the attributes of the subject, object, and possibly environment conditions.

Within this definition, environmental conditions are considered the operational or situational context in which access requests occur. As such, environmental conditions are detectable environment characteristics. Environment characteristics are independent of the subject or object, and may include the current time, day of the week, location of a user, or the current threat level.

The execution flow of any ABAC-compliant access control system is depicted in Figure 16. In step 1, the subject initiates an access request in order to perform a specific operation on a specific object. In the following steps, the Access Control Mechanism consults a policy repository to obtain the rules related to the requested object (step 2a), retrieves the subject's (step 2b) and the object's attributes (step 2c), as well as the Environment Conditions (step 2d) in order to determine if the access will be granted or denied.

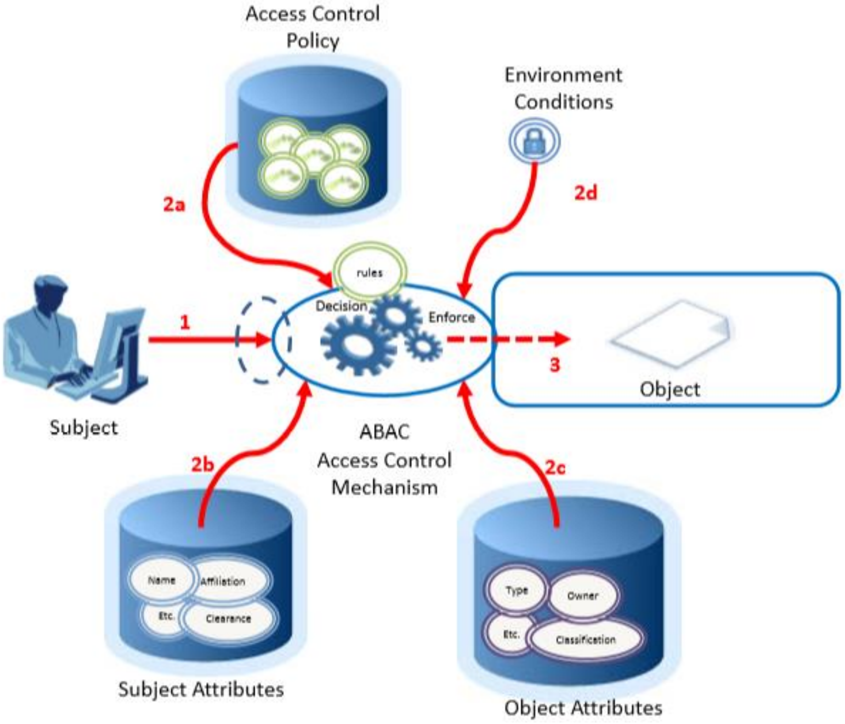


Figure-28 Authorization & Access Control Engine (ABAC-based) execution flow (Source: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf)

5.2.6.2.1. Design and Functionalities Overview

ABAC is an access control model and not a normative standard, as such it has many reference implementations. Within the context of TheFSM, we opt for one of the most dominant reference implementations, which is the eXtensible Access Control Markup Language (XACML). XACML is a standard provided by the Organization for the Advancement of Structured Information Standards (OASIS). XACML was selected as it offers separation of the authorization functionality from any proprietary environment, attribute and policy management, as well as operational efficiency. Additionally, XACML is also widely recognized by both the research and vendor communities and is adopted in multiple industries. The acceptance of XACML is also evident by the increasing number of implementations of XACML available as product offerings by several software vendors. In order to facilitate the implementation of the XACML standard, the Policy Manager is composed by five main internal sub-components as per the XACML specification, namely the **Policy Enforcement Point (PEP)**, the **Policy Decision Point (PDP)**, the **Policy Information Point (PIP)**, the **Policy Administration Point (PAP)** and the **Context Handler** with the following main functionalities:

- The PEP is the interface that intercepts all the access requests originating from the subjects, provides the request to Context Handler for processing and denies or allows the access based on the access control result.
- The Context Handler is the entity that translates the access requests from the native request format to valid XACML requests and send them to PDP for actual access decision making. Additionally, it coordinates with PIP for the attribute collection as request by PDP.
- The PDP is the XACML main decision point for all access requests utilising the information provided in the XACML request and the rules set in the policy in order to yield a decision. Furthermore, it utilizes the Context Handler in order to retrieve the relevant attributes for the policy evaluation.
- The PIP is used by the Context Handler in order to retrieve all the necessary attributes for the policy evaluation as requested by PDP from several external or internal actors.
- The PAP is the sub-component responsible for managing the policies through a dedicated interface or API which are stored in the repository. Moreover, PAP is responsible for providing the policies to PDP upon request.

The **main functionalities of the Authorization & Access Control Engine** are as follows:

- Provide the access control mechanism that is based on the ABAC model and the XACML reference implementation that will be used as the authorisation engine of the TheFSM platform.
- Control and restrict the access of any type of resource of the TheFSM platform based on the set of access control policies that are managed and maintained within the access control mechanism.
- Provide the interfaces that will manage and process any access request in order either grant or deny the access to the requestor.

The core subcomponents of the Authorization & Access Control Engine are:

- **Access Policy Management**: It provides a policy administration point and is responsible for validating an access request against the specified policies. The component provides an

API and a user interface for the definition and the management of the policies that need to be applied to a specific dataset.

- **Policy Enforcement Business Logic**: Issues native requests for accessing the data and receives responses for accessing the dataset. It also receives and forwards the final access response to the requestor. If access is permitted, then the subcomponent permits access to the resource; otherwise, it denies access.
- **Access Request Transformation Handler**: It transforms the native access request to the internal format and reconstructs the request by extending it with additional attributes provided necessary for the validation of the relevant access policies rules.
- **Attributes Handler**: It collects the requested additional attributes which are needed in order to validate an access policy. These attributes include the attributes of the subjects, resource, action, environment. The subject represents any user or organization that has been uniquely identified and authenticated. The resource refers to the dataset, the action consists of the operations to be performed on the resource (eg. read-only, write, download etc.) while the environment refers to the current state of the system's environment, the current session of a user etc.

The interactions between the subcomponents as well as TheFSM platform are presented in the sequence diagram, below:

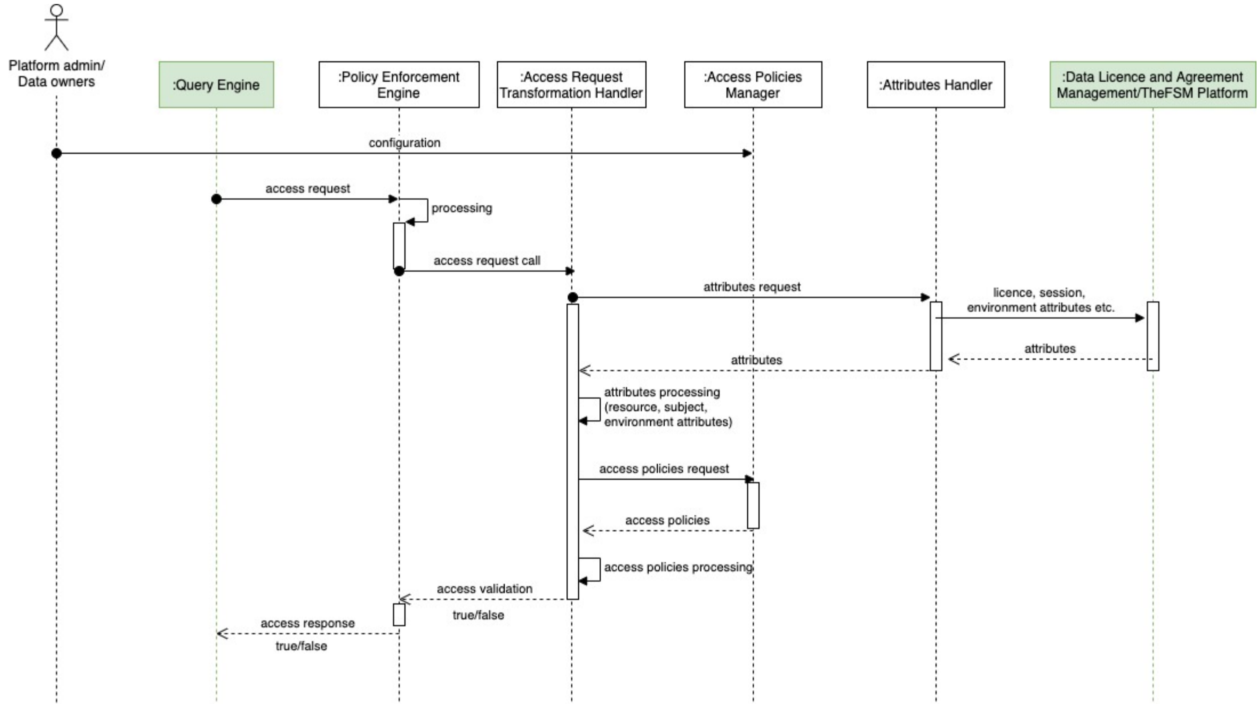

Platform admin/ Data owners
:Query Engine
:Policy Enforcement Engine
:Access Request Transformation Handler
:Access Policies Manager
:Attributes Handler
:Data Licence and Agreement Management/TheFSM Platform
configuration
access request
processing
access request call
attributes request
licence, session, environment attributes etc.
attributes
attributes
attributes processing (resource, subject, environment attributes)
access policies request
access policies
access policies processing
access validation
true/false
access response
true/false

Figure-29 A2C Engine Subcomponents

5.2.6.3. Anonymization Framework

Due to the sensitive nature of the data hosted on TheFSM, it is paramount to provide pseudonymisation and anonymisation capabilities. Pseudonymisation refers to procedures where sensitive data are mapped to generic values, so that they can be protected, while anonymization maps sensitive data to generic, random values. Assuming "X" was originally ID=3, the main difference lies in the fact that with the former it is still possible to deduce that "X" refers to the same information every time "X" is encountered, while the latter can map 3 to "X", "Y", "Z" for every time it is encountered throughout the text.

Pseudonymisation obviously exposes some knowledge about the original data, however this can be useful. For example, risk estimation can take into consideration sensitive data about companies which are pseudonymized and conduct a thorough analysis, without ever exposing their identities.

5.2.6.3.1. Design and Functionalities Overview

The initial approach for FSM is the utilization of pseudonymisation, which can then be adapted into full anonymization, should the needs of the project require it.

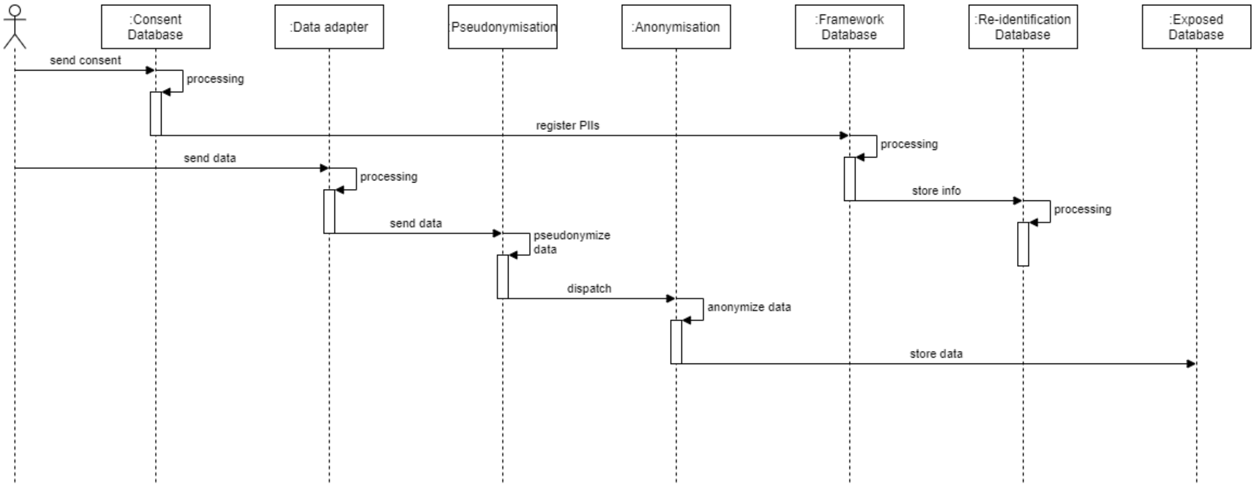


Figure-30 Pseudonymisation/Anonymisation process sequence diagram

The Anonymisation component is responsible to implement the pseudonymisation and anonymisation of the platform data. The component includes the following sub-components:

Consent database: A database which stores the data subjects who have provided consent to the TheFSM platform.

