SOFIE - Secure Open Federation for Internet Everywhere
779984

DELIVERABLE D5.1

Baseline System and Measurements

Project title	SOFIE – Secure Open Federation for Internet Everywhere
Contract Number	H2020-IOT-2017-3 – 779984
Duration	1.1.2018 – 31.12.2020
Date of preparation	29.6.2018
Author(s)	Ioannis Oikonomidis (SYN), Helen C. Lelligou (SYN), Giuseppe Raveduto (ENG), Vincenzo Croce (ENG), Francesco Bellesini (EMOT), Michele Pagliaccia (EMOT), Francesca Santori (ASM), Alessio Cavadenti (ASM), David Mason (ROV), Priit Anton (GT), Dmitrij Lagutin (AALTO), Santeri Paavolainen (AALTO), Tommi Elo (AALTO), Antonis Gonos (OPT), Elias Kanakis (OPT), Antonis Xagoraris (OPT)
Responsible person	Ioannis Oikonomidis (SYN), oikonomidis@synelixis.com
Target Dissemination Level	Public
Status of the Document	Completed
Version	1.00
Project web-site	https://www.sofie-iot.eu/

Table of Contents

1 Introduction

The pilots in the SOFIE project are responsible for demonstrating the applicability of SOFIE's reference platform in different real-life use cases. The pilots' aim is to provide an overall evaluation of the SOFIE framework by utilizing the Reference Platform and the Business Platforms that will be developed conforming to the Architecture and Framework specifications.

This deliverable describes the baseline system of each pilot, including a high-level overview, the technologies that are to be used (the ones that already exist as well as those that are under development), the related scenarios and use cases, describing in detail the pre- and post-conditions to be met, the key actors involved, the metrics to be measured and the objective of each scenario as well as a brief overview of the data to be captured and the collection methodology. The captured data is in line with D6.5 Data Management Plan document which includes, among others, Fair Data guidelines and policies.

This deliverable does not include descriptions of any Distributed Ledger Technologies (DLTs) that will be used; their use within each pilot context will be defined and described in the next pilot deliverable along with each pilot overall architecture and components. However, the reader can refer to deliverable D2.1 (State of the Art) for detailed descriptions of all the candidate DLTs that are currently under consideration for the pilots.

The pilot phase will combine the deployment of federated IoT platforms with DLTs which will be able to interact intra-pilot as well as inter-pilot via SOFIE's Business Platforms. SOFIE will demonstrate four pilots from three sectors:

- Food Supply Chain pilot (Greece)
- Energy pilot (Estonia)
- Energy pilot (Italy)
- Mobile Gaming pilot (Finland)

The first outcomes of the pilots will form the content for the next Work Package 5 deliverable D5.2, which will include an Initial Evaluation of the SOFIE framework.

1.1 Structure of the Deliverable

Chapter 2 provides high-level descriptions for each pilot. Chapter 3 includes a more thorough description for each pilot, including scenarios and use cases that will be implemented in the pilots. Finally, Chapter 4 gives a brief overview of the data that will be collected during the pilots.

1.2 List of Acronyms

BP   Business Platform (for pilots)

DLT   Distributed Ledger Technology

DSO   Distribution System Operator

EV   Electric Vehicle

EVSE   Electric Vehicle Supply Equipment

IoT   Internet of Things

TSO   Transmission System Operator

RP   Reference Platform

2 Baseline System

This section presents the four pilots that will be deployed in SOFIE, the description of each pilot setup and the main technology platforms that will be utilized. In addition, we split (where applicable) the Technologies section into two subsections, one where the technologies/platforms that exist already and will be used as is or with small modifications are described, and another where the technologies/components that will be developed for SOFIE are briefly described. The candidate DLT technologies have been identified and thoroughly described in deliverable D2.1 - State Of The Art, so the reader can refer to that deliverable for their detailed description. From those, Ethereum and Guardtime KSI®Blockchain have already been selected to be used in the pilots while Hyperledger Fabric and IOTA have been identified as main candidates and are currently being considered along with other candidates. The main approach in all pilots is to interconnect the federated IoT platforms (each of them utilizing DLT) via a BP that follows the specifications set by SOFIE's architecture and framework that will be defined and described in SOFIE deliverables D2.2 and D2.3.

2.1 Food Chain Pilot (Greece)

2.1.1 Pilot Description

This pilot will serve as a proof-of-concept for the validation and demonstration of the capabilities of the SOFIE platform to combine and interconnect, in a secure way, different IoT platforms that are involved in the food chain supply sector. The pilot will consider the field-to-fork route that a specific type of food product follows and will involve the entire IoT infrastructure that is triggered along this path. The path from field to fork can be split into 5 segments:

1. **Table Grapes Field (TGF)**. This is a table grape field located in Corinth region, Greece. TGF is where SynField hardware will be deployed to monitor the crop. The deployment will consist of one SynField Head Node which includes, among others, temperature, humidity, wind speed/direction, rainfall, and soil moisture sensors. The data from all these sensors will be transmitted to and stored at the SynField Cloud Server.
2. **Transportation Route A (TRA)**, from TGF to the Storage & Distribution Center. This segment includes the path from TGF to SDC. This path will be static and predefined, subject to change only due to unpredictable situations; the total transportation time is typically between 1.5 and 3 hours. It will be traversed by vehicles equipped with GPS tracking sensors as well as temperature sensors. Data from those sensors will be stored at the Transportation IoT platform.
3. **Storage & Distribution Center (SDC)**. SDC is located in the Attica region of Greece. This is where the smart boxes with table grapes will be stored until they are transported to the Supermarket. In SDC there will be an extended version of Optimum's Aberon IoT platform deployed, monitoring, among others, temperature and presence of the boxes. The data will be transmitted to and stored at the Aberon Cloud Server.
4. **Transportation Route B (TRB)**, from SDC to the Supermarket premises. This segment includes the path from SDC to SM. This path will be static and predefined, subject to change only due to unpredicted situations while the transportation time varies from 30 minutes to 1.5 hours. It will be traversed by vehicles equipped with GPS tracking sensors as well as temperature sensors. Data from those sensors will be stored at the Transportation IoT platform.
5. **Super Market (SM)**. SM is the goods' final destination in the pilot's context. SM is located in Attica region of Greece. There are two areas of interest in the supermarket; the area where the boxes are kept until they are placed in the customer area and the

customer area where the table grapes are available for the customers. Before the table grapes are removed from the smart boxes to be placed to the customers' area, QR labels will be created (refer also to section 3.1) and applied on the table grape packages so that supermarket customers can retrieve this information using their smartphones. The actor roles involved in this segment are those of the supermarket employee and the supermarket customer.

Figure 1 provides an overview of the five segments of the Food Chain Pilot:

Figure 1: Food Chain Segments

Table grapes will be collected in packages and placed in "smart" boxes which will be equipped with RFID readers. Those boxes will traverse the whole path; therefore, they cannot be regarded as a segment-specific entity but rather as an inter-segment entity. The RFID tags that will be used (cards, keyrings, etc) will have been given to all the actors that need to interact with the boxes. Each tag will be uniquely mapped to an actor (i.e. the id of the tag will be attributed to a specific person) to provide a means of user identification. Data from the RFID readers (tag swipes) will be transmitted to the Transportation IoT platform since it is the IoT platform that will be "present" in all actor interactions that involve boxes.

2.1.2 Technologies

2.1.2.1 Existing entities

SynField Platform

The SynField platform is a cloud-based platform implemented by Synelixis. Given the SynField platform, any user is able to register a field and setup the network of the installed SynField nodes (devices) on it. Synelixis is the manufacturer of two types of nodes: the head node that is the gateway towards the Internet and the peripheral node that is able to communicate only with a head node that belongs to the same network. Figure 2 presents an indicative network of nodes (in the left side) and how these are connected. Typically, each field contains one head node and optionally, one or more peripheral nodes. The head-to-peripheral (and vice-versa) communication is performed using RF technologies while the head node is able to communicate (upload measurements, retrieve configuration and commands) with the SynField platform (REST API) through WIFI or GPRS/3G.
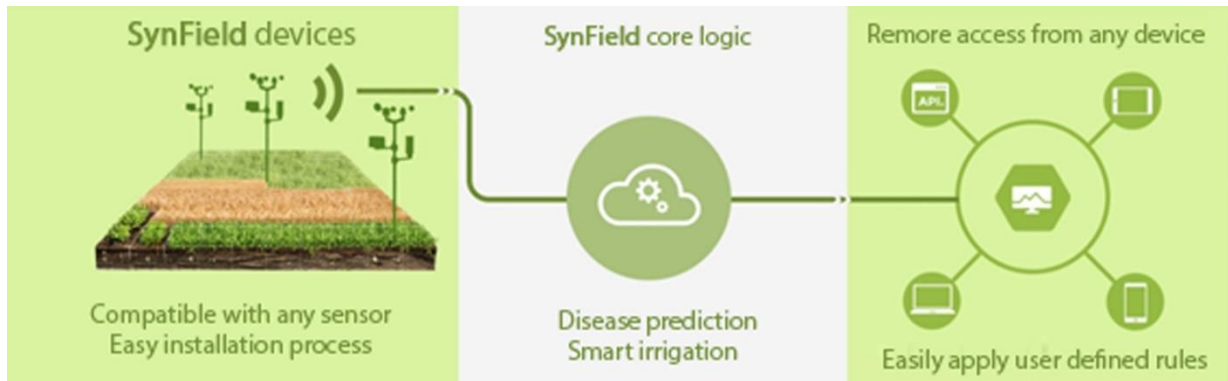
Figure 2: SynField ecosystem