Framework database: A database which contains the PIIs (Personally Identifiable Information) of all the data subjects.

Re-identification database: A database which contains the original data of the data subjects or other data which can be used to match the pseudonymised (or anonymised) data to the data subjects. These data need to be pseudonymised (or anonymised) and their access is restricted only to the authorised personnel.

Exposed database: A database which contains the pseudonymised data which are accessed and disseminated to the various parties which use TheFSM.

Pseudonymisation: A component which will perform pseudonymisation transformations on the data.

Anonymisation: A component which will anonymise the data.

Data adapter: A software component which is responsible to implement the pseudonymisation of the data.

The pseudonymisation process is briefly described below:

When collecting personal data, the Data Adapter will query the Consent database and the Framework database. The consent database will have stored a map of all subjects that have provided consent to TheFSM. The Framework database will contain the PIIs of all data subjects. If confirmation from the consent or the framework database occurs, the Pseudonymisation Module will perform pseudonymisation on the data; it will store the pseudonymised data in an open dataset that can generally be accessed by parties being in communication with TheFSM and will store the re-identification data in a separate database; the Re-identification database. The Re-identification database will not be publicly accessed but will be used and maintained by each of the data controller's users. When re-identification is needed at run-time (e.g. when the e-mail of a user needs to be verified), the Pseudonymisation Module will communicate with the Re-identification database to obtain the original data; apart from this case, access to the re-identification database will be restricted.

After storage, an extra *Anonymisation* module will provide the functionality of generating anonymised data from the exposed data set. The implementation of the anonymisation module will be based on the **ARX Framework**[5] and will produce a data set with high *k-value*, *l-diversity* and *t-closeness* parameters. In case the platform operator imports a population table, the *Anonymisation* module will also produce a low value of *δ* (for the specifics of *k-value, l-diversity, t-closeness* and *δ-difference*. The anonymised data set will contain all useful information regarding user actions and cases and can still be used to compute analytics and provide useful feedback. Since data subjects cannot be de-identified from the anonymised data set, it can be stored or archived regardless of the status of consent forms.

In case that a subject is removed from the framework database or a consent is revoked, the Pseudonymisation Module will remove for this subject the re-identification data form the re-identification database. The pseudonymised data will be automatically converted to anonymous data upon this removal, so they can still be stored in the Exposed database. Upon revocation of consent, the deletion of re-identification data may take some time due to the system having to poll the consent database and the technical expert receiving the notification to delete re-identification data. This will be explicitly noted in the consent form.

[5] https://arx.deidentifier.org/

The *Pseudonymisation* module will perform a combination of techniques. The administrator of the platform will be able to define which transformations are needed to ensure proper pseudonymisation or anonymisation.

The set of transformations offered will consist of both one-way hashes[6] and two-way encryption (possibility to encrypt and decrypt the data) as well as all the data masking techniques, except from shuffling. The reason that shuffling is excluded is because it couples data of multiple subjects. If one subject revokes consent, it is difficult to undo the transformation without affecting data corresponding to other subjects.

5.2.7. Data Marketplace and Added Value Services

A value-added service (VAS) is a popular telecommunications industry term for non-core services, or, in short, all services beyond standard voice calls and fax transmissions. However, it can be used in any service industry, for services available at little or no cost, to promote their primary business. In the competitive markets, these services have a significant importance. For instance, in terms of revenue, these services provide a significant amount of money to telecom companies by enabling them to upturn average revenue per user.

On the other hand, they enable operators to establish customers' loyalty. Customers are attracted to platforms companies that offer more VASs. These services also make customers happy. And, customers are more likely to continue using services of the company that makes them happy. Thus, these services play a significant role in ensuring customer satisfaction and retention.

For TheFSM, a main goal is to provide a set of added value services to empower the food safety and certification industry which will address: a) Provision of data to stakeholders through intelligent query engine, b) Data sharing and monetization services, c) Traceability data services, d) support the analytics algorithms workflow design and execution, by making the best known and widely accepted algorithms in the food safety and certification industry available, so as to allow all related stakeholders to analyse and visualize results downstream of big data applications and generate new knowledge and insights. Providing analytics of this sort can elevate them to VAS status, as premium features TheFSM will support.

This layer will implement an API regarding the aforementioned services, aiming to provide a common, unified point of data exchange and services execution of TheFSM Data Platform. External applications, developers, end-users will be able to access, consume, exchange data and retrieve analytics.

FOODAKAI 2.0 and Agrivi 2.0 will make use of these data services in order to extend their services.

5.2.8. TheFSM Extended Applications

5.2.8.1. FOODAKAI 2.0

[6] A one-way hash function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence. Furthermore, a one-way hash function is designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way).

The FOODAKAI 2.0 application will be developed as an extension of the FOODAKAI platform and will focus on the risk prediction services for supplier assessment (verification). FOODAKAI 2.0 is based on FOODAKAI the Food Safety Data Incidents Platform (FSI Data Platform) developed by Agroknow. The Data Platform is currently used to collect, process, index (for searching) and publish the food safety incidents data. The platform includes the following components:

A data aggregation and processing methodology

A data aggregation and processing software Specifically the aggregation software includes amongst other features

a. **A data collection component** used to collect dynamically data from several official data sources
b. **A data processing component that transforms** the information to an internal rich format
c. **A data enrichment component** that adds missing terms for hazards and products using the textual information of a food safety incident
d. **A data curation environment** that allow curators to review, organise and enrich the data
e. **A data indexing and publishing component** (Data Services) that is used by the front end applications to get the data.

A dataset that is continuously updated with new food safety incidents (recalls, food import rejections, alerts) and that includes also Companies and Product Brand information.

The relevant architecture of the FSI Data Platform is provided below:

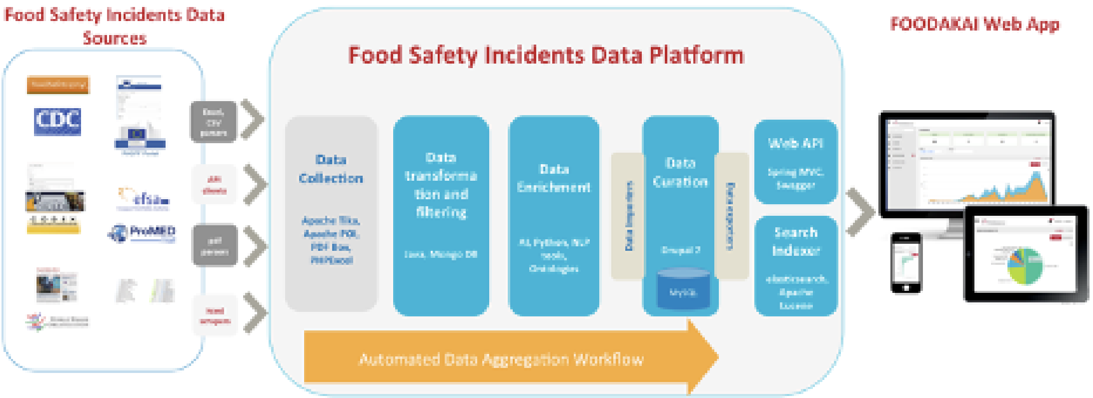

Food Safety Incidents Data Sources
CDC
efsa
ProMED
Excel, CSV parsers
API clients
pdf parsers
html scrapers
Food Safety Incidents Data Platform
Data Collection
Apache Tika, Apache POI, PDF Box, PHPExcel
Data transformation and filtering
Java, Mongo DB
Data Enrichment
R, Python, NLP tools, Ontologies
Data Importers
Data Curation
Drupal 7
MySQL
Data exporters
Web API
Spring MVC, Swagger
Search Indexer
elasticsearch, Apache Lucene
Automated Data Aggregation Workflow
FOODAKAI Web App

Figure-31 FSI Data Platform architecture

A machine learning API has been created for the enrichment of FOODAKAI's entities using machine learning techniques. This API uses 2 different models based on the annotation that will be attempted:

- one is using the title and textual description of the recall and is trained to identify the hazard which caused the recall, and

- the other one is also using the title and description of the recall and identifies products.

For both of them the SGDClassifier was used, along with a TFIDF vectorizer. This API has endpoints for the generation of the model with a new train dataset and for the identification of hazard and product terms, and is built using the Flask framework for Python. More details on the FSI Data Platform will be provided in D4.1.

The FOODAKAI 2.0 includes two main parts, a backend and a front end part. More specifically:

- The back end part includes mainly the intelligence API of the FSI Data Platform
- The front end part is developed using Ruby on Rails and ReactJS and includes all the functionalities that are provided to the end user for the supplier assessment. The application also includes a PostgreSQL database.

The FOODKAI 2.0 application will integrate with the TheFSM Platform to securely identify and exchange information relevant to the supplier that is needed for the assessment and prediction of supplier’s risk. Currently only data about the food safety incidents are used for the assessment of the supplier. The goal is to get additional information about the supplier, such as inspection results and reports, laboratory test results and certificates in order to create a risk matrix for each supplier that will help in remote verification activities.

5.2.8.2. FoodInspector

The main goal of this application is to transform the current food safety inspection process that involves paperwork and exchange of files, to a fully digital process with data assets that the inspector can click upon, interact with, and use to get prepared for an audit. The application will provide services that will allow inspectors dig deeper into data slices and combinations - such as a particular ingredients and products in a time period of interest. By having a way to dynamically dig deeper into the results of the inspection audits and the lab testing results, inspectors will be able to perform more accurate and fast assessment of all risk dimensions, in order to select the critical control point that should be of higher priority for a physical inspection. This means that the Certification Body can save time and money from unnecessary inspections and the food producer or manufacturer can avoid redundant product, device and lab testing activities.

The application will include a front end part that will integrate to the front end of FOODAKAI platform and a back end part that will rely on the data exchange services of TheFSM platform. More specifically

- The front end will be developed using Ruby on rails and ReactJS. It will implement all the functionalities that the inspectors of a Certification Body need in order to assess the risks of a company that they will audit.
- The backend will include a software module that will invoke the APIs of the TheFSM platform, to retrieve information about a food company and inspections’ outcomes. The information will include laboratory tests, previous audits, ingredients, traceability data etc.

5.2.8.3. Agrivi 2.0

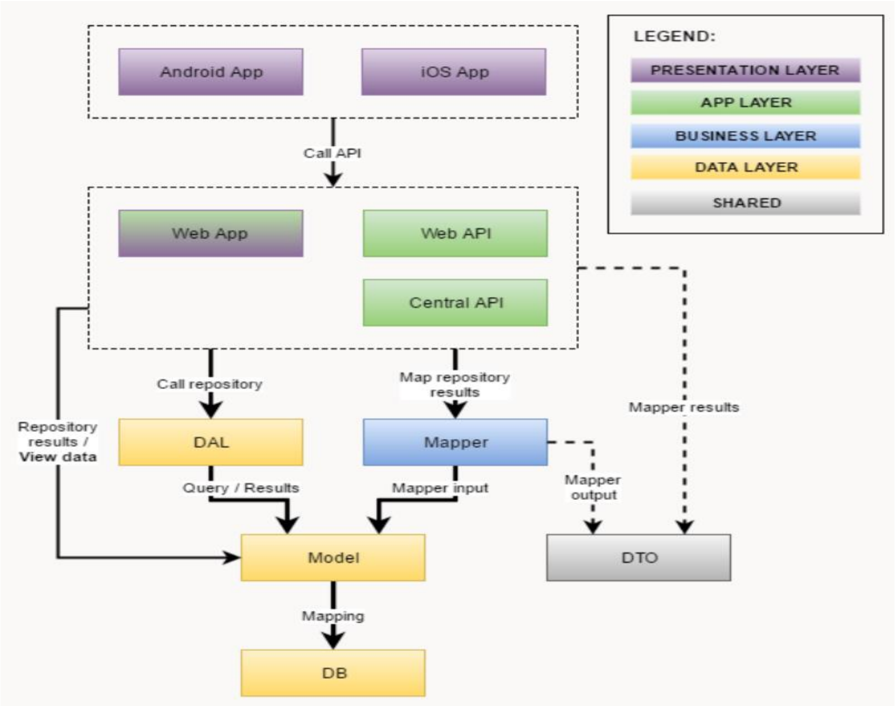
Agrivi 2.0 application is an external farm management system intended primarily for producers (farmers) and food processors that are buying the produce from producers (farmers) in the context of supplier risk assessment. Agrivi 2.0 consists of:

- Agrivi FMS platform – existing farm management platform
- Extensions for theFSM project – specific add-ons to the farm management platform that will be developed during the project focused on additional attributes and reports specific for Global G.A.P. certification process

Agrivi 2.0 farm management system will serve primarily to producers (farmers) and food processors in terms of exchanging sourced produce traceability information and applied growing practices in terms of quality standards expected by the food processors.

Goal of the farm management solution for food processing companies is to ensure complete transparency and traceability of sourced produce from farmers and to tackle key challenges faced, such as: quantity volatility from farmer to farmer, applied farming practices that affect quality requirements, lack of produce traceability throughout the vegetation season and lack of efficient collaboration with farmers.

Agrivi 2.0 will also serve consultants and Global G.A.P. certified auditors to perform a virtual and efficient auditing process for farmers based on the farm data available in reports within the farm management system of the farmer. Agrivi architecture and its components is presented in the diagram, below:



Figur-32 AGRIVI's high-level architecture

AGRIVI's interaction and integration points with TheFSM will be implemented through an API.

6. INTEGRATION APPROACH

6.1. Integration Plan

The development of the data curation and semantic enrichment components, as well as, the core backend components related to security (A2C engine and ABE) and secure storage are planned to be developed and integrated first since they are required from a wide number of the requirements and the rest of the components. More specifically, the first prototype of the data services and the A2C engine are under development, while their implementation will be continued until M12. The distributed identity management, the OTN traceability data management, as well as, the data processing and analysis services are under development and the relevant integration services are expected to start on M11. The extended services of the identity management, blockchain abstraction, and the marketplace smart contracts and data brokerage will build on top of the previous results and their implementation will due until and after M12 and will be delivered after M12, in the second version of TheFSM Platform. The new application design of FOODAKAI 2.0 has already provided a first prototype which is already being demonstrated to a set of end users. The first version of TheFSM Platform is expected to integrate with FOODAKAI 2.0 and Agrivi 2.0 only for data consumption and semantic enrichment. The first integration activities for the first version of TheFSM Platform are foreseen to begin by M11.

7. CONCLUSIONS

The purpose of the current deliverable at hand was to deliver the user requirements and the technical requirements of TheFSM, as well as to deliver the first version of the conceptual architecture of the TheFSM platform.

At first, TheFSM agile development methodology was presented, describing all the processes, instruments, roles and methods that are adopted in all the phases of the development of TheFSM platform. Within this methodology, the User Stories definition was clearly defined providing all the guidelines and the additional management information that were used as a guidance during the process. Moreover, the requirements definition in terms of key characteristics and requirements classification was presented, along with the TheFSM stakeholders and their interactions with TheFSM platform.

In accordance with this methodological approach, the User Stories, that that are stemming directly from the end-user partners of the TheFSM project were collected in collaboration with technical partners. These User Stories presented the expected behaviour of all sub-systems of the platform from the end-user perspective and were provided as input for the user requirements elicitation process.

From these User Stories, the user requirements were extracted ensuring the compliance with the requirements characteristics defined in the methodology. These extracted user requirements were classified into functional requirements and non-functional requirements. The list of functional and non-functional user requirements were analysed thoroughly in order to extract the list of TheFSM technical requirements. These concrete and solid technical requirements were provided as input in the design and specification definition of the components of TheFSM architecture. Within the scope of this deliverable the complete requirement backlog has been provided for TheFSM.

A comprehensive analysis of these technical requirements provided the design of the first version of the conceptual architecture of the integrated TheFSM platform. TheFSM architecture is a modular architecture, composed by a set of key components with distinct roles and scope towards the aim of providing the envisioned platform features and that will be address TheFSM stakeholders' needs. Each component was carefully designed having in mind that it should address a specific set of technical requirements from the list of the technical requirements. For each component a comprehensive description of the design and functionalities has been documented.

It should be stressed at this point that the current deliverable presents the first version of TheFSM conceptual architecture, as well as the user and technical requirements. These outcomes will drive the implementation phase of TheFSM platform that will be performed within the context of WP2, WP3 and WP4. However, as the design of TheFSM architecture and the identification and analysis of the functional and non-functional requirements, as well as their translation into technical requirements, is living iterative process that will last until M36, the forthcoming versions of this deliverable will include updates on both the architecture and the components of the architecture based on the feedback received.

8. BIBLIOGRAPHY

[1] Cohn, M. (2010). Agile Softwareentwicklung: mit Scrum zum Erfolg!. Pearson Deutschland GmbH

[2] Ericson, C. A. (2015). Hazard analysis techniques for system safety. John Wiley & Sons.

[3] "Non Functional Requirements" [Online] Available: https://www.scaledagileframework.com/nonfunctional-requirements/ [Accessed:16-10-2020]

[4] Johan ter Bekke (1992). Semantic Data Modeling. Prentice Hall.

[5] Shashank Agrawal and Melissa Chase, FAME: Fast Attribute-Based Message Encryption., 2007

[6] Kan Yang, Xiaohua Jia, Bo Zhang, and Ruitao Xie, DAC-MACS: Effective data access control for multiauthority cloud storage systems., 2013

[7] Amit Sahai and Brent Waters, Fuzzy Identity-Based Encryption., 2005

[8] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Wate, Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data., 2006

[9] John Bethencourt, Amit Sahai, and Brent Waters, Ciphertext-Policy Attribute-Based Encryption., 2007

[10] Vincent Hu et al., Guide to Attribute Based Access Control (ABAC) Definition and Considerations., 2014

[11] Vincent Hu, D. Kuhn, and David Ferraiolo, Attribute-Based Access Control., 2015.

ANNEX I USER STORIES

The following table provides TheFSM user stories, as they are defined by the business requirements provided in D1.1.

ID	Business requirement no	Category	User Story		
			As a	I want to <user>	So that
US_1	BR_nr2_1	Analytics	Producer	Collect different data related to business characteristics and the final product	I can have a better view of products I am interested in / i can confirm (reveal) that my production process conforms with the certification requirements
US_2	BR_nr2_2	Analytics	Producer	Be able to manage and evaluate data from different heterogeneous sources	I can draw conclusions for analysis, legislative requirements, etc.
US_3	BR_nr2_3	Notifications	Producer	Be constantly updated about information shown to me	I can make valid decisions
US_4	BR_nr2_4	Logging	Producer	Record up to date data assets for exploitation	I can catalogue data which is of interest to me
US_5	BR_nr2_6	Certification	Producer	Be able to validate GLOBALGAP certificates	I can be certain about the credibility of the certificates I am viewing
US_6	BR_nr2_7	Logging	Producer	Archive agreed specifications on the delivered product	I can make cooperation easier
US_7	BR_nr2_8	Integration	Producer	Be able to interconnect with the food processor's recording system	I can view terms of critical product data, tracking per batch and certificates of conformity
US_8	BR_nr2_12	Profiling	All	Be able to personalize the data I will use in my daily operations	I can have a more personalized experience
US_9	BR_nr2_14, BR_nr5_10, BR_nr4_1, BR_nr4_5, BR_nr4_	Data, Certification	Producer, Food processor, Industry, Inspector/auditor	Replace physical documents with a complete digital collection	I can organize daily work faster and more efficiently

	8, BR_nr4_12, BR_nr4_18, BR_nr4_21, BR_nr5_2				
US_10	BR_nr2_16, BR_nr4_11, BR_nr4_15	Decision making	All	Use real-time data	Reduce decision-making time
US_11	BR_nr2_20	Decision making	Food Processor	Be able to segregate critical control points data (regarding product safety) from functional control points data	I can better assess both
US_12	BR_nr2_21	Monitoring	Food Processor	Be constantly updated about information that directly or indirectly affects food safety	I can ensure better quality for the product
US_13	BR_nr2_22, BR_nr2_35	Data, Traceability, Certification	Food Processor, Certification Body	Be able to easily access aggregated data from various sources (e.g., suppliers)	I can assess compliance with food safety standards and with the requirements of certified schemes
US_14	BR_nr2_24	Monitoring	Food Processor	Be immediately notified about any non-conformity raised for the producer and their certified product	I can take proper action
US_15	BR_nr2_25	Certification	Food Processor	Be able to easily access valid info to operational licenses for actors I interact with, as well as info regarding the accrediation of different kind of labs	I can validate my working collaborators and verify the effectiveness of the FSMS

US_16	BR_nr2_27	Profiling	Food Processor	Be able to categorize, modify and transfer my data in a common point of protected and controlled access	I can ensure my data is safe
US_17	BR_nr2_33	Monitoring	Food Processor	Have the ability of finding new partnerships and cooperation, via accessing information relevant to the current market needs	I can produce products which will cover above needs
US_18	BR_nr2_36	Certification	Certification Body	Be able to access up-to-date data from different sources and access to new and amended legislation	I can ensure the transparency of the certification process
US_19	BR_nr2_37	Certification	Certification Body	Be able to use a representative sample of the processed data	I can evaluate compliance with product specifications
US_20	BR_nr2_39	Certification	Certification Body	Be able to collect needed documentation prior to the certification decision	The decision can be properly certified
US_21	BR_nr2_40	Certification	Certification Body	Have different methods of sending and receiving information	I can collect documentation during the certification process
US_22	BR_nr2_45, BR_nr4_2	Monitoring, Certification	Certification Body, Inspector/auditor	Have direct and official information on findings of the National Audit Authorities in certified Producers, Food processors and Retailers	I can consult this information for decision making
US_23	BR_nr2_46, BR_nr3_6, BR_nr3_14	Certification	Certification Body, Producer, Food processor	Be able to easily obtain evidence for the justification of compliance criteria for the actors I am supervising	I can ensure transparency