Each node, head or peripheral one, can retrieve measurements from one or more wired installed sensors. The exact number of the sensors that may be installed on each node depends on its type, head versus peripheral, and its hardware version. SynField nodes are compatible with various types of sensors; the only limitation is the interface of the sensors. Currently, ADC, PULSE, I2C and SERIAL sensors are fully supported using RJ connectors. Apart from the sensors, the SynField nodes are compatible with a set of actuators. Also, the SynField cloud platform has been extended so as to support external devices. As external devices we consider those that are not compatible with or not plugged in the SynField nodes.
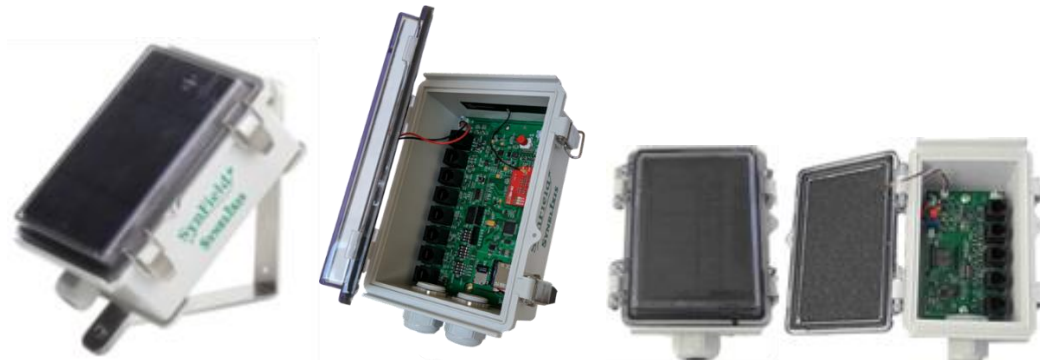
Figure 3: SynField Head Node (left) and Peripheral Node (right)

As shown in Figure 3, SynField nodes are compact and self-contained. They feature a Photovoltaic panel in order to be autonomous and a Regulated Lead-Acid (Lithium) battery to operate for days even without being charged. Moreover, the electronic circuit is located in a waterproof box (IP-67), which protects the system from rain, snow and hail.

Figure 4 provides a typical SynField installation, where one headnode and multiple peripherals in ad-hoc networking architecture are installed.
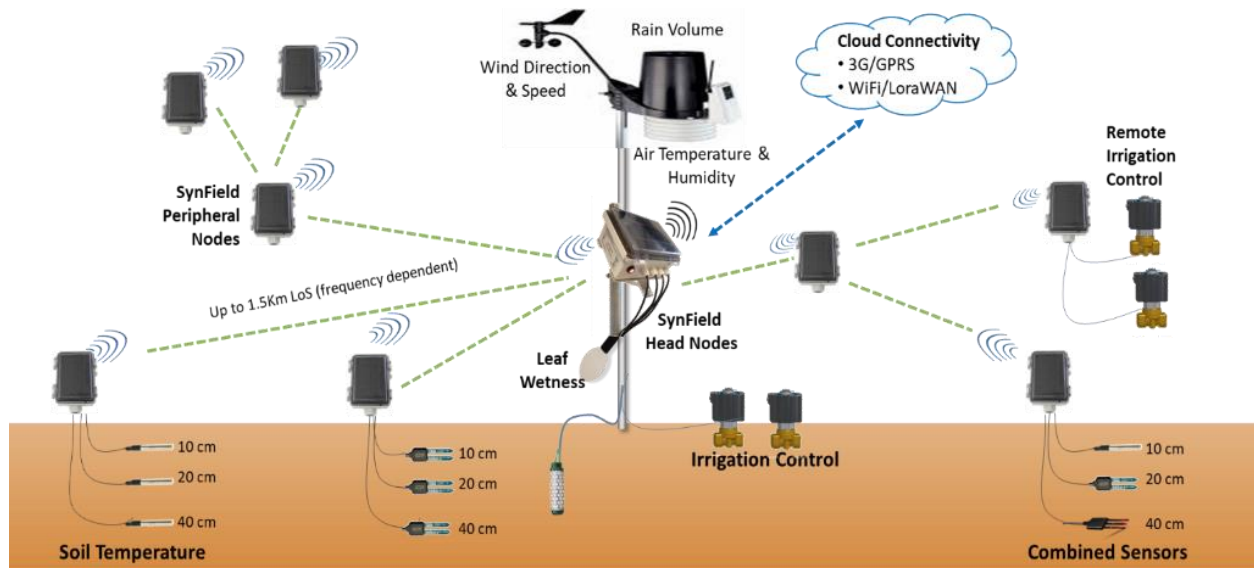
Figure 4: Typical SynField installation

Aberon Platform

Aberon WMS is a flexible Warehouse Management System, provided by Optimum, and constitutes the core of the solutions provided for managing and optimizing the supply chain. Aberon WMS is friendly, easy-to-use, flexible and modular.

Aberon WMS can utilize a wide range of different equipment and automation techniques, from basic warehouses, in field terminals and fully automated distribution centers.
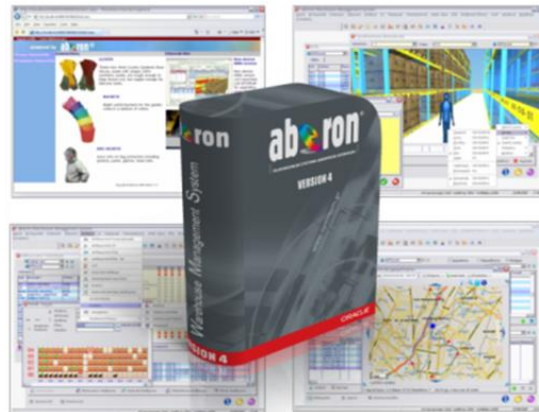
Figure 5: Aberon WMS commercial package

Inbound Management is responsible for identifying, labelling, and receiving incoming materials (final products, semi-finals, raw materials) in the warehouse and for put-away. The inbound management module supports preparation of receipts, barcode labelling of the logistics units, management of pre-receiving ASN (Advanced Shipped Notices), standardization of storage units, as well as cross docking functions.

Aberon WMS uses wireless barcode technology and RFID technology to monitor incoming products or materials in the warehouse.

Typically, the attribute identification of consumer goods is achieved by identifying and preparing barcode Labels conforming to the GS1 Standard.

Aberon WMS can also monitor and validate the distinct attributes of SKUs within the warehouse.

The main mission of a Warehouse or a Distribution Centre is to accurately process the orders by making efficient use of the available warehouse resources (employees and equipment). Aberon WMS manages all functions of preparing picking orders, such as order data entry, order processing, inventory blocking, order grouping, load and packaging, and order pre-routing.

A main feature of Aberon WMS is the maintenance of the products' lot tracking (FIFO-FEFO) and the traceability management. The system supports all order picking types and methods, such as picking per order, per customer group, per loading wave, per route, on an aggregate basis, per picking zone, per lot or based on the special designation etc. Order picking via Aberon WMS is made using wireless terminals, RFID terminal, carton labels, coupons, picking lists, pick-by-light, or pick-cart systems and can be integrated with weighing scale devices and other warehouse automation systems.
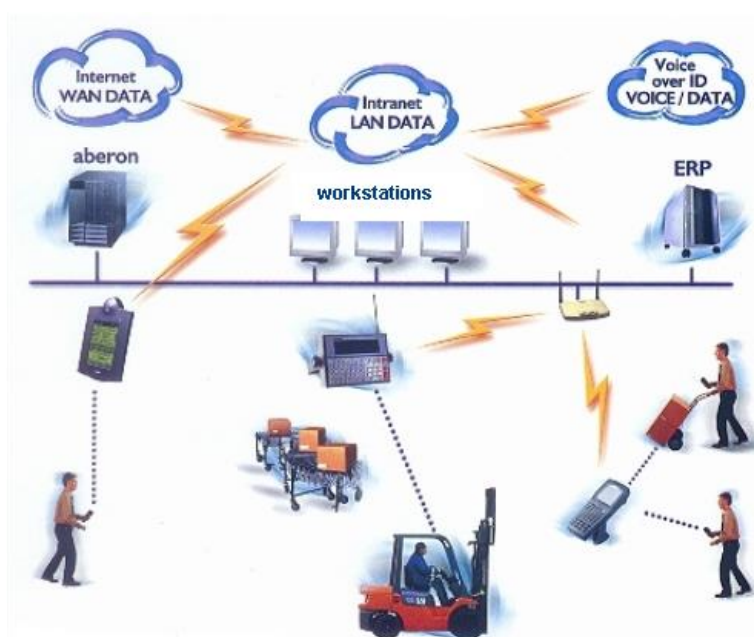
Figure 6: Aberon WMS deployment

Aberon WMS coordinates and optimizes the workload in the warehouse by creating work tasks that are sent in real-time to the wireless terminals of forklifts and pedestrian operators. It allows Distribution Centre officers to monitor the performance rates of the warehouse resources and enables them to draw correct forecasting and reviews of all works.

Aberon WMS allows two-way and real-time communication with external software and hardware systems such as ERP systems, MRP systems, wireless networks, weighing scales, ASRS (Automatic Storage and Retrieving Systems), conveyor belts, sorters, pick-by-light systems, pick-carts etc. Aberon WMS records in detail all tasks and processes, contributing to the detection of errors and the extraction of statistics helping management to make proper decisions.

Transportation IoT Platform

The transportation IoT platform will be based on the IoT component that SYN developed for the purposes of the InLife H2020 project (http://www.inlife-h2020.eu/index.php/en/).

The InLife IoT component aims to deliver a flexible and scalable data and resource management framework guaranteeing consistency, security, and reliability in the development of smart IoT applications. In InLife, the IoT component is implemented as a cloud solution, where the sensing devices expose application-agnostic elementary functionality while the

application logic is entirely deployed in the cloud environment. The primary role of the IoT component is to provide a reliable and scalable cloud-enabled IoT environment to effectively manage data acquired from the physical space and support the implementation of smart IoT applications.