US_24	BR_nr2_48	Auditing, Certification	Certification Body	Be able to obtain on-demand immediate stakeholder profile in terms of certification history	I can easier analyze the audit risk and for control/validation
US_25	BR_nr2_50	Risk estimation, Auditing	Certification Body	Be able to use and re-examine previous customers' audit findings, grouped into certain categories	I can highlight areas of high risk for subsequent audits
US_26	BR_nr2_51, BR_nr3_5, BR_nr3_13, BR_nr3_21	Traceability	Retailer, Producer, Food processor, Distributor	Be able to access detailed information about final shelf product, as well as correlation with critical factors	I can maintain a robust traceability and be able to efficiently withdraw products, should the need arise
US_27	BR_nr3_8, BR_nr3_16, BR_nr3_22, BR_nr3_24, BR_nr3_32, BR_nr2_53	Traceability	Retailer, Producer, Certification Body, Distributor, Food processor	Be able to access fully traced information	I can have transparency and ensure no unfair trade practices effect consumers
US_28	BR_nr2_55	Profiling	Retailer	Be able to present important data relevant to QA actions taken by my company	I can enhance customer's trust on my brand name
US_29	BR_nr1_1	Decision making	Retailer	Be able to access information regarding findings of the inspection of suppliers in the food chain	I can make better decisions based on evidence
US_30	BR_nr1_2	Certification	Retailer	Be able to access current status of food supply actors, as far as audit results of certify organizations are concerned	I can validate their credibility for cooperation

US_31	BR_nr1_3	Risk estimation	Retailer	Have access to innovative tools	I can have enhanced risk monitoring capabilities
US_32	BR_nr3_2, BR_nr3_10, BR_nr3_18	Certification	Producer, Food processor, Distributor	Be able to locate with precise criteria required certificates and seals of approval, as requested by a customer/ Be able to access detailed information regarding certificate validity and scope of certification	I can speed up certification and validation
US_33	BR_nr3_3, BR_nr3_11, BR_nr3_19	Decision making	Producer, Food processor	Have a way to view an estimation of costs and expenditures regarding the certification process/Be able to chose appropiate certificate scheme	Have more information when considering/ I can meet the requirements of different organizations (retailers, distributor, processors)
US_34	BR_nr3_4, BR_nr3_12, BR_nr3_20, BR_nr3_30	Decision making, Auditing	Producer, Distributor, Certification Body, Food processor	Be able to support remote audits	I can reduce decision-making under difficult situations
US_35	BR_nr3_7, BR_nr3_15, BR_nr3_23, BR_nr3_31	Decision making, certification	Producer, Distributor, Certification Body, Food processor	Have access to validated data of all stakeholders	I can support decision-making processes
US_36	BR_nr3_21		Distributor	assess data	I Can conduct fact driven management
US_37	BR_nr3_26	Certification	Certification Body	Be able to understand the specific	I can speed up the certification process without grey areas

				requirements of an organization	
US_38	BR_nr3_27	Certification	Certification Body	Be able to directly interact with organizations requesting certification	To speed up the certification process
US_39	BR_nr3_33	Certification, Auditing	Certification Body	Be able to have a better overall view of the ability of an audited organization	I can have better audit results
US_40	BR_nr3_35, BR_nr3_36	Risk estimation	Retailer	Reduce the number of product recalls	I can improve efficiency
US_41	BR_nr4_4, BR_nr4_7	Monitoring	Inspector/Auditor	Be able to interact with data of different Certification Bodies	The data has increased reliability
US_42	BR_nr4_5	Certification	Certification Committee	Be able to verify a digital report	
US_43	BR_nr4_9, BR_nr4_10, BR_nr4_13, BR_nr4_14, BR_nr4_16, BR_nr4_17, BR_nr4_19, BR_nr4_20, BR_nr4_22	Traceability	Farmer/ Producer, Distributor	Be able to trace input suppliers	Ensure the quality of my product
US_44	BR_nr4_23		Public authorities	Be able to check and verify product data with respect to compliance with certification regulations	I can ensure transparency

US_45	BR_nr5_1	Monitoring	Public Authorities (NVWA)	Be able to predict when/what/where to check	I can ensure food safery and effeciency
US_46	BR_nr5_2	Monitoring	Public Authorities (NVWA)	Be able to have access to the degital format of the inspection	I can ensure effeciency
US_47	BR_nr5_3	Monitoring	Public Authorities (NVWA)	Be able to to search past audit performance per actor (producer, supplier, etc.)	I can ensure food safety and inspection effeciency
US_48	BR_nr5_4	Risk estimation	Public Authorities (NVWA)	Be able to conduct risk-based monitoring	I can conduct effecient sampling
US_49	BR_nr5_8	Certification	Public authorities	Be able to assess the performance of the producers in complying to the certification standards	I can decide to what extent they comply with law and certification standards
US_50	BR_nr5_12	Monitoring	Industry	Be able to inspect market needs and new clients	I can better supervise the supply chain process
US_51	BR_nr5_13	Monitoring	Industry	Be able to establish an up to date communication channel with traders	I can ensure communication

Table ANNEX I TheFSM user stories

ANNEX II USER STORIES – END USERS RANKING

ID	AGROKNOW			WFSR			TAR			VALOR			TAH		
	Priority		Value	Priority		Value	Priority		Value	Priority		Value	Priority		Value
	business maturity/ feasibility	time urgency	critical to business success/competitive advantage	business maturity/ feasibility	time urgency	critical to business success/competitive advantage	business maturity/ feasibility	time urgency	critical to business success/competitive advantage	business maturity/ feasibility	time urgency	critical to business success/competitive advantage	business maturity/ feasibility	time urgency	critical to business success/competitive advantage
US_1	Medium	Low	Low	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	High	Medium	High
US_2	Low	Low	Low	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	High	Medium	High
US_3	Low	Low	Low	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	High	Medium	High
US_4	Low	Low	Low	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	Medium	Low	High
US_5	Low	Medium	Medium	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	Medium	Medium	Medium
US_6	Medium	Low	Medium	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	Medium	Medium	Medium
US_7	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	Low	n/a	n/a	n/a	Medium	Medium	High
US_8	High	Medium	Medium	n/a	n/a	n/a	High	n/a	High	n/a	n/a	n/a	High	High	High
US_9	Low	Medium	Medium	n/a	n/a	n/a	High	n/a	High	High	High	High	High	High	High

US_10	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	High	Medium	Medium	High	Medium	Medium	High
US_11	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	High
US_12	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	Medium	High
US_13	Medium	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	High
US_14	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Low	High
US_15	Low	Low	Low	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	High
US_16	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	Medium	High
US_17	Low	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Low	High
US_18	Low	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	High
US_19	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	Medium	High
US_20	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	Medium	High
US_21	Medium	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	High	High

US_22	Low	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	Medium	High
US_23	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	Medium	High
US_24	Medium	High	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	High
US_25	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	High
US_26	Medium	Low	Low	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	High	High
US_27	Medium	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	High	High
US_28	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Low	High
US_29	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_30	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_31	High	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_32	Medium	Medium	Medium	n/a	n/a	n/a	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_33	Low	Low	Low	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

US_34	Medium	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_35	Medium	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_36	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_37	Medium	Low	Low	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_38	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_39	Medium	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_40	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_41	High	High	High	n/a	n/a	n/a	n/a	n/a	n/a	Medium	Medium	Medium	n/a	n/a	n/a
US_42	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	High	High	High	n/a	n/a	n/a
US_43	Medium	High	Medium	n/a	n/a	n/a	n/a	n/a	n/a	Low	Low	Medium	n/a	n/a	n/a
US_44	Low	Low	Low	n/a	n/a	n/a	n/a	n/a	n/a	High	High	High	n/a	n/a	n/a
US_45	Medium	Medium	High	High	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

US_46	Medium	Medium	High	Medium	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_47	High	High	High	Low	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_48	High	High	High	High	Medium	High	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_49	Medium	High	High	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_50	Low	Low	Low	Medium	Medium	Medium	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
US_51	Low	Low	Low	Medium	Low	Low	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Table ANNEX II TheFSM user stories – End-users ranking

ANNEX III USER STORIES – TECHNICAL PARTNERS RANKING

ID	Agroknow			UBITECH			SAI			PROSPEH			Agrivi			Final
	Feas	Prer	Mean	Feas	Prer	Mean	Feas	Prer	Mean	Feas	Prer	Mean	Feas	Prer	Mean	
US_1	2	4	3	2	3	3	5	1	3	4	3	4	3	3	3	**4**
US_2	3	4	4	3	4	4	5	1	3	4	3	4	3	4	4	**4**
US_3	3	4	4	3	4	4	2	4	3	3	4	4	3	4	4	**4**
US_4	3	3	3	3	3	3	4	2	3	4	2	3	3	4	4	**4**
US_5	4	3	4	4	4	4	4	4	4	5	2	4	4	3	4	**4**
US_6	3	4	4	3	4	4	4	2	3	5	2	4	3	4	4	**4**
US_7	1	3	2	2	4	3	3	3	3	4	4	4	2	3	3	**3**
US_8	4	2	3	4	2	3	4	3	4	4	3	4	4	3	4	**4**
US_9	2	4	3	2	4	3	4	5	5	4	4	4	2	4	3	**4**
US_10	2	5	4	3	5	4	5	5	5	4	5	5	3	5	4	**5**
US_11	1	5	3	2	5	4	5	2	4	2	3	3	2	5	4	**4**
US_12	4	2	3	4	3	4	2	4	3	5	3	4	4	3	4	**4**
US_13	5	2	4	5	2	4	5	5	5	5	4	5	4	3	4	**5**
US_14	5	3	4	3	3	3	2	4	3	4	3	4	4	3	4	**4**
US_15	2	4	3	2	4	3	5	4	5	5	5	5	2	4	3	**4**
US_16	3	5	4	3	5	4	5	3	4	5	4	5	3	5	4	**5**
US_17	2	5	4	2	3	3	3	2	3	3	4	4	2	5	4	**4**
US_18	3	2	3	3	4	4	5	5	5	4	4	4	3	4	4	**4**
US_19	2	4	3	3	4	4	4	4	4	4	3	4	3	4	4	**4**
US_20	2	5	4	3	4	4	5	4	5	4	5	5	3	4	4	**5**
US_21	2	5	4	2	4	3	1	1	1	2	3	3	3	4	4	**3**
US_22	2	2	2	2	4	3	2	4	3	4	4	4	2	2	2	**3**
US_23	1	5	3	2	4	3	4	4	4	4	4	4	2	4	3	**4**
US_24	4	3	4	4	4	4	4	4	4	4	3	4	4	4	4	**4**
US_25	3	4	4	3	3	3	5	2	4	4	2	3	3	4	4	**4**
US_26	2	4	3	3	4	4	5	2	4	4	5	5	3	4	4	**4**
US_27	2	5	4	3	5	4	3	5	4	4	5	5	3	4	4	**5**
US_28	3	3	3	3	3	3	5	3	4	4	4	4	3	4	4	**4**
US_29	4	2	3	4	4	4	4	3	4	4	3	4	4	4	4	**4**
US_30	3	3	3	3	3	3	5	3	4	4	3	4	3	4	4	**4**
US_31	4	2	3	4	3	4	5	1	3	3	2	3	3	4	4	**4**