The functional block diagram of the IoT component is shown in Figure 7. As shown in the figure, the IoT component is implemented in a modular way, consisting of three main modules:

- The IoT access API
- The IoT cloud server
- The (local) IoT gateways
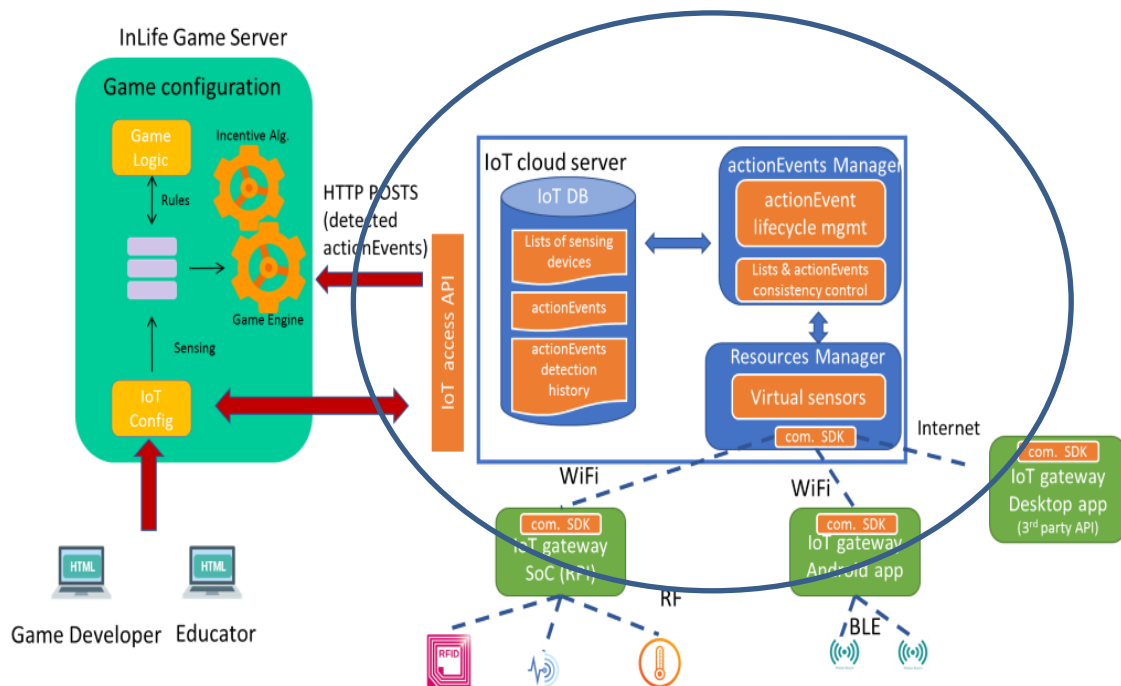
Figure 7: Functional block of the IoT component in the InLife EU H2020 project

2.1.2.2　Entities under development

DLT-enhanced IoT platforms

The IoT platforms described in the previous subsection do not have DLT capabilities. Therefore, we plan to enhance all the IoT platforms with support for DLTs. Even though the selection of the technologies has not been finalized yet (expected to be finalized during the next two months), the candidates that have so far qualified are Ethereum, Hyperledger Fabric, and Guardtime KSI®Blockchain (the final decision to be made in the next two months). These will keep (meta)data from the original IoT platforms' and make it available through the Data history marketplace.

Data History Marketplace

This will be the Business Platform (BP) for this pilot, combining data from the IoT platforms involved so as to provide services offering product history and description as well as auditability and traceability services. This platform will allow the various actors of the scenarios of this pilot (described in section 3.1.3) to perform tasks/actions (described in section 3.1) that require interaction with data collected along the path from-field-to-fork.

2.2 Energy Pilot (Estonia)

2.2.1 Pilot Description

This core idea of this pilot is to provide a proof-of-concept for secure data exchange and agreements to data access rights between smart meter infrastructure owners and energy service providers (Intermediaries, distributors, brokers). The pilot will develop and use the capabilities of the SOFIE federated platform for the validation and demonstration of the defined scenarios and use-cases.

Pilot will be based on the Estfeed open software platform for energy consumptions monitoring and management from the customer (consumers/ prosumers) side. It consists of 700 000 smart meters in Estonia. This system is operated by energy company Elering (Transmission system operator in Estonia). There will be data exchange demonstration with two different types of systems: one similar to Elering smart meter platform (Dutch smart meter platform operated by TenneT) and the other smaller system with only a few thousand smart meters in place. The goal is to prove, how different energy grid actors can provide reliable smart meter data feeds based on the consent of smart meter owners.

The concept of data exchange is show on the Figure 8 where energy market suppliers and distributors can get access to energy consumption from Estfeed platform. During the SOFIE energy pilot there will a demonstration on:

a) how a distributor from another country can access the smart meter data
b) how different IoT platform (like Estfeed) can exchange data to Estonian system
c) how the small smart meter grid, like local windfarm can provide trusted and verified data to larger systems.
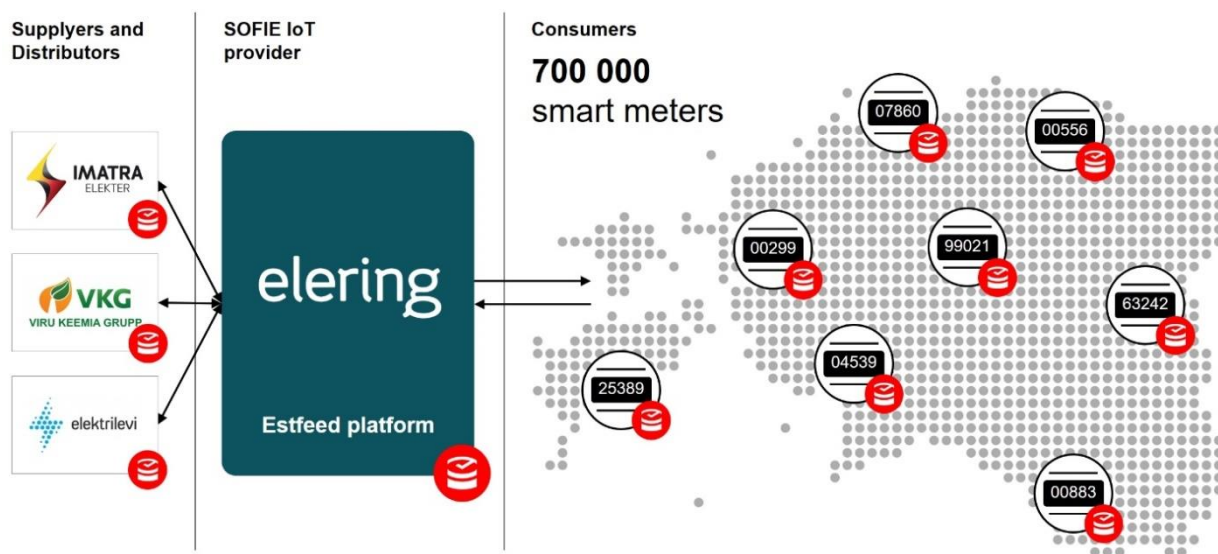
Figure 8: Smart meter data exchange platform

Estonian energy pilot goal is to prove how using SOFIE federated platform with blockchain technology can improve the existing energy sector platforms:

- Integrity of energy consumption data and transparency mechanisms.
- Provide trust between energy market participants.
- Protect the entity (Elering, TenneT) who provide access to smart meter data from court cases.
- Provide energy consumption readings which are correct beyond dispute.

- Provide the provenance throughout the infrastructure that energy company is responsible for until delivery is made to 3rd party environment.

Furthermore, the current energy pilot should investigate and demonstrate opportunities how use of new technology can allow more open access to metering data and therefore enable 3rd parties to develop applications on top of smart meter readings federated platform provided by the SOFIE framework. This could initiate a really distributed energy trading marketplace to build flexible energy services

2.2.2 Technologies

Smart meters

There are two difference data sources regarding the smart meters. Smart grid operators have various types of smart meters in place and during the SOFIE energy pilot there will not be focus on the hardware part of these systems. Platform owners will be responsible for data input from the system.

Another data source is related to small smart meter instances where a chipset RL78/I1B meters will be used. This smart meter setup will demonstrate the full data provenance chain form the smart meter chipset to the agreed parties who exchange the information.

KSI® Blockchain

One of the core elements used in the pilot is KSI®Blockchain, to provide the integrity of smart meter data, authentication process and agreements between parties.

KSI®Blockchain is a method and a globally distributed network infrastructure for the issuance and verification of KSI signatures.

Unlike traditional digital signature approaches, e.g. Public Key Infrastructure (PKI), that depend on asymmetric key cryptography, KSI uses only hash-function cryptography, all owing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain. A blockchain is a distributed public record of events; an append-only record of events where each new event is cryptographically linked to the previous. New entries are created using a distributed consensus protocol.

A user interacts with the KSI system by submitting a hash-value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, integrity of the signed data, as well as attribution of origin i.e. which entity generated the signature.

A user interacts with the KSI system by submitting a hash-value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, integrity of the signed data, as well as attribution of origin i.e. which entity generated the signature.

Elering Estfeed platform

This is an existing platform that serves as a data source for SOFIE energy pilot. Estfeed solution connects all smart meter data in Estonia together and through the platform participants can interface with various data sources and these data can be used in the applications desired.

There are various in production technologies used in Estfeed platform like:

- Estonian X-Road Data Exchange Layer operated by The Estonian Information System Authority. More information can be found here: https://www.ria.ee/en/x-road.html
- Estfeed Service Payload Formats Y-1028-8 and Estfeed Contract Controller Service. Y-1028-7 developed and owned by Cybernetica AS

- ETSI. ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf

More information about the Estfeed platform can be found here: https://elering.ee/en/smart-grid-development.

2.3 Energy Pilot (Italy)

2.3.1 Pilot Description

The real-world energy pilot implemented by ASM and Emotion in the city of Terni aims to demonstrate the capability of creating smart micro-contracts and micro-payments in an energy environment characterized by a large number of distributed renewable energy sources embedded in the medium voltage (MV) and low voltage (LV) distribution networks. One (1) biomass plant, five (5) hydro power generators and 1,234 solar photovoltaic (PV) units are currently connected to ASM's MV and LV distribution networks, reaching the total installed capacity of around 70 MW. In this regard, it is worth pointing out that, based on the energy mix shown in Figure 9, in 2016 370 GWh were delivered to the consumer, 230 GWh drawn from National Transmission Grid (NTG) and 193 GWh produced by Distributed Energy Resources (DER) plants connected to the ASM's power network; the yearly Reverse Power Flow (RPF) measured in the substations reached 25 GWh (Figure 10) and about 40% of the measurements shows that the locally-produced energy overcomes energy drawn from the NTG.
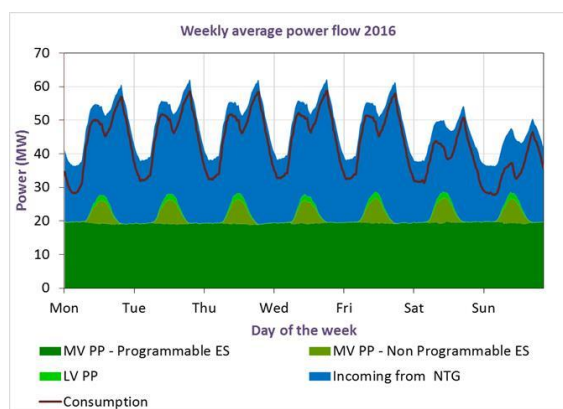
Figure 9: Average weekly profile of consumption and production in the ASM power network
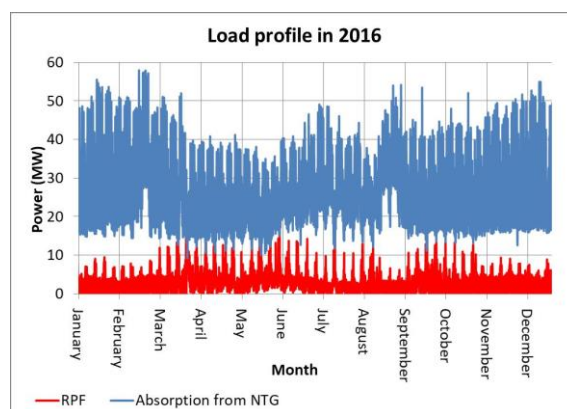
Figure 10: Load profile (2016)

RPF can create instabilities in the system, resulting in overvoltage on the feeder, protection discoordination, increased fault currents and incorrect operation of equipment. Therefore, to avoid the bidirectional power flow, the goal is for local energy consumption to follow the energy production.

Electric mobility, including dynamic and coordinated fleet management, will offer significant benefits in case of coordination of electrical vehicle (EV) charging needs with local green energy availability. In this regard, the Terni pilot will demonstrate in real-world conditions at what extent the SOFIE solutions could help reaching this goal, especially when the production exceeds loads in the ASM's headquarters, by using the EVs of its fleet.

Basically, the SOFIE trial will be run at ASM's headquarters, located in a suburb of the city of Terni. It comprises different production and consumption units such as:

- Two (2) PV arrays (180 kWp and 60 kWp), connected to the LV network
- 72 kW 2nd life Li-ion battery energy storage, an innovative unit, able to be charged and discharged depending on the excess of local energy production
- ASM Terni buildings comprising of i) a 4,050 m² three-floor office building; ii) a 2,790 m² single-floor building consisting of technical offices, a computer center and an operation control center and iii) a 1,350 m² warehouse; usually the base load varies between 50 kW and 90 kW and peak load is between 120 kW and 170 kW, depending on seasonal factors.
- Three (3) electric vehicle (EV) charging stations, two (2) fast, delivering 22kW, and one (1) rapid at 52kW power output.

All the aforementioned Units are connected to the secondary substation "ASM" as shown in Figure 11.
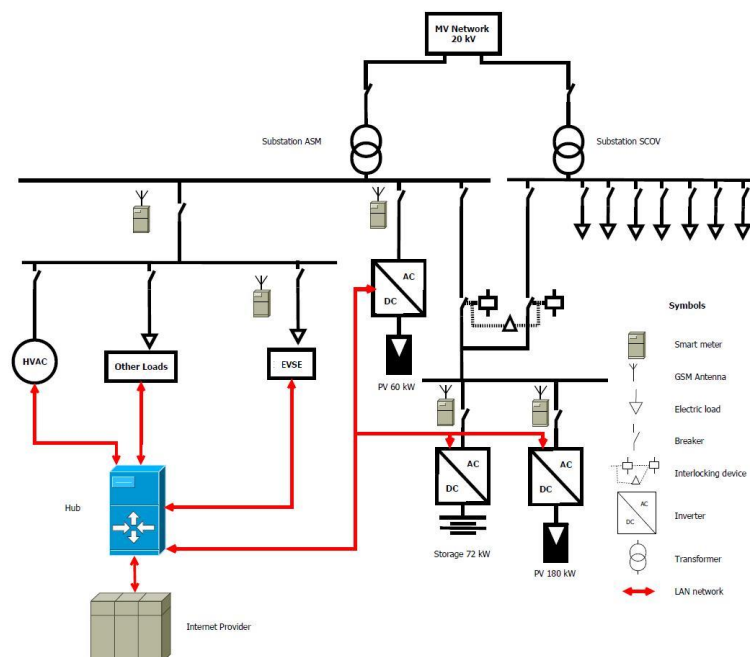
Figure 11: Electricity grid diagram of ASM's headquarters

At ASM's headquarters a fleet of 270 vehicles are used on daily basis for different services (maintenance works, sampling, water or electrical emergencies, etc.). They are managed by the Head of Unit who is responsible for their assignment and for their itineraries.

2.3.2 Technologies

2.3.2.1 Existing entities

Smart meters

The smart meters installed at the Terni pilot site are either 3-phase ZMD meters (Landis+Gyr) or new generation smart meters that are able to get a real time measure and to support real time operations in a Smart Grid. The latter includes a class A power quality analyzer, WALLY A-RTU, manufactured by TeamWare - a 3-phase high-precision analyzer and recorder, power quality, power meter, fault recorder and energy meter).

Electric Vehicle Supply Equipment (EVSE)

Two (2) SPOTLINK - EVO smart charging stations able to manage up to 32A (mono-phase / three-phase); thanks to its single-board computer it is even connected to Spotlink e-mobility platform, developed by Emotion, providing energy data in real time and different services like

charger localization, charger state, micro-payment, energy cost management, EV/EVSE charging management, EV/EVSE monitoring management and dynamic demand response as a service (DDRaaS).

One (1) EFAPOWER EV-QC45 charging station which is able to charge all electric vehicles compliant with CHAdeMO charging system and Combined Charging System (CCS) standards. It can charge the actual available electric vehicles from 0% (Zero) to 80% in less than 30 minutes.

Figure 12: Emotion Spotlink EVO Charging Station

Figure 13: EVSE data communication overview

Plug Numbers	1/2
Plug Type	Type 2
Power MAX	25 kW
Voltage	400 V
Frequency	50-60 Hz
Controllable Power	Yes
Monophase/Triphase	Both
Degree of Protection	IP 54
Interlocking	Yes
Display	Touch screen 7"
RFID	Yes
Communication Protocol	OCPP
Reporting	Yes

Figure 14: Spotlink EVO features

Electric Vehicles (EVs)

Six (6) EVs, each of them equipped with an Emotion OBD device which was developed through a reverse engineering process and designed for real-time reading of the electric vehicle data (Renault ZOE and Nissan LEAF). Data communication from the electric vehicle to the monitoring system of the Emotion partner is achieved through a SIM card that uses the UMTS to send data to the client-server TCP/IP in a Python server at Emotion, which can be accessed remotely to show in real time the state of the vehicle (doors, engine), battery SOC, geolocation and battery charging times.

Figure 15: Emotion customized EV (Renault ZOE)

Figure 16: Prototype of Emotion OBD connected to Renault ZOE

EV data communication
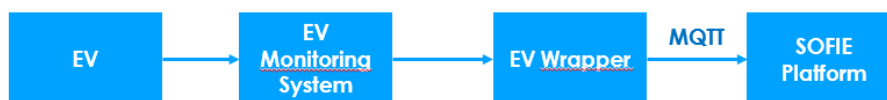
EV data: Battery State-of-Charge, residual Autonomy, minutes to Full Charge, Geolocation, Doors Car State, Engine Car State

Figure 17: EV data communication overview

2.3.2.2 Entities under development

Load and production forecasting software

This software will be used to forecast the need for a flexibility request, based on historical data regarding production, consumption and reverse power flow. This will be used as an input to schedule requests on the flexibility marketplace.

Furthermore, it will be used to forecast the daily EV charging load, in order to know how much the EV fleet recharge could satisfy the Distribution System Operator's (DSO) flexibility need.

Flexibility Marketplace

This platform will receive flexibility requests by the DSO containing information about required energy in kWh, charging station GPS coordinates, time interval information, incentive information and offers from the Fleet Owner. Incentives will be provided in the form of token credits. Smart meters data will be stored for auditability and will ensure that the accepted flexibility requests will be fulfilled. The marketplace will be enabled via a blockchain infrastructure.