US_32	3	3	3	3	3	3	4	2	3	4	5	5	3	3	3	**4**
US_33	4	1	3	4	2	3	5	1	3	3	1	2	4	2	3	**3**
US_34	2	5	4	3	4	4	5	1	3	4	4	4	3	4	4	**4**
US_35	2	5	4	3	5	4	5	5	5	5	5	5	3	4	4	**5**
US_36	2	4	3	3	4	4	5	1	3	3	3	3	3	4	4	**4**
US_37	3	2	3	3	2	3	4	1	3	3	2	3	3	4	4	**4**
US_38	4	2	3	4	3	4	5	1	3	5	3	4	4	4	4	**4**
US_39	4	2	3	4	2	3	5	2	4	5	2	4	4	4	4	**4**
US_40	3	5	4	3	3	3	1	1	1	3	2	3	4	4	4	**3**
US_41	1	5	3	2	3	3	3	1	2	3	5	4	2	4	3	**3**
US_42	3	3	3	3	3	3	5	1	3	5	5	5	3	3	3	**4**
US_43	2	4	3	3	4	4	3	3	3	5	1	3	3	4	4	**4**
US_44	3	2	3	4	3	4	3	4	4	5	1	3	5	2	4	**4**
US_45	1	2	2	2	2	2	3	2	3	5	1	3	1	1	1	**3**
US_46	2	4	3	3	4	4	2	5	4	5	1	3	2	5	4	**4**
US_47	3	4	4	3	3	3	3	4	4	5	1	3	2	4	3	**4**
US_48	4	4	4	4	3	4	4	3	4	5	1	3	3	3	3	**4**
US_49	4	3	4	4	3	4	3	4	4	5	1	3	5	2	4	**4**
US_50	4	3	4	3	4	4	4	5	5	5	1	3	2	3	3	**4**
US_51	3	0	2	3	1	2	4	1	3	5	1	3	3	2	3	**3**

ANNEX IV THEFSM FUNCTIONAL REQUIREMENTS

Reference ID	Business scenario	Business Requirement ID	Title	Actors	Category
FR_1	nr_1	BR_nr1_2, BR_nr1_1	Create user account	All	User account
FR_2	nr_1	BR_nr1_2, BR_nr1_1	Create company profile	All	Company profile
FR_3	nr_1	BR_nr1_2, BR_nr1_1	Upload certification info	Producer	Certification validation
FR_4	nr_1	BR_nr1_2, BR_nr1_1	Upload laboratory analysis test info	Producer	Certification validation
FR_5	nr_1	BR_nr1_2	Estimate risk	Retailer (FSQA expert)	Risk assessment
FR_6	nr_1, nr_2	BR_nr1_2, BR_nr2_8, BR_nr2_9	Request an audit by third party	Retailer (FSQA expert), Producer	Alerting, Auditing
FR_7	nr_1, nr_2	BR_nr1_2, BR_nr2_8, BR_nr2_9	Receive audit request	Certification Body	Alerting, Auditing
FR_8	nr_1	BR_nr1_2	Submit audit results	Certification Body	Certification validation
FR_9	nr_1	BR_nr1_2, BR_nr1_1	Upload lab results	Lab expert	Certification validation
FR_10	nr_1	BR_nr1_2, BR_nr1_1	New audit notification	Retailer (FSQA expert)	Alerting, Auditing
FR_11	nr_1	BR_nr1_2, BR_nr1_1	New test results notification	Retailer (FSQA expert)	Alerting, Auditing
FR_12	nr_1	BR_nr1_2, BR_nr1_1	View tracebility report for a cultivation	Retailer (FSQA expert)	Product details, Traceability
FR_13	nr_1	BR_nr1_2, BR_nr1_1	View IoT data (from farm, production) of a specific product	Retailer (FSQA expert)	Product details, Monitoring
FR_14	nr_1	BR_nr1_2, BR_nr1_1	Provide IoT data (from farm, production) of a specific product	Producer	Product details
FR_15	nr_1	BR_nr1_1	View findings of the inspection of suppliers in the food chain	Retailer (FSQA expert)	Product details
FR_16	nr_1	BR_nr1_2, BR_nr1_1	Select specific suppliers/professionals of interest to monitor their status	Retailer (FSQA expert)	Monitoring, Traceability
FR_17	nr_1	BR_nr1_2, BR_nr1_1	Show product history based on traceability unit id (LOT number)	Retailer (FSQA expert)	Product details
FR_18	nr_1	BR_nr1_2, BR_nr1_1	Predict an increasing risk for a supplier	Retailer (FSQA expert)	Risk assessment

FR_19	nr_1	BR_nr1_1	View specific certification for a producer	Supplier	Monitoring
FR_20	nr_1	BR_nr1_1	View tracebility history for cultivation	Supplier	Product details, Traceability
FR_21	nr_1	BR_nr1_2, BR_nr1_1	View lab results and the certification of analysis for a specific producer	Supplier	Company profile, Traceability
FR_22	nr_1	BR_nr1_1	View information for a supplier (Name, products, location)	Supplier	Company profile
FR_23	nr_1	BR_nr1_2, BR_nr1_1	View information about audits and inspections for a specific producer/grower	Supplier	Auditing, Monitoring
FR_24	nr_1	BR_nr1_1	View information for the food recalls ,border rejections and inspections for a specific supplier	Supplier	Monitoring
FR_25	nr_1	BR_nr1_2, BR_nr1_1	Access to Producer-entered data (production plans, progress, practices, risks, deliveries)	Supplier	Company profile
FR_26	nr_1	BR_nr1_2, BR_nr1_1	Access to Retail-entered data (production plans, progress, practices, risks, deliveries)	Supplier	Company profile
FR_27	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	View real-time data related to cultivation conditions	Producer	Monitoring, Product details
FR_28	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	View additional data related to cultivation conditions	Producer	Monitoring
FR_29	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	View characteristics of plots (plots' distribution and their topographic features)	Producer	Monitoring
FR_30	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	Collect data related to characteristics relevant to the agricultural plots (soil), to the plantation etc., before implementing agricultural practices	Producer	Monitoring
FR_31	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	Extract insights about the plots status	Producer	Monitoring
FR_32	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	Get notified about potential risks	Producer	Monitoring, Alerting
FR_33	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14	Provide/view available resources of producer's business	Producer	Monitoring, Company profile

FR_34	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14, BR_nr2_16	Share measurement of the concentration (residues) of Plant Protection Substances in the final	Producer	Monitoring, Certification validation
FR_35	nr_2	BR_nr2_1, BR_nr2_2, BR_nr2_3, BR_nr2_10, BR_nr2_14, BR_nr2_16	Share measurements of characteristics relevant to the agricultural plots (soil), to the plantation etc., before implementing agricultural practices	Producer	Monitoring, Certification validation
FR_36	nr_2	BR_nr2_8, BR_nr2_16	Share data from all correlation stages with the food processor	Producer	Monitoring, Traceability
FR_37	nr_2	BR_nr2_8, BR_nr2_16	Share certificate history of a specific product	Producer	File management, Certification validation
FR_38	nr_2	BR_nr2_8	Validate certificate from GLOBALGAP database	Producer	Certification validation
FR_39	nr_2	BR_nr2_9, BR_nr2_8, BR_nr2_7,	Support negotiation with food processor about the characteristics of the product	Producer	Traceability
FR_40	nr_2	BR_nr2_5, BR_nr2_9, BR_nr2_8,	Share directly production data related to the traceability units with processor	Producer	Traceability
FR_41	nr_2	BR_nr2_6, BR_nr2_9, BR_nr2_8, BR_nr2_5	Share of the GlobalGAP Number (GGN) with the processor for certificate validation	Producer	Certification validation, Compamy profile
FR_42	nr_2	BR_nr2_6, BR_nr2_9, BR_nr2_8, BR_nr2_5	Correlate the certification with tracking batches	Producer	Traceability, Certification validation
FR_43	nr_2	BR_nr2_8, BR_nr2_9	Share production data with the Certification Body	Producer	Certification validation
FR_44	nr_2	BR_nr2_8, BR_nr2_9	View production data of producer	Certification Body	Monitoring
FR_45	nr_2	BR_nr2_8, BR_nr2_9	Support negotiation with certification body about the financial offer	Producer	Certification validation, Traceability
FR_46	nr_2	BR_nr2_8, BR_nr2_9	Receive an alert that my company is uploaded in the GLOBALGAP database	Producer	Certification validation, Alerting
FR_47	nr_2	BR_nr2_8, BR_nr2_9	Upload and manage audit data and files	Certification Body	Auditing, File management
FR_48	nr_2	BR_nr2_8, BR_nr2_9	Create audit report	Certification Body	Auditing
FR_49	nr_2	BR_nr2_8, BR_nr2_9	Share audit report with producer	Certification Body	Auditing, Authentication/Authorization
FR_50	nr_2	BR_nr2_8, BR_nr2_9	Upload final audit data in the GLOBALGAP database	Certification Body	Auditing
FR_51	nr_2	BR_nr2_8, BR_nr2_9	Issue a certification for producer	Certification Body	Certification validation

FR_52	nr_2	BR_nr2_21, BR_nr2_20, BR_nr2_28	View/access farm data on the traceability of a particular batch from producer	Food Processor	Monitoring, Traceability
FR_53	nr_2	BR_nr2_20, BR_nr2_32, BR_nr2_31, BR_nr2_28, BR_nr2_21	View/access product safety verification data from producer	Food Processor	Risk assessment, Traceability
FR_54	nr_2	BR_nr2_20, BR_nr2_32, BR_nr2_31, BR_nr2_28, BR_nr2_21	View/access food recall data from producer	Food Processor	Risk assessment, Traceability
FR_55	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	View/access retailer's requirements Data from retailer	Food Processor	Product details, Risk assessment
FR_56	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	Define product data requirements to food processor	Retailer	Product details, Risk assessment
FR_57	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	Provide feedback about a specific product to food processor	Retailer	Product details, Risk assessment
FR_58	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	View feedback about a specific product from retailer	Food Processor	Product details, Risk assessment
FR_59	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	Access to certificates generated in previous phases	Food Processor	Certification validation, Product details
FR_60	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	View suppliers who hold a specific certificate	Food Processor	Company profile
FR_61	nr_2	BR_nr2_32, BR_nr2_20	View food recall data and recieve alerts	Food Processor	Monitoring, Alerting
FR_62	nr_2	BR_nr2_32, BR_nr2_20	View supplementary product data	Food Processor	Monitoring, Product details
FR_63	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	Share raw materials specifications to producer	Food Processor	Product details, Negotiation support
FR_64	nr_2	BR_nr2_31, BR_nr2_24, BR_nr2_34, BR_nr2_33	Share final product safety verification data to retailer	Food Processor	Product details, Certification validation

FR_65	nr_2	BR_nr2_22, BR_nr2_21, BR_nr2_39, BR_nr2_36, BR_nr2_30, BR_nr2_46	Share compliance Data, which evidently reveal conformity of the packaging process against the requirements of the food safety standards (FSSC22000, IFS) to the Certification Body	Food Processor	Product details, Certification validation
FR_66	nr_2	BR_nr2_22, BR_nr2_21, BR_nr2_39, BR_nr2_36, BR_nr2_30, BR_nr2_46	Share certification data with the Certification Body	Food Processor	Product details, Certification validation
FR_67	nr_2	BR_nr2_21, BR_nr2_20	To monitor data from all stages of food processing	Food Processor	Product details, Monitoring
FR_68	nr_2	BR_nr2_35, BR_nr2_36, BR_nr2_37, BR_nr2_38, BR_nr2_39	To receive/view/access data from producer, processor, retailer in order to check if the stakeholder complies with the certification schemes	Certificatio n Body	Certification validation, Monitoring
FR_69	nr_2	BR_nr2_35, BR_nr2_36, BR_nr2_37, BR_nr2_38, BR_nr2_39	To receive/view/access laboratory analysis reports	Certificatio n Body	Certification validation, Traceability
FR_70	nr_2	BR_nr2_6, BR_nr2_9, BR_nr2_8, BR_nr2_5	Share of the GlobalGAP Number (GGN) and relevant valid certificate	Producer	Certification validation, Company profile
FR_71	nr_2	BR_nr2_6, BR_nr2_9, BR_nr2_8, BR_nr2_5	Have access on a the FSSC certification checklist	Certificatio n Body	Certification validation
FR_72	nr_2	BR_nr2_38, BR_nr2_39, BR_nr2_46	Share my evaluation data from the National Accreditation Council	Certificatio n Body	Data management
FR_73	nr_3	BR_nr3_1, BR_nr3_3	Provide relevant data to the planned comprehensive database (FSM)	Producer, Foor Processor, Distributor	Certification validation, Data management
FR_74	nr_3	BR_nr3_1, BR_nr3_2, BR_nr3_3	Retailer provides specific requirements regarding certification and seals of approval	Retailer	Certification validation
FR_75	nr_3	BR_nr3_1, BR_nr3_2, BR_nr3_3, BR_nr3_7	CB provides detailed information regarding standards, seals of approval and certification process	Certificatio n Body	Certification validation, Alerting
FR_76	nr_3	BR_nr3_1, BR_nr3_3, BR_nr3_5	Data exchange between orgs	All	Data management, Alerting
FR_77	nr_3	BR_nr3_1, BR_nr3_2,	Find all necessary information for planning and realizing the certification process	Certificatio n Body	Certification validation, Data management

		BR_nr3_3, BR_nr3_6			
FR_78	nr_3	BR_nr3_1, BR_nr3_2, BR_nr3_6	Provide specific customer requirements, standards, seals of approval to producers	Producer	Certification validation
FR_79	nr_3	BR_nr3_1, BR_nr3_3, BR_nr3_6	Determine which standards and seals of approval should be implemented to meet all customer requirements to raise competitiveness	Producer	Certification validation
FR_80	nr_3	BR_nr3_1, BR_nr3_3, BR_nr3_6	Notify producer on prerequisites to fulfill the specific requirements and which resources must be allocated	Producer	Certification validation, Alerting
FR_81	nr_3	BR_nr3_1, BR_nr3_6	Provide a way for producers to determine which certification body can certify which elected standards	Producer	Certification validation, Alerting
FR_82	nr_3	BR_nr3_1, BR_nr3_6	Manage high amounts of data, from heterogenous sources	All	Data management
FR_83	nr_3	BR_nr3_1, BR_nr3_6	Regular data exchange between producer and food processor	Producer, food processor	Data management, Alerting
FR_84	nr_3	BR_nr3_1, BR_nr3_6	Regular data exchange between producer and retailer	Producer, retailer	Data management, Alerting
FR_85	nr_3	BR_nr3_1, BR_nr3_6	Presale data of producer and company	Producer	Company profile, Certification validation
FR_86	nr_3	BR_nr3_1, BR_nr3_6	Search and request certification from distributor	Producer	Data management, Alerting
FR_87	nr_3	BR_nr3_1	Request certification data from certification body	Producer	Certification validation, Data management
FR_88	nr_3	BR_nr3_1, BR_nr3_6	Producer send requirements to food processor, or food processor directly contacting producer	Food Processor, producer	Certification validation, Alerting
FR_89	nr_3	BR_nr3_1, BR_nr3_6	Producer send requirements to retailer, or retailer directly contacting producer	Retailer, producer	Certification validation, Alerting
FR_90	nr_3	BR_nr3_1, BR_nr3_6	Regular publication of distributor certificates	Distributor	Certification validation, Data management
FR_91	nr_3	BR_nr3_1, BR_nr3_4, BR_nr3_6	CB provide audit reports to producer	Producer	Certification validation, Auditing
FR_92	nr_3	BR_nr3_1, BR_nr3_4, BR_nr3_6	Allow consulants to collect data, conduct internal audits, for decision support	Consultant	Certification validation, Auditing
FR_93	nr_3	BR_nr3_1	Enable labs to post certificates after lab tests	Lab expert	Certification validation, Data management
FR_94	nr_3	BR_nr3_1, BR_nr3_6, BR_nr3_8	Allow public authorities to extract information, ensure the legality of the procedures, as also utilize traceability data and analytics	Public Authorities	Monitoring, Traceability
FR_95	nr_3	BR_nr3_9, BR_nr3_14	Regular data exchange between food processor and food processor	Food processor (x2)	Data management, Alerting
FR_96	nr_3	BR_nr3_9, BR_nr3_14	Regular data exchange between food processor and retailer	Food processor, retailer	Data management, Alerting
FR_97	nr_3	BR_nr3_9, BR_nr3_14	Presale data of distributor and company	Food processor	Data management, Alerting

FR_98	nr_3	BR_nr3_9	Request certification data from certification body	Food processor	Certification validation, Data management
FR_99			Food processor send requirements to retailer, or retailer directly contacting food processor	Food processor, distributor	Certification validation, Alerting
FR_100	nr_3	BR_nr3_9, BR_nr3_14	Search and request certification from distributor	Food processor	Data management, Alerting
FR_101	nr_3	BR_nr3_9, BR_nr3_12, BR_nr3_14	CB provide audit reports to food processor	Food processor	Data management, Alerting
FR_102	nr_3		Distributor send requirements to retailer, or retailer directly contacting distributor	Retailer, distributor	Certification validation, Alerting
FR_103	nr_3	BR_nr3_25, BR_nr3_26, BR_nr3_28, BR_nr3_29, BR_nr3_30	Provide impartial certification processes, procedures and practices	Certification Body	Certification validation, Data management
FR_104	nr_3	BR_nr3_25, BR_nr3_28, BR_nr3_29, BR_nr3_30	Provide competent audits by certification scheme owners	Certification Body	Certification validation, Data management
FR_105	nr_3	BR_nr3_25, BR_nr3_26, BR_nr3_28, BR_nr3_29, BR_nr3_30	Support independent decision-making on certification issuing	Certification Body	Certification validation, Data management
FR_106	nr_3	BR_nr3_25, BR_nr3_26	Provide certification data, requirements, standards, to: producer, food processor, distributor	Certification Body	Certification validation, Data management
FR_107	nr_3	BR_nr3_25, BR_nr3_28, BR_nr3_33	Interact with consultants	Certification Body	Certification validation, Auditing
FR_108	nr_3	BR_nr3_25, BR_nr3_26, BR_nr3_27	Interact with companies	Certification Body	Certification validation, Data management
FR_109	nr_3	BR_nr3_34, BR_nr3_36	Search and request certification from distributor	Retailer	Data management, Alerting
FR_110	nr_3	BR_nr3_34, BR_nr3_36	Producer send requirements to retailer, or retailer directly contacting producer	Retailer, producer	Certification validation, Alerting
FR_111	nr_3	BR_nr3_34, BR_nr3_36	Interact with certification body to obtain audit reports, certificates and seals of approval	Retailer, Certification Body	Certification validation, Alerting
FR_112	nr_3	, BR_nr3_36	Provide traceability data to consumers	Retailer	Certification validation, Traceability
FR_113	nr_3	BR_nr3_34, BR_nr3_36	Receive regular updates on certifications and product specifications	Retailer	Certification validation, Alerting
FR_114	nr_3	BR_nr3_34, BR_nr3_36	Cooperate with consultants for audits	Retailer	Certification validation, Auditing
FR_115	nr_3	BR_nr3_35	(optional) provide detailed risk analysis for products	Retailer	Risk assessment, Data analysis
FR_116	nr_3	BR_nr3_34, BR_nr3_36	Provide samples to labs for testing	Retailer	Certification validation, Data management

FR_117	nr_4	BR_nr4_1, BR_nr4_2	Make available the auditing reports and/or non-compliances found	Public Authorities	Auditing, Data management
FR_118	nr_4	BR_nr4_1, BR_nr4_2, BR_nr4_3, BR_nr4_4	Integration with national DBs like SIAN (it is a registry), to allow wine cellars to collect data about every wine movement	Public Authorities, Producer	Monitoring, Product details
FR_119	nr_4	BR_nr4_1, BR_nr4_2	Enable auditors to fill in reports in digital form	Inspector/Auditor	Auditing, Data management
FR_120	nr_4	BR_nr4_1, BR_nr4_2, BR_nr4_4	Integrate legal requirements, lab certifications, specific parameters for auditor	Inspector/Auditor	Data management
FR_121	nr_4	BR_nr4_7	Evaluate inspector reports	Certification Body	Data management
FR_122	nr_4	BR_nr4_6	Issue certification	Certification Body	Authentication/Authorization, Certification validation
FR_123	nr_4	BR_nr4_6	Send digital certification to winegrower/winemaker/bottler (producer?)	Certification Body	Certification validation, Alerting
FR_124	nr_4	BR_nr4_7	Enable communication between Certification Body and inspector if doubting information	Certification Body, Inspector	Alerting
FR_125	nr_4	BR_nr4_6	Issue measure of non-compliance/irregularity if Operator (producer?) doesn't meet requirements	Certification Body	Certification validation, Alerting
FR_126	nr_4	BR_nr4_7	Periodically check traceability and status of products by checking inspection reports	Certification Body	Monitoring, Traceability
FR_127	nr_4	BR_nr4_5	Verify integrity of digital report	Certification Body	Data management
FR_128	nr_4	BR_nr4_8	Notify producers about regulations to be fulfilled	Producer	Alerting, Monitoring
FR_129	nr_4	BR_nr4_8	Ensure producer has up to date status on buying and selling, farm files	Producer	Alerting, Monitoring
FR_130	nr_4	BR_nr4_8	Interaction with auditors for farm inspection	Producer	Auditing, Monitoring
FR_131	nr_4	BR_nr4_8	Provide timelines, products or techniques suggestions, certification information	Producer	Certification validation, Data management
FR_132	nr_4	BR_nr4_8	Update vineyard info if not in touch with consultant	Producer	Certification validation, Data management
FR_133	nr_4	BR_nr4_19, BR_nr4_21	Receive producer's data about harvest period of certified product, certification validity and report	Bottler	Traceability, Certification validation
FR_134	nr_4	BR_nr4_19, BR_nr4_20, BR_nr4_21	Reach retailers to communicate the value of the certified product.	Bottler	Traceability, Alerting
FR_135	nr_4	BR_nr4_22	Receive certificate from producer	Supplier	Certification validation, Traceability
FR_136	nr_4	BR_nr4_22	User certification data for marketing purposes	Supplier	Certification validation, Traceability
FR_137	nr_4	BR_nr4_23, BR_nr4_24	Populate official databases with farm data and food health data from operators, as well as their certifications	Public authorities	Data management, Data management

FR_138	nr_4	BR_nr4_23, BR_nr4_24	Provide remote control, monitoring and traceability capabilities	Public authorities	Monitoring, Traceability
FR_139	nr_5	BR_nr5_2, BR_nr5_3, BR_nr5_5	Collect data, inspections on-site at all actors, issue results and upload to db	Public authorities (NVWA)	Data management, Data analysis
FR_140	nr_5	BR_nr5_2, BR_nr5_4, BR_nr5_6	Schedule inspections	Public authorities (NVWA)	Auditing, Monitoring
FR_141	nr_5	BR_nr5_2, BR_nr5_4, BR_nr5_6	Notify concerned actors about upcoming inspection/auditing	Public authorities (NVWA)	Alerting, Monitoring
FR_142	nr_5	BR_nr5_2, BR_nr5_3, BR_nr5_4	Ability to evaluate inspectors against EU regulations (such as (EG) nr. 178/2002)	Public authorities (NVWA)	Monitoring, Alerting
FR_143	nr_5	BR_nr5_2, BR_nr5_3, BR_nr5_4	Get product analysis to verify compliance towards certifications	Public authorities (NVWA)	Certification validation, Monitoring
FR_144	nr_5	BR_nr5_2, BR_nr5_3, BR_nr5_4, BR_nr5_6	Communicate complaints - accusations for certified producers or processors	Public authorities (NVWA)	Certification validation, Monitoring
FR_145	nr_5	BR_nr5_7, BR_nr5_8, BR_nr5_9, BR_nr5_10	View reports of inspection, audits reports, combined data collected from all actors in the supply chain such as declared volumes/quantities/prices	Producer, Industry	Data management, Monitoring
FR_146	nr_5	BR_nr5_7, BR_nr5_9, BR_nr5_10	Fill forms for inspection, report volumes, prices and food safety results to authorities, exchange reports with the certification bodies	Producer, Industry	Data management, Certification validation
FR_147	nr_5	BR_nr5_10, BR_nr5_12, BR_nr5_13	Trade certified processed products in the market	Industry	Certification validation, Negotiation support
FR_148	nr_5	BR_nr5_10, BR_nr5_12	Accept inspections by food authorities and certification bodies for compliance	Industry	Auditing, Monitoring
FR_149	nr_5	BR_nr5_10, BR_nr5_12	Set product specifications for products it sends to the market to retailers	Industry	Data management
FR_150	nr_5	BR_nr5_10	Contact consultants for audits, guide implementation of best practices against certification standards	Industry	Certification validation, Data analysis