2.4 Mobile Gaming Pilot (Finland)

2.4.1 Pilot Description

The goal of this project is to identify and test use case of SOFIE technologies within the mobile game industry. The mobile gaming pilot in the SOFIE project will instigate proof of concept prototypes to explore the potential of distributed ledger technologies to enable new and scalable gaming experience. The pilot will research and prototype gaming experience via the use of DLTs.

There are several potential use cases of DLT within the gaming including:

IAP Payment - Cryptocurrency	Payments network for mobile games based on blockchain using **Cryptocurrency based payment** for in-app purchase transactions between player and developer and between players for items or for work in a game.

IAP Payment - Cryptocash	Payments network for mobile games based on blockchain using **Cryptocash based payment** for in-app purchase transactions between player and developer or between players for items or for work in a game. Based on real-world money and regulated.
App Advertising + User Acquisition	Transparent User Acquisition with consumers in control of what ads they want to see and of their data, with the removal of attribution tracking providers.
Games Features	Players can trade in-game content swapping or buying from other players e.g. weapons, equipment, parts, worlds. This provide means for player ownership and also the potential to enable player content creation.
Location Games using IoT	IoT devices as part of gaming - where a device is used to extend game play into the real-world. Devices could be accessories to the game e.g. weapon or wand, or location based achievements with beacon or digital signage.
Consumer products	Manage scarcity of real world collectables using a blockchain so that the consumer knows that their item is scarce.

The pilot plans to build a core game prototype based on DLT with mini game(s) to leverage the core game and connect to IoT devices via the SOFIE platform.

The pilot is expected to consist of the following (see Figure 18):

Core Game: Enables players to collect and trade in-game content swapping or buying from other players (e.g. characters, weapons, equipment, parts) leveraging DLTs to provide player ownership of the asset, an open market for trading transactions, transparency and consistency of asset attributes and transactions. Attributes of the in-game assets would be published on the blockchain.

Mini Game(s): Enables extension games ("mini-games") to be built on top of the assets published on the blockchain. This will enable innovation potentially by other developers and extension of the original core game providing players with increased game depth. These could leverage attributes of the core game assets via the blockchain.

IoT Mini Game(s): These extension games would enable IoT games to be built around the core game. These games would leverage IoT devices accessible via the SOFIE platform to provide game experiences, for example using Beacons for a scavenger hunt completing 'collection' missions built on the assets from the core game potentially providing a reward in the game or from the locations visited (e.g., a retailer)
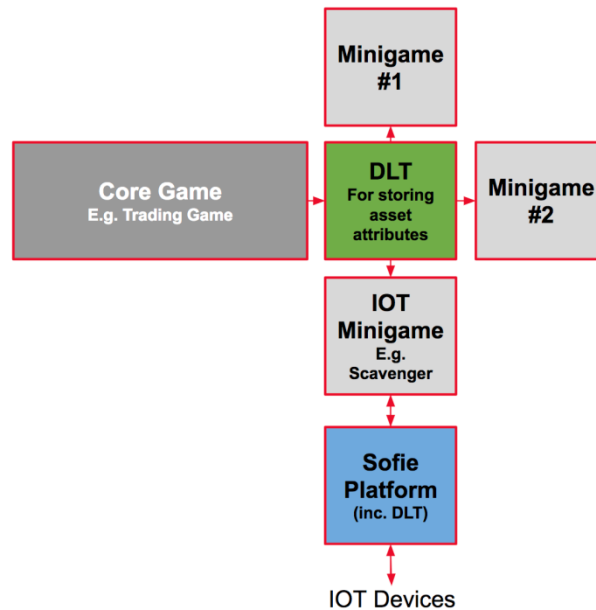
Figure 18: Mobile gaming pilot basic component overview

2.4.2 Technologies

2.4.2.1 Existing entities

Entities that are already available are

- Smartphone game platform (iOS / Android) - mass scale and reach with 2 billion plus smartphone users

- Game development engine (Unity / HTML5), server infrastructure (Rovio's Game Server Template for AWS) and services (analytics, live ops) leveraging Rovio's Beacon platform.

2.4.2.2 Entities under development

The principle technical challenge will be to provide scalable DLTs to support cost-effectively millions of active users per day with thousands of transactions per second. Within the pilot scope we also plan to investigate the use of Ethereum potentially leveraging a public or private implementation, and adopt the Proof of Stake of Ethereum.

3 Scenarios and Use Cases

In SOFIE, a Scenario is a sequence of steps that describe the interaction between the various IoT platforms and one or more actors. Scenarios will help with visualising the platforms' and actors' interactions. In order to describe the Scenarios in a structured and coherent way, we use the template shown in Table 1, where all the main characteristics/aspects of the scenario are aggregated.

SCENARIO	
FIELD	**DESCRIPTION**
History	Author - Version - Action
Scenario ID	Unique ID
Scenario Name	Representative title for the scenario
Key Actors	Actors involved
Assumptions / Dependencies	Preconditions that must hold
Objective(s)	The objective(s) addressed by the scenario
Description	Story description
Services	Services of the SOFIE platform used to address the needs of the actors
Metrics	Metrics measuring the performance and evaluating whether the objectives are achieved

Table 1: Scenario template

This section also describes in more detail SOFIE's pilot use cases. A use case defines a goal-oriented set of interactions between a number of actors and SOFIE components. Each use case is initiated by an actor with a particular goal in mind and is considered successfully completed when that goal is satisfied. Again, in order to present the use cases in a structured and coherent way, we use the template shown in Table 2.

USE CASE	
FIELD	**DESCRIPTION**
ID	Sequential reference number
Name	Short name of the use case
Actors	The subjects and their means that trigger system reactions
Storyline	Describe in a few sentences the storyline of the "main success scenario" addressed by the use case
Trigger events	The main action that starts the use case execution
Pre-conditions	Those actions that must occur before the execution of the use case in order to obtain the described behaviour
Post-conditions	Those conditions that could occur once the use case has been executed and the system continues its operations
Data	Data involved in the use case. Description, type, access (if applicable, public/private), storage location (if applicable)
Related scenario(s)	Scenario(s) addressing the use case
Priority	Must/Should/Could

Table 2: Use case template

It is important to have a consistent terminology, so as to drive the extraction of functional requirements. Therefore, we will use the following form:

[Condition][Subject][Action][Object][Constraint],

where some parts may be optional. For example, the following statement can be translated in a functional requirement:

"When a farmer places a box with fruits in the truck [Condition], the IoT system in place [Subject] issues an "accepted" status [Action] in the distributed ledger used [Object] if the environment temperature is above the predefined threshold [Constraint]"

In addition, prioritization is established utilizing the MoSCow methodology:

1. "Must" - The use case must be supported.
2. "Should" - The use case should be supported as it will create additional benefits.
3. "Could" - Nice-to-have use case but not necessary.

3.1 Food Chain Pilot (Greece)

3.1.1 Pilot Objectives

The main objective of the Food Chain pilot is to provide consumers, producers, traders, transporters and employees with a way to reliably verify information from the whole supply chain. This main objective can be split into three sub-objectives:

1. To enable consumers to verify, in a reliable way, the product's history, i.e. the farmer from whom the product originates, the quality of the soil and the air in the producer's premises, the weather conditions, transportation distance, the storage conditions, etc.
2. To provide a tamper-proof digital product description, i.e. marking the product with pieces of information that will be used in a digital marketplace, e.g. description, pricing, quantity, photos, etc.
3. To provide a way to trace and audit every transaction so that any irregularities can be addressed. This can be initiated if some incident is reported, such as quality issues. Since the system will be completely transparent, all such issues can be traced back to the responsible party.

3.1.2 Actors

The actor roles that will appear in the pilot are:

1. **Producer**, this actor is the responsible person(s) for the TGF segment. He/she is the person who is responsible for growing the products to a consuming-ready state. His/her responsibility and control end when the products are handed over for transportation.
2. **Transporter**, the responsible person(s) for the TRA and TRB segments. This actor is the driver of the transportation vehicle, the person who accompanies the products on their route from one location to another. His/her responsibility and control over the products holds up until the products are handed over to a site's employee.
3. **Warehouse employee**, the responsible person(s) for the SDC segment. This actor has control and responsibility over the product for as long as the products stay stored at the warehouse premises, up to the moment they are handed over to a transporter.
4. **Supermarket employee**, the actor representing the responsible person(s) for the SM segment. This person receives the boxes from the transporter and is responsible for creating the QR labels for each package, as well as storing and placing the packages while at the supermarket premises. For the purposes of the pilot, this actor also has the responsibility to trace back a product quality issue when reported by a supermarket customer. However, in reality we expect that different people/organizations would be responsible for that.

5. **Supermarket customer**, the candidate consumer(s) of the product. This role represents the customers that enter the supermarket interested in buying the stored products. The customers have no responsibility or control over the products.

3.1.3 Scenarios

In this section we describe the various scenarios that will take place during the Food Chain Supply pilot. In different places we mention "web application" which will be either a Graphical User Interface (GUI) provided to all the IoT platforms as a part of the Business Platform (BP) or an IoT platform specific GUI displaying information retrieved by the BP. In the following scenarios most of the participants are asked to swipe their RFID tags whenever they receive an item. This action replaces the previous way of handing over responsibility of an item by signing on a paper. We are fully aware that doing so for every item is not a scalable solution; however we opted for this solution in order to be more in control of the actions of the participants for the pilot phase. For the commercial exploitation of the food supply chain, a more automated way for responsibility hand-over should be designed, probably by introducing a more automated (and more capital intensive) RFID tagging system.