ANNEX IV BUSINESS REQUIREMENTS

Business requirement no	Business Scenario	Business requirement	Actor	Component 1	Component 2	Component 3
BR_nr2_1	nr2	Collection of many different data with reference to the characteristics of the business and the final product	Producer	Data Management Services (T2.2)		
BR_nr2_2	nr2	Management of Data (data evaluation) deriving from different sources (with great variability) and with different characteristics (e.g. numerical, non-numerical - documents, etc.) to draw conclusions (e.g. results of analyses with legislative requirements, etc.)	Producer	Data Management Services (T2.2)	Data Management, Indexing & Processing (T3.5)	New Application Design & Deployment (T4.2)
BR_nr2_3	nr2	Need for constant updating of data and data sources and access to information	Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Population (T2.4)	Data Management, Indexing & Processing (T3.5)
BR_nr2_4	nr2	Recording of up-to-date and valid data assets (assets) of exploitation from a database of competent Authorities (e.g. Integrated Administration and Control System (IACS)) with limited access, provided by the producer	Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	Authorization & Access Control (T3.2)
BR_nr2_5	nr2	Acess to Real Time data, based on recorded plot data	Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_6	nr2	Validity of GLOBALGAP certificates from GLOBALGAP Database	Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)		

BR_nr2_7	nr2	Archiving the agreed specifications, on the delivered product (olives), for cooperation	Producer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr2_8	nr2	Interconnection of producer and processor recording systems, in terms of critical product data (dates of recent applications of phytosanitary preparations before harvest, harvest dates), tracking per batch and its connection with corresponding Certificates of Conformity	Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_9	nr2	Connecting channels to transfer information	Producer	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_10	nr2	Connecting the different databases from where the information is collected	Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_12	nr2	To personalize the data in the platform that the producer will use in his daily operations, in order to get customized information	Producer	Data Management, Indexing & Processing (T3.5)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Authorization & Access Control (T3.2)

BR_nr2_14	nr2	Replacing physical files with a complete digital database that will organize the daily work	Producer	Data Models & Interoperability (T2.1)	Data Management Services (T2.2)	
BR_nr2_15	nr2	Through the information that will be obtained about the needs of the market and the adaptation of the works in the direction of the production of products that will cover the above needs, an opportunity is created for possible finding of new customers	Producer	New Application Design & Deployment (T4.2)		
BR_nr2_16	nr2	Real-time data will be obtained and therefore decision-making time will be reduced	Producer	New Application Design & Deployment (T4.2)		
BR_nr2_17	nr2	Due to the digitization, the production process will be more effectively controlled in terms of the control of the financial data as well as statistical analyzes regarding possible deviations, improving the efficiency of production costs	Producer	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)
BR_nr2_18	nr2	Due to the common use of a single platform which is used individually for the producer and based on specific needs regarding the dissemination of information from the producer to the processor, the long-term collaborations between those involved in the supply chain are strengthened	Producer	New Application Design & Deployment (T4.2)		
BR_nr2_20	nr2	Segregation of data for assessment, in terms of those arising from control points critical to product safety (regular data), and those relating to functional control points (periodical data)	Food Processor	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	

BR_nr2_21	nr2	Need for constant updating of information for points that directly (critical limits for food hazards, recalls etc.) and indirectly (food regulation etc.) affect food safety	Food Processor	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_22	nr2	Easy access (e.g. to Certification Body) to aggregated data to assess compliance with food safety standards.	Food Processor	Data Management, Indexing & Processing (T3.5)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	
BR_nr2_23	nr2	Gathering of information from multiple producers (suppliers) regarding the quality characteristics of the raw material (olives) to maintain traceability.	Food Processor	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)
BR_nr2_24	nr2	Direct and immediate info for any non-conformity raised for the producer regarding its certified product, after he has delivered the raw material (olives) to the producer.	Food Processor	Data Management Services (T2.2)	Data Management, Indexing & Processing (T3.5)	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)
BR_nr2_25	nr2	Easy access and valid info relevant to operational licenses of each type of sub-actor who provides its services to the processor	Food Processor	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)		

BR_nr2_26	nr2	Valid info regarding the accreditation of the different kind of laboratories that verify the effectiveness of the FSMS	Food Processor	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_27	nr2	Categorizing and modifying all data in an editable format and transferring them in a common point of protected and controlled access.	Food Processor	Data Management, Indexing & Processing (T3.5)		
BR_nr2_28	nr2	Interconnection of processor’s and producer’s recording systems, in terms of critical product’s data (dates of recent applications of phytosanitary preparations before harvest, harvest dates), tracking per batch and its connection with corresponding Certificates of Conformity.	Food Processor	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr2_29	nr2	Reduction on the cost for maintaining an evergreen Food Safety Management Systems (FSMS) since the "The FSM" platform, will allow for easy access to critical info, which could be principle even when two or more different food safety standards interrelate between each other and are working in parallel (e.g. GLOBALGAP, FSSC 22000, IFS Food, etc.).	Food Processor			
BR_nr2_30	nr2	Improving the effectiveness of the food safety management system, by simultaneously checking all the agreed obligations of the cooperating suppliers, linking them to deviations from the requested specifications, as well as depicting these deviations in terms of financial results.	Food Processor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Data Management, Indexing & Processing (T3.5)	New Application Design & Deployment (T4.2)

BR_nr2_31	nr2	Replacing physical files with a professional digital database that is easy to use and more efficiently organize the daily work, as it can be interoperable with other central management applications (eg data logger, etc.).	Food Processor	Data Models & Interoperability (T2.1)	Data Management Services (T2.2)	
BR_nr2_32	nr2	Reduction of the decision-making time because real-time data can be obtained. For example, information on accredited laboratories, supplier certifications and their certification status, databases, etc	Food Processor	New Application Design & Deployment (T4.2)		
BR_nr2_33	nr2	Capability for finding new partnerships and cooperation, through the information that will be obtained relevant to the current market needs and adaptation of the operational works in the direction of producing products with characteristics that will cover the above needs.	Food Processor	New Application Design & Deployment (T4.2)		
BR_nr2_34	nr2	Strengthen long-term partnerships between those involved in the food supply chain who are users of an effective platform that can ensure data reliability and users' private data protection.	Food Processor	New Application Design & Deployment (T4.2)		
BR_nr2_35	nr2	Use of processed (aggregated) data to assess compliance with the requirements of certified schemes	Certification Body	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Management Services (T2.2)	
BR_nr2_36	nr2	Need for access to up-to-date data from different sources and access to information relevant to new and amended legislation, new schemes' version, supervision of the competence of inspectors, accreditation issues etc.	Certification Body	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Management Services (T2.2)	

BR_nr2_37	nr2	The Certification Body has to use a representative sample of the processed' (aggregated) data in order to evaluate compliance with product specifications	Certification Body	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Management Services (T2.2)	API Gateway (T2.2, T3.4, T3.5, T4.3)
BR_nr2_38	nr2	Collection of updated and valid data relevant to the farm operation or / and the processing unit, deriving from different official database of the corresponding public authorities (e.g. Intergrade Administration and Control System, General Registry etc.) under limited access given by producer/ processor.	Certification Body	API Gateway (T2.2, T3.4, T3.5, T4.3)		
BR_nr2_39	nr2	Collection of needed documentation that the CB requires to obtain prior to the certification decision.	Certification Body	New Application Design & Deployment (T4.2)	Data Population (T2.4)	
BR_nr2_40	nr2	Connecting different methods of receiving and sending information, in order to facilitate the collection of documentation during the certification process	Certification Body	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Secure Voltage (T3.3)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)
BR_nr2_45	nr2	Have direct and official information on the findings of the National Audit Authorities in certified Producers, Processors and Retailers	Certification Body	API Gateway (T2.2, T3.4, T3.5, T4.3)		
BR_nr2_46	nr2	More easily to obtain all the evidence for the justification of compliance criteria (eg personal data of the producer, application files, etc.)	Certification Body	Secure Voltage (T3.3)	Authorization & Access Control (T3.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information

						Exchange (T3.4)
BR_nr2_47	nr2	Have access to a valid and up-to-date all-in-one database (legal requirements, accreditation for laboratories, MRL limits, official PPP approvals)	Certification Body	Secure Voltage (T3.3)	Data Management Services (T2.2)	
BR_nr2_48	nr2	Immediate profile of a stakeholder (food company) in terms of its certification history, its size so that it would be easier to analyze the audit risk e.g. in terms of taking a sample for analysis and control / verification	Certification Body	Secure Voltage (T3.3)	Data Management Services (T2.2)	
BR_nr2_49	nr2	Increase audit's efficiency, in terms of time and cost of audit e.g. by aligning certification processes with "TheFSM", to increase efficiency and reduce the required resources of the certification mechanism (audit plan and notification of the auditor's appointment, unexpected or urgent changes in the audit scheduling etc.)	Certification Body	New Application Design & Deployment (T4.2)		
BR_nr2_50	nr2	Effective use and re-examination of all previous customers' audit findings, which are grouped into certain categories 'to further highlight the areas of high risk / concern for each subsequent audit, performed by different audit teams.	Certification Body	Data Management Services (T2.2)	Data Management, Indexing & Processing (T3.5)	

BR_nr2_51	nr2	Access to detailed information about the final shelf product and its correlation with critical factors treated by the previous stakeholders in the food supply chain, thus to maintain a robust traceability system allowing efficient withdrawal of products.	Retailer	Data Management, Indexing & Processing (T3.5)	New Application Design & Deployment (T4.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)
BR_nr2_52	nr2	Reduction of the decision-making time since up-to-date data can be obtained relevant his contracted suppliers. For example, fully documented quick supplier's risk assessment can be conducted by direct access to principle information about their certification status, their business performance etc., through real-time data and reliable stored data (statistical analysis). having	Retailer	New Application Design & Deployment (T4.2)		
BR_nr2_53	nr2	The availability of fully traced downstream information improves transparency and prevents unfair trade practices that have significant implications for consumers and the environment.	Retailer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr2_54	nr2	Strengthen long-term partnerships between the users of the platform that can ensure data reliability and users' private data protection.	Retailer	New Application Design & Deployment (T4.2)		