3.1.3.1 Food quality history information scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	Yannis Oikonomidis, Antonis Gonos, - v0.1 - First scenario description
Scenario ID	FoodChain_Scenario_1
Scenario Name	Food Quality monitoring scenario
Key Actors	Producer, transporter A, warehouse employee, transporter B, supermarket employee, supermarket customer
Assumptions / Dependencies	SOFIE platform is installed and running. IoT platforms are installed and running including - SynField field nodes and Cloud platform - Transportation platform with smart boxes equipped with RFID readers, vehicles with temperature, GPS, and other sensors - Aberon platform All key actors, except for the supermarket customer, have RFID tags.
Objective(s)	Monitor and ensure food quality and change of responsibility along the whole supply chain from the field to the fork
Description	The producer owns a field where she grows table grapes. In this field there is a SynField deployment which helps her with monitoring and controlling her crop's quality. SynField field nodes collect and transmit temperature data to SynField cloud component. The sensor data provided by the SynField nodes triggers logic embedded in the SynField cloud platform that actuates a deployed smart irrigation system on the field **(FCP_UC5)**. The producer has an agreement to sell her goods to a specific supermarket brand. The agreement dictates that when the producer collects the grapes from the field, she has to swipe her RFID tag every time she fills a "smart" box (boxes equipped with RFID readers) with grapes. When her goods are ready to be transported, she arranges for a transportation vehicle to arrive at her field where she will, with the assistance of transporter A, load the boxes into the vehicle. At this point, transporter A, whose transportation company has also an agreement with the supermarket, has to swipe his tag on every box that he loads on his vehicle. The transportation vehicle is equipped with temperature and GPS sensors which collect and transmit data to the Transportation IoT platform while the vehicle is on the move. Transporter A drives the vehicle to the Storage & Distribution Centre where the Aberon platform is deployed monitoring arriving packages. The boxes are received by the warehouse employee who also has to swipe his RFID tag at every smart box he unloads from the vehicle. The warehouse

	employee, according to the ripening level of the contents of each package, places the packages at the correct spot within the storage facility. While the boxes stay at the storage center, information regarding temperature as well as location and storage duration is collected. Boxes are collected from the storage center by a transportation vehicle which is driven by transporter B. Transporter B swipes her tag at every box she loads into the vehicle. The boxes arrive at the supermarket where supermarket employees unload them from the vehicle and swipe their RFID tags at the boxes. They connect to a web application and through a user friendly GUI they create QR labels that contain all the information (from both box and field) collected from the field to the supermarket (**FCP_UC1**). The grape packages are then marked with those QR labels and they are placed by the supermarket employees at the appropriate spot inside the customer area. Box information during the transportation from the field to fork are continuously and automatically being checked, so that in case of a wrong state (e.g. bad temperature value) notifications are sent to the appropriate Cloud platform. A supermarket customer scans the QR labels with his smartphone while passing by those spots to see and evaluate the temperature history, the storage duration, the origin producer location, etc. of the products inside the box, having in that way a reliable means of deciding upon purchasing and consuming the product (**FCP_UC2**).
Services	SOFIE communication services between various blockchain enhanced IoT platforms
Metrics	Check whether the products' complete information can be securely stored, retrieved, and presented

3.1.3.2 Food quality monitoring scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	Yannis Oikonomidis, Antonis Gonos - v0.1 - First alert scenario description
Scenario ID	FoodChain_Scenario_2
Scenario Name	Food Quality alert scenario
Key Actors	Producer, transporter A, warehouse employee, transporter B, supermarket employee, supermarket customer
Assumptions / Dependencies	SOFIE platform is installed and running. IoT platforms are installed and running including • SynField field nodes and Cloud platform • Transportation platform with smart boxes equipped with RFID readers, vehicles with temperature, GPS, and other sensors • Aberon platform All key actors, except for the supermarket customer, have RFID tags.
Objective(s)	Create alert in case of food quality irregularity and trace back to the source of this issue along the whole supply chain from the field to the fork
Description	The producer owns a field where she grows table grapes. In this field there is a SynField deployment which helps her with monitoring and controlling her crop's quality. SynField field nodes collect and transmit temperature data to the SynField cloud component. The producer has an agreement to sell her goods to a specific supermarket brand. The agreement dictates that when the producer collects the grapes from the field, she has to swipe her RFID tag every time she fills a "smart" box (boxes equipped with RFID readers) with grapes. When her goods are ready to be transported, she arranges for a transportation vehicle to arrive at her field where she will, with the assistance of transporter A, load the boxes into the vehicle. At this point, transporter A, whose transportation company has also an agreement with the supermarket, has to swipe his tag on every box that he loads on his vehicle. The transportation vehicle is equipped with

	temperature and GPS sensors which collect and transmit data to the Transportation IoT platform while the vehicle is on the move. Transporter A drives the vehicle to the Storage & Distribution Centre where Aberon platform is deployed monitoring arriving packages.
	The boxes are received by the warehouse employee who also has to swipe his RFID tag at every smart box he unloads from the vehicle. While the boxes stay at the storage center, information regarding temperature as well as location and storage duration is collected.
	Boxes are collected from the storage center by a transportation vehicle which is driven by transporter B. Transporter B swipes her tag at every box she loads into the vehicle. The boxes arrive at the supermarket where supermarket employees unload them from the vehicle and swipe their RFID tags at the boxes. They connect to a web application and through a user friendly GUI they create QR labels that contain all the information (from both box and field) collected from the field to the supermarket. The grape packages are then marked with those QR labels and they are placed by the supermarket employees at the appropriate spot inside the customer area. Box information during the transportation from the field to fork are continuously and automatically being checked, so that in case of a wrong state (e.g. bad temperature value) notifications are sent to the appropriate Cloud platform. While being at the distribution storage center, the temperature rose above the desired level for more than a predefined time period. Consequently, an alert was generated and sent to the monitoring application **(FCP_UC3)**. The warehouse employee did not notice the alert, as the temperature dropped again to the desired levels; hence the package continued its path.
	A supermarket customer scanned the QR label of the package, noticed the temperature issue and reported it to a supermarket employee. The various parties involved in the food supply chain, as well as legal authorities, trace back the issue and verify the source and the responsible entity **(FCP_UC4)**.
Services	SOFIE communication services between various blockchain enhanced IoT platforms
Metrics	Check whether, in a case of a product quality irregularity, the issue is successfully reported and the source of the problem can be traced back.

3.1.4 Use Cases

In this section we describe the various use cases that can be extracted from the scenarios described in 3.1.3. In different places we mention "web application" which will be either a Graphical User Interface (GUI) provided to all the IoT platforms as a part of the BP or a IoT platform specific GUI displaying information retrieved by the BP.

3.1.4.1 Creation of a QR label containing the product information from field-to-fork

USE CASE	
FIELD	**DESCRIPTION**
ID	FCP_UC1
Name	QR label creation
Actors	Supermarket employee
Storyline	When the supermarket employee needs to remove the table grape packages from the smart box and place them at the customer area, he/she logins to a web application that creates a QR label with all the relevant information that was collected from the whole route from the field to the supermarket
Trigger events	Supermarket employee logins to the web application
Pre-conditions	Table grape data (temperature, presence, GPS, etc.) are collected and made available to the IoT platforms
Post-conditions	QR label is generated and made available for downloading and printing
Data	User data (username, password, employee id, etc.), stored at the web application

	database that is used by the supermarket employees. This data will be used to provide the supermarket employee access to the web application. Product data (sensor data, other product information), stored at the various IoT platforms along the supply chain path, that will be retrieved to create the QR label. All data will be private.
Related scenario(s)	FoodChain_Scenario_1
Priority	Must

3.1.4.2 Check of product description using the QR label

USE CASE	
FIELD	**DESCRIPTION**
ID	FCP_UC2
Name	Product description using QR label
Actors	Supermarket customer
Storyline	When a supermarket customer wants to get information about a table grape package, he/she scans the QR label attached to the package and all the available information is displayed on his/her smartphone screen.
Trigger events	Supermarket customer scans a package's QR label
Pre-conditions	Table grape data (temperature, presence, GPS, etc.) are collected and available in the IoT platforms. Supermarket customer has installed the application in his smartphone. A QR label has been created and attached to the package.
Post-conditions	Table grape package history information is displayed on the supermarket customer's screen
Data	Product data (sensor data, other product information), stored at the various IoT platforms along the supply chain path, that will be used to create the QR label. Data will be publicly available to the supermarket customers through the QR labels.
Related scenario(s)	FoodChain_Scenario_1, FoodChain_Scenario_2
Priority	Must

3.1.4.3 Alert user in case of a product irregularity

USE CASE	
FIELD	**DESCRIPTION**
ID	FCP_UC3
Name	Alert mechanism
Actors	Warehouse employee
Storyline	When the product's temperature rises above an acceptable level for more than a predefined time period, an alert is generated and sent to the web application
Trigger events	A product's temperature rises above an acceptable level for more than a predefined time period
Pre-conditions	Table grape data (temperature, presence, GPS, etc.) are collected and available in the IoT platforms
Post-conditions	Alert and information about a package are sent and displayed on the warehouse employee application screen
Data	Product data (sensor data, other product information), stored at the various IoT platforms along the supply chain path, that will be sent along with the alert message. All data will be private.
Related scenario(s)	FoodChain_Scenario_2
Priority	Should

3.1.4.4 Trace back in case of a product irregularity

USE CASE	
FIELD	**DESCRIPTION**
ID	FCP_UC4
Name	Product information auditability
Actors	Supermarket customer
Storyline	When a supermarket customer scans the QR label on a package and notices an irregularity, he/she reports this to the supermarket employee who then accesses the web application in order to trace back the issue
Trigger events	A supermarket customer notices a product's irregularity
Pre-conditions	Table grape data (temperature, presence, GPS, etc.) are collected and available in the IoT platforms. An alert is generated at some point during a product's route.
Post-conditions	Product's alert history is displayed
Data	User data (username, password, employee id, etc.), stored at the web application database that is used by the supermarket employees. This data will be used to provide the supermarket employee access to the web application. Product data (sensor data, other product information), stored at the various IoT platforms along the supply chain path, that will be used to create the QR label. Data will be publicly available to the supermarket customers through the QR labels.
Related scenario(s)	FoodChain_Scenario_2
Priority	Must

3.1.4.5 Smart Irrigation actuation

USE CASE	
FIELD	**DESCRIPTION**
ID	FCP_UC5
Name	Smart irrigation actuation
Actors	-
Storyline	When logic rules in the SynField platform get triggered by sensor data, smart irrigation is actuated
Trigger events	A predefined combination of field sensor data values
Pre-conditions	Table grape data (temperature, soil humidity, presence, GPS, etc.) are collected and available in the SynField IoT platform
Post-conditions	Smart irrigation system is actuated
Data	Product data (sensor data, other product information), stored at the SynField IoT platform
Related scenario(s)	FoodChain_Scenario_1
Priority	Must

3.1.4.6 Ripening level

USE CASE	
FIELD	**DESCRIPTION**
ID	FCP_UC6
Name	Check ripening level
Actors	Warehouse employee
Storyline	When the warehouse employee receives the boxes from the transportation employee, he checks the ripening level of the products within the boxes so as to place them at the right (from a temperature point of view) spot in the warehouse. He

	checks the ripening level through a web application.
Trigger events	The warehouse employee receives the boxes from the transportation employee
Pre-conditions	Table grape data (temperature, soil humidity, ripening level, presence, GPS, etc.) are collected and available in the IoT platforms.
Post-conditions	Ripening level information displayed to the warehouse employee
Data	User data (username, password, employee id, etc.), stored at the web application database that is used by the warehouse employees. This data will be used to provide the warehouse employee access to the web application. Product data (sensor data, other product information), stored at the various IoT platforms along the food supply chain.
Related scenario(s)	FoodChain_Scenario_1
Priority	Should

3.1.5 User Engagement and Feedback

Since there are end users involved in this pilot, i.e. the supermarket customers, we need to identify and deploy mechanisms to engage them into using the information provided by the system as well as getting their feedback from their experience using it. In SOFIE, we will boost user engagement through the following means:

- Offer rewards for users that scan the QR label or for those who find out that something is wrong with a product. We could do this by embedding a unique code in the QR label information so that a customer can use it to receive a discount at the cashier on the product's original price.
- Encourage active participation of the customers by promoting the quality information included in the QR label as well as giving emphasis on the discount available upon using it.
- Support product ratings by showing additional information in the QR label regarding the times it has been reported by customers a problematic product. This will not pinpoint to a specific part of the food supply chain, leading all the involved parties to be responsible and accountable for any issue as a whole in the eyes of their customers.

Regarding feedback collection we plan on designing anonymous questionnaires that the users will fill at the products' location in the supermarket. The plan for the questionnaires is to formulate a short number of questions addressed to the supermarket customer, aiming to identify the following:

- The usefulness of the product information included and whether it helps him/her towards making a decision on purchasing the product.
- The user-"friendliness" of the displayed information, how easy it was to understand the information presented and how well it was presented.
- What other information might be useful for the customer.

The questionnaires will be placed next to the products in the supermarket in a spot that will allow the customers to find them easily. The questionnaires will be collected in a box at the same location.

3.2 Energy Pilot (Estonia)

3.2.1 Pilot Objectives

The main objective of the Energy pilot is to enable trust between parties who exchange energy meter readings. From the smart meter platform owner's side (TSO or DSO) there is a need for guarantee; who is responsible after the data exchange and how to agree and prove the responsibility. From the brokers, aggregators, energy traders and other energy readings users'

side it is important to be reliably verify information from the whole data provenance chain. There is also the smart meter data owner part, which requires transparent overview on who the data access rights are given to and who is responsible for private data handling. Main objective can be divided into three separate goals:

1. To provide means to verify the integrity of smart meter data and processes. This is needed for all participants being owners of smart meter data; either platform operator or the flexible energy service provider or broker.
2. To provide a tamper-proof evidence of smart meter data in case of disputes.

To provide a way to enable and trace the agreements between different parties taking into consideration the challenge coming from the multiple different systems involved in the data exchange, different technologies being used and geographical/cross border distribution of participants.

3.2.2 Actors

The actor roles that will appear in the pilot are:

1. **Smart meter system operator (SMSYS)** – Usually TSO *(Transmission System Operator)* but can also be **DSO**, *Distribution System Operator*. The entity responsible for national or regional smart meter network. Has the obligation to run the network grid and manage the smart meter infrastructure. Also they have the role of providing access (when granted by data owner) to the smart meter data to all interested parties.
2. **Energy service provider (SERVICE)** - DSO, energy company etc. The entity responsible for providing the energy service to the end-user. Main communicator between customer and grid operator. Can own low, medium voltage grid and smart meter infrastructure but it is possible to have no grid/infrastructure responsibilities. In current energy pilot the microgrid (a small electricity network attached to a centralized national grid but is able to function independently) manager and user have the same need towards other participants and can be handled, to simplify the scenarios, to have the same role. Main user of the smart meter data to provide cross country flexibility services in energy sector.

Smart meter owner (OWNER), Private entity or company who is legally bound to smart metering point and is interested to consume/produce energy. Has the right to give access of smart meter data.

3.2.3 Scenarios

3.2.3.1 SmartMeter access scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	Priit Anton– V01 – Scenario description
Scenario ID	Energy_EST_Pilot_Scenario_1
Scenario Name	Access to SmartMeter data
Key Actors	SMSYS 1, SMSYS 2, OWNER
Assumptions / Dependencies	• Both SMSYS operate their own grid and have customer relationship with the OWNER to get consent for giving data access to third parties. • The smart meter readings are received by SMSYS platform side in 15 min period.
Objectives	To give access of a specific smart meters from one platform to another and registering the participants and agreements. Being able to prove in case of dispute who gave access and who received the data under what agreement and time.
Description	The SMSYS 1, gets a request from OWNER that his smart meter data should be accessed by SMSYS 2. After checking the digital identity match with Smart meter

	owner SMSYS sends a proposal to SMSYS 2 for data access and terms of accessing the data. SMSYS 2 confirms the request, agrees on the terms and data access to the SMSYS 2 is committed.
Services	Elering Estfeed TenneT (or similar operator) smart meter platform KSI®Blockchain CORDA R3 distributed ledger Customer request management system
Metrics	Trusted data exchange (agreement on both sides, provable by 3rd party without customer data exposure, low overhead to existing systems integration)

3.2.3.2 Data import scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	Priit Anton – V02 – Scenario description
Scenario ID	Energy_EST_Pilot_Scenario_2
Scenario Name	Data import to National Smart meter platform
Key Actors	SMSYS 1, OWNER, SERVICE
Assumptions / Dependencies	• SERVICE and OWNER have set up a microgrid (network of smart meters) for energy consumption and have a contract. • SMSYS does not have direct access and means to validate or trust the SERVICE operated microgrid. • Microgrid data is not connected to the national smart meter platform.
Objectives	SMSYS 1 needs to trust third party data and be able to verify smart meter readings and metadata. Need to agree on the responsibility of the data access and reception.
Description	OWNER requests service from the SMSYS 1 and gives consent to the SERVICE and SMSYS 1. SERVICE provides SMSYS the access to the smart meter together with the provable data provenance chain and smart meter opt-in process. SMSYS 1 receives the input data, verifies and accepts the terms and opens the data transfer to his smart meter platform. After receiving the OWNER smart meter data feed SMSYS 1 can provide requested service to the OWNER.
Services	DSO forecast system; fleet manager; management system requests for flexibility; flexibility marketplace
Metrics	Seamless microgrid data import to National Smart meter platform together with and agreed responsibilities.

3.2.4 Use Cases

3.2.4.1 Dispute solution

USE CASE	
FIELD	**DESCRIPTION**
ID	EST_Energy_UC1
Name	Dispute solution
Actors	SMSYS1, SERVICE
Storyline	After receiving smart meter data from National Smart meter platform, SERVICE has dispute about the consumption data provided by the SMSYS 1. When the demand for explanation has been made by SERVICE SMSYS 1 asks for the smart meter data (metadata include) for analysis. The comparison of provided smart meter readings and time to the agreed data transfer out of SMSYS 1 system prove that incorrect readings (and the cause of the error) are made outside the SMSYS 1

	operated system.
Trigger events	The request from SERVICE side who has potential financial loss caused by false readings.
Pre-conditions	The SMSYS 1 system is connected with smart meter data exchange platform.
Post-conditions	A data exchange, responsibilities and integrity of the exchanged asset are agreed by all parties involved.
Data	Smart meters data used to offer flexible energy service. Private, local. On a blockchain and in distributed ledger.
Related scenario(s)	Energy_EST_Pilot_Scenario_1;
Priority	Must

3.2.4.2 Flexibility service request

USE CASE	
FIELD	**DESCRIPTION**
ID	EST_Energy_UC2
Name	Flexibility service Request
Actors	OWNER, SERVICE, SMSYS 1
Storyline	OWNER request green energy package from SMSYS 1. OWNERs smart meter is connected to microgrid and has contract and infrastructure provided by SERVICE. SERVICE enables access of the smart meter to SMSYS 1 platform with agreed responsibilities and terms. SMSYS 1 starts providing the service through third party microgrid. Based on data SERVICE provides one service invoice will be provided to OWNER who receives a more flexible and cheaper service.
Trigger events	Request from the OWNER to change the energy service provider.
Pre-conditions	SMSYS 1 and SERVICE have agreed on the process of opt-in smart meters and securing the data provenance chain.
Post-conditions	Open market for flexible energy service providers. Possible specialization on specific service sector (solar power production, large household, farmhouse energy service etc.)
Data	Smart meters data used for invoice. On a blockchain and in distributed ledger.
Related scenario(s)	Energy_EST_Pilot_Scenario_2
Priority	Must

3.2.5 User Engagement and Feedback

The involved users in this pilot will be the two Transmission System Operators (TSOs), one service provider operating a microgrid and multiple end-users who own the smart meters.
To ensure the user engagement there is LoI agreed between the SOFIE consortium and Elering. There are also benefits to other parties that will be promoted by GuardTime like new business opportunities, less investment into integration of existing systems and more nature friendly / lower carbon emission energy services for end-users.