BR_nr2_55	nr2	Enhance customers trust on the retailer's brand name, by presenting (with limited access to the company's profile in the platform) some important data relevant to the quality assurance actions taken by the company (e.g. additional laboratory test etc.)	Retailer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	New Application Design & Deployment (T4.2)	
BR_nr2_56	nr2	Access to detailed information about the final shelf product and its correlation with critical factors treated by the previous stakeholders in the food supply chain, thus to maintain a robust traceability system allowing efficient withdrawal of products.	Retailer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	New Application Design & Deployment (T4.2)	
BR_nr2_57	nr2	Reduction of the decision-making time since up-to-date data can be obtained relevant his contracted suppliers. For example, fully documented quick supplier's risk assessment can be conducted by having direct access to principle information about their certification status, their business performance etc., through real-time data and reliable stored data (statistical analysis).	Retailer	New Application Design & Deployment (T4.2)		
BR_nr2_58	nr2	The availability of fully traced downstream information improves transparency and prevents unfair trade practices that have significant implications for consumers and the environment.	Retailer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	New Application Design & Deployment (T4.2)	
BR_nr1_1	nr1	To access information regarding findings of the inspection of suppliers in the food chain	Retailer	Authorization & Access Control (T3.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information	

					Exchange (T3.4)	
BR_nr1_2	nr1	Access to current status of food supply actors regarding audit results of certify organisations	Retailer	API Gateway (T2.2, T3.4, T3.5, T4.3)	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)
BR_nr1_3	nr1	Innovative tools to support risk monitoring	Retailer	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr1_4	nr1	Improve the risk assessment procedure for each supplier	Retailer	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr1_5	nr1	Establishment of a trusted profile as a supplier to retailers	Supplier	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_1	nr3	Accelerate the preparation and realization of certification	Producer	New Application Design & Deployment (T4.2)		
BR_nr3_2	nr3	Enable the precise finding of required certificates and seal of approval required by a specific customer	Producer	Secure Voltage (T3.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_3	nr3	Gives an estimation of costs and expenditures in respect to the certification process.	Producer	New Application Design & Deployment (T4.2)		
BR_nr3_4	nr3	Supports realization of remote audits	Producer	Blockchain-powered Smart Contracting Layer Secure		

				Storage & Information Exchange (T3.4)		
BR_nr3_5	nr3	Allows integrated data assessments for fact driven management of the business.	Producer	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_6	nr3	Enable a comprehensive just on time evaluation of data from different sources and stakeholders which supports fast decision processes	Producer	Data Management Services (T2.2)		
BR_nr3_7	nr3	Provides validated data of all stakeholder	Producer	New Application Design & Deployment (T4.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Authorization & Access Control (T3.2)
BR_nr3_8	nr3	Enable just-on-time traceability of products	Producer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_9	nr3	Accelerate the preparation and realization of certification	Food Processor	New Application Design & Deployment (T4.2)		
BR_nr3_10	nr3	Enable the precise finding of required certificates and seal of approval required by a specific customer	Food Processor	Secure Voltage (T3.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_11	nr3	Gives an estimation of costs and expenditures in respect to the certification process.	Food Processor	New Application Design & Deployment (T4.2)		

BR_nr3_12	nr3	Supports realization of remote audits	Food Processor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_13	nr3	Allows integrated data assessments for fact driven management of the business.	Food Processor	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_14	nr3	Enable a comprehensive just on time evaluation of data from different sources and stakeholders which supports fast decision processes	Food Processor	Data Management Services (T2.2)		
BR_nr3_15	nr3	Provides validated data of all stakeholder	Food Processor	New Application Design & Deployment (T4.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Authorization & Access Control (T3.2)
BR_nr3_16	nr3	Enable just-on-time traceability of products	Food Processor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_17	nr3	Accelerate the preparation and realization of certification	Distributor	New Application Design & Deployment (T4.2)		

BR_nr3_18	nr3	Enable the precise finding of required certificates and seal of approval required by a specific customer	Distributor	Secure Voltage (T3.3)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_19	nr3	Gives an estimation of costs and expenditures in respect to the certification process.	Distributor	New Application Design & Deployment (T4.2)		
BR_nr3_20	nr3	Supports realization of remote audits	Distributor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_21	nr3	Allows integrated data assessments for fact driven management of the business.	Distributor	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_22	nr3	Enable a comprehensive just on time evaluation of data from different sources and stakeholders which supports fast decision processes	Distributor	Data Management Services (T2.2)		
BR_nr3_23	nr3	Provides validated data of all stakeholder	Distributor	New Application Design & Deployment (T4.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Authorization & Access Control (T3.2)
BR_nr3_24	nr3	Enable just-on-time traceability of products	Distributor	Blockchain-powered Smart Contracting Layer Secure Storage &		

				Information Exchange (T3.4)		
BR_nr3_25	nr3	Accelerate the preparation and realization of certification	Certification Body	New Application Design & Deployment (T4.2)		
BR_nr3_26	nr3	Enable the understanding of the specific requirements of an organization.	Certification Body	New Application Design & Deployment (T4.2)		
BR_nr3_27	nr3	Direct interaction of organizations, which requires certification and certification bodies, at the platform facilitate acquisition processes of certification bodies.	Certification Body	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_28	nr3	Boost the efficiency in preparation of the audit process	Certification Body	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	API Gateway (T2.2, T3.4, T3.5, T4.3)
BR_nr3_29	nr3	Boost the efficiency of audit realization	Certification Body	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	
BR_nr3_30	nr3	Supports realization of remote audits	Certification Body	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_31	nr3	Provides validated data of all stakeholder.	Certification Body	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Secure Voltage (T3.3)	Authorization & Access Control (T3.2)

BR_nr3_32	nr3	Enable just-on-time traceability of products.	Certification Body	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr3_33	nr3	Deliver a better overall view of the ability of an audited organization and therefore better audit results	Certification Body	New Application Design & Deployment (T4.2)	Data Management, Indexing & Processing (T3.5)	API Gateway (T2.2, T3.4, T3.5, T4.3)
BR_nr3_34	nr3	Accelerate results regarding compliance of suppliers	Retailer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Secure Voltage (T3.3)	Authorization & Access Control (T3.2)
BR_nr3_35	nr3	Allow detailed risk analysis of delivered products (if necessary)	Retailer	New Application Design & Deployment (T4.2)		
BR_nr3_36	nr3	Avoid unnecessary product recalls through possibility of integrated data evaluation through the whole food chain	Retailer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_1	nr4	Transformation of the reporting to digital reporting	Inspector/Auditor	Data Processing Services (T2.3)		
BR_nr4_2	nr4	Quick access to the official info of the National Control Authorities	Inspector/Auditor	API Gateway (T2.2, T3.4, T3.5, T4.3)		
BR_nr4_3	nr4	Access to a database which uncludes all the info regaring the product (legal requirements, accreditation certifications for laboratories, specific parameters)	Inspector/Auditor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Secure Voltage (T3.3)	Authorization & Access Control (T3.2)

BR_nr4_4	nr4	Increase reliability by allowing the interaction of data sources from different CBs	Inspector/Auditor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_5	nr4	Verification of a digital report	Certification Committee	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_6	nr4	Quick access to the official info of the National Control Authorities	Certification Committee	API Gateway (T2.2, T3.4, T3.5, T4.3)		
BR_nr4_7	nr4	Increase reliability by allowing the interaction of data sources from different CBs	Certification Committee	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management Services (T2.2)	
BR_nr4_8	nr4	Replace the hardcopy archives to a digital database	Farmer/Producer	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management Services (T2.2)	
BR_nr4_9	nr4	Traceability of input supliers	Farmer/Producer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_10		Traceability of products until the consumer	Farmer/Producer	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		

BR_nr4_11	nr4	Access to Real Time Data in order to control and minimize the responsive time of decision making regarding the porduction processes	Farmer/Producer	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Processing Services (T2.3)	
BR_nr4_12	nr4	Replace the hardcopy archives to a digital database	Winegrowers	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management Services (T2.2)	
BR_nr4_13	nr4	Traceability of input supliers	Winegrowers	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_14	nr4	Traceability of products until the consumer	Winegrowers	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_15	nr4	Access to Real Time Data in order to control and minimize the responsive time of decision making regarding the porduction processes	Winegrowers	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	Data Processing Services (T2.3)	
BR_nr4_16	nr4	Traceability of input supliers	Winemakers	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_17	nr4	Traceability of products until the consumer	Winemakers	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		

BR_nr4_18	nr4	Accumulate all the information regarding the production practices, processes, certifiactions to a digital database	Winemakers	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management Services (T2.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)
BR_nr4_19	nr4	Traceability of wine regarding the production practices, processes, certifiactions	Bottlers	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_20	nr4	Traceability of products until the consumer	Bottlers	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_21	nr4	Accumulate all the information regarding the production practices, processing methods, certifiactions to a digital database	Bottlers	API Gateway (T2.2, T3.4, T3.5, T4.3)	Data Management Services (T2.2)	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)
BR_nr4_22	nr4	Traceability of wine regarding the wine origin, production practices, processing methods, certifiactions	Distributor	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)		
BR_nr4_23	nr4	Check product data and verify compliance with certification regulations.	Public authorities	API Gateway (T2.2, T3.4, T3.5, T4.3)		

BR_nr4_24	nr4	Connect public bodies, authorities and certification bodies.	Public authorities	Blockchain-powered Smart Contracting Layer Secure Storage & Information Exchange (T3.4)	Data Management, Indexing & Processing (T3.5)	
BR_nr5_1	nr5	Support NVWA inspectors to predict when to check, what, where	Public Authorities (NVWA)	TheFSM Platform	Data Processing Services (T2.3)	
BR_nr5_2	nr5	Digitization of the inspection and certification information flow in the broiler meat supply chain in the Netherlands	Public Authorities (NVWA)	TheFSM Platform	Data Processing Services (T2.3)	
BR_nr5_3	nr5	Provide past audit performance per actor (producers, suppliers, etc.)	Public Authorities (NVWA), Producer, Industry, Certification body	Data Connectors (T2.1, T2.2, T2.3, T2.4, T3.5, T4.3)	TheFSM Platform	
BR_nr5_4	nr5	Tools to support risk-based monitoring	Public Authorities (NVWA)	TheFSM Platform	Data Processing Services (T2.3)	
BR_nr5_5	nr5	Have an all in one database (legal requirements, accreditation certs for laboratories, MRL Limits, official PPP Approvals)	Public Authorities (NVWA)	TheFSM Platform	Integration with Data Platform (T4.3)	
BR_nr5_6	nr5	Increase the effectiveness (time/cost) of the audits (Align certification processes with the “TheFSM”, to increase effectiveness and reduce the needed resources of the certification mechanism).	Public Authorities (NVWA)	TheFSM Platform	Data Models & Interoperability (T2.1)	

BR_nr5_7	nr5	Provide meat as certified product	Producer	TheFSM Platform	Data Models & Interoperability (T2.1)	
BR_nr5_8	nr5	Assessment of producers by food authority and certification bodies to decide to what extent they comply with law and certification standards	Producer, Certification Body, Public authorities	TheFSM Platform	Data Models & Interoperability (T2.1)	
BR_nr5_9	nr5	Replacement of the hardcopy archives to a digital database	Producer, Industry, certification bodies	TheFSM Platform	Integration with Data Platform (T4.3)	
BR_nr5_10	nr5	Digitalize the certification flow of information	Industry, All actors	TheFSM Platform	Integration with Data Platform (T4.3)	
BR_nr5_11	nr5	Have all in one database (suppliers of packaging material etc.)	Industry	TheFSM Platform	Integration with Data Platform (T4.3)	
BR_nr5_12	nr5	Direct access to market needs (Up to date info) & new clients	Industry	TheFSM Platform	Data Management Services (T2.2)	
BR_nr5_13	nr5	Up-to-date communication channel with traders (retailers) regarding agreed timelines, terms & conditions	Industry	TheFSM Platform	Data Models & Interoperability (T2.1)	