Feedback collection we will be handled by making interviews with all parties and conducting one questionnaire for TSOs and Service provider to get feedback on the value proposition and potential attractive use-cases for the parties. Also, feedback to the potential risks and adaptation to the new offered technology will be collected.

3.3 Energy Pilot (Italy)

3.3.1 Pilot Objectives

The pilot site of Terni will test the blockchain technology applied to a peer to peer mechanism between the DSO, owner of the electricity distribution network (low voltage/medium voltage network), and the Aggregator (EV Fleet Manager). We are considering an end-to-end scenario from electricity production, to distribution, storage and consumption. During the scenario electricity produced by renewable sources (PVs) are fed into the low voltage (LV) electricity network. Most of this electricity will be normally consumed by energy customers (i.e. houses, offices, etc.). However, the surplus of generated power would generate reverse power flows through the LV distribution network substation. The electricity distribution network is designed to handle only unidirectional electricity flows, thus reverse flows may generate significant issues. To avoid this abnormal operation, electrical vehicles (EV) will be offered significant promotional benefits to match their EV charging needs with the network time and space balancing requirements.

3.3.2 Actors

The actor roles that will appear in the pilot are:

1. **DSO** (Distribution System Operator). The entity responsible for: the distribution network planning and development; the safe and secure operation and management of the distribution network; for data management associated with the use of the distribution network; the request for flexibility services.
2. **Fleet manager** (Aggregator). Actor that operates and controls the EV fleet in the pilot.
3. **EV Users** (Electric Vehicle User). They are users who will use EVs in the pilot.

3.3.3 Scenarios

3.3.3.1 Pull scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	Alessio Cavadenti – V01 – Scenario description
Scenario ID	Energy_Pilot_Scenario_1
Scenario Name	Pull Offers
Key Actors	DSO, Fleet manager, EV User
Assumptions / Dependencies	• DSO foresees and provides flexibility to the grid, using charging stations matching time and space balancing requirements; • the management system is able to retrieve information in real time
Objectives	To stabilize the power grid due to the geo/local time flexibility provided by the charging stations and to maximize local energy consumption
Description	The DSO, after checking the load and production forecasting of the whole distribution grid, needs to shave peaks of energy produced locally the day after so that instability of the system, overvoltage on the feeder, protection discoordination, increased fault currents, and incorrect operation of equipment could be avoided. Using the marketplace, it will put a flexibility request in the day-ahead market, asking for an amount of energy (kWh), a timeslot, a location (GPS coordinates), granting an incentive (tokens). Meanwhile, the fleet owner performs day ahead itinerary and charging plans for its EV fleet, checking the EV charging price in the platform and matching fleet needs with offers in the platform to achieve the maximum bonus available in terms of incentives, accepting the corresponding offers in the marketplace.
Services	DSO forecast system; fleet manager;

	management system requests for flexibility; flexibility marketplace
Metrics	Reduction of the reverse flow

3.3.3.2 Push scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	Giuseppe Raveduto - 0.1 - Scenario description
Scenario ID	Energy_Pilot_Scenario_2
Scenario Name	Push Offers
Key Actors	DSO, Fleet Manager, EV User
Assumptions / Dependencies	- the management system is able to retrieve information in real time from the EV - DSO foresees the need for a flexibility request to balance the grid - the fleet manager (FM) is able to profile EV users - EV user is able to pay using virtual tokens, and can receive tokens as incentive
Objective(s)	To stabilize the power grid due to the geo/local time flexibility provided by the charging stations and to maximize local energy consumption
Description	The DSO, after checking the load and production forecasting of the whole distribution grid, needs to shave peaks of energy produced locally in the same day, to avoid system instability. Using the marketplace, it will put a flexibility request, asking for an amount of energy (kWh), a timeslot, a location (GPS coordinates), granting an incentive (tokens). The system will try to identify potential candidates to fulfil the request, based on: - user type - current location - residual autonomy - EV current status Selected users will receive a notification, offering a token incentive if they agree to charge the vehicle using a predetermined charging station in a specific time interval.
Services	DSO forecasting service; Fleet management system; EV user app; EV users profiling system; Flexibility marketplace;
Metrics	Reduction of the reverse flow

3.3.4 Use Cases

3.3.4.1 Flexibility request

USE CASE	
FIELD	**DESCRIPTION**
ID	EP_UC1
Name	Flexibility Request
Actors	DSO
Storyline	When the DSO foresees a potential reverse flow, the IoT system creates a new request in the flexibility marketplace

Trigger events	The forecast system indicates a potential reverse power flow to be mitigated
Pre-conditions	The DSO system is connected with the flexibility marketplace
Post-conditions	A flexibility request is created in the marketplace, ready to be matched
Data	Smart meters data used for the forecast. Private, local. Settled offers. Public(?), on a blockchain.
Related scenario(s)	Energy_Pilot_Scenario_1; Energy_Pilot_Scenario_2
Priority	Must

3.3.4.2 Pull offer request

USE CASE	
FIELD	**DESCRIPTION**
ID	EP_UC2
Name	EV Offers request (Pull)
Actors	Fleet Manager
Storyline	When the fleet owner performs day ahead itinerary and charging plans for its EV fleet, he will accept the flexibility requests available in the flexibility marketplace if the requests are compatible with his needs
Trigger events	Fleet Manager is planning day-ahead EV charging and itinerary
Pre-conditions	EVs need to be charged. Load can be postponed to match flexibility requests.
Post-conditions	The EV is charged Fleet Manager receive the agreed incentives for fulfilling the requests.
Data	EVs charging state. Private, local. Planned routes. Private, local. Settled offers. Public(?), on a blockchain.
Related scenario(s)	Energy_Pilot_Scenario_1
Priority	Must

3.3.4.3 Push offer request

USE CASE	
FIELD	**DESCRIPTION**
ID	EP_UC3
Name	EV Offers request (Push)
Actors	Fleet Manager; EV User
Storyline	When the user receives a discounted price notification, he will accept the flexibility request available in the flexibility marketplace if the request is compatible with his transport needs.
Trigger events	EV User is alerted by a discounted price notification
Pre-conditions	EV need to be charged. Load can be postponed to match flexibility requests.
Post-conditions	The EV is charged The user receives the agreed incentive for fulfilling the request.
Data	EVs charging state. Private, local. User Profile. Private, local. Settled offers. Public(?), on a blockchain.
Related scenario(s)	Energy_Pilot_Scenario_2
Priority	Must

3.3.4.4 Fleet monitoring

USE CASE	
FIELD	**DESCRIPTION**
ID	EP_UC4
Name	EV and EVSE fleet monitoring
Actors	Fleet Manager
Storyline	To perform both Energy Pilot Scenarios, Fleet Manager have to constantly monitoring EV and EVSE fleet
Trigger events	Monitoring can be executed periodically or on demand triggered by the EV/EVSE fleet manager
Pre-conditions	Deployed EVs and EVSEs; The EVSE and EV data will be handled considering the EU and national laws regarding privacy and data protection; Data should be reliable and consistent; EVSE unique identifier; EV unique identifier; Security in communications; Connectivity and Interoperability between EV and EVSE systems.
Post-conditions	Correct communication between actors. Overview on the status of the EVSE portfolio and the EV fleet.
Data	EV status information: Battery State-of-Charge (%), residual Autonomy (Km), minutes to Full Charge (m), Geographic location, Doors Car State, Engine Car State (On/Off); EVSE status information: out of service, number of sockets in use, current vehicle ID attached.
Related scenario(s)	Energy_Pilot_Scenario_1, Energy_Pilot_Scenario_2
Priority	Should

3.3.4.5 Load forecasting

USE CASE	
FIELD	**DESCRIPTION**
ID	EP_UC5
Name	EV load forecasting
Actors	Fleet Manager
Storyline	To perform the Pull Offers Scenario, the Fleet Manager has to constantly calculate EV load forecasting to estimate the amount of energy that electric vehicles can consume to meet the DSO's flexibility demand.
Trigger events	The EV load forecasting will be calculated periodically (every day).
Pre-conditions	The data collection from EVSE should be performed to have historical data and to know the status of the EVSEs
Post-conditions	The EV load forecasting is updated in the Fleet Manager data repository to be used
Data	Energy parameters, measured by a smart meter on each EVSE socket: power, voltage, current and energy.
Related scenario(s)	Energy_Pilot_Scenario_1
Priority	Should

3.3.4.6 District forecasting

USE CASE	
FIELD	**DESCRIPTION**
ID	EP_UC6
Name	District forecasting
Actors	DSO
Storyline	To perform Energy Scenarios, the DSO has to constantly calculate building consumption forecasting, PV production forecasting and manage batteries to estimate the amount of energy demand at ASM substation
Trigger events	Forecasting will be calculated periodically (every day). Need to reduce undesired reverse power flows
Pre-conditions	The data collection should be performed in real time (or very close to real time) and should be secure and reliable
Post-conditions	The building load forecasting is updated in the DSO data repository to be used The RES production will be monitored and forecasted in order to reduce reverse power flow
Data	Energy parameters, measured by a smart meter: power, voltage, current and energy. Weather parameters: solar irradiance (in W/m2), outdoor temperature, presence of rain, presence of snow.
Related scenario(s)	Energy_Pilot_Scenario_1, Energy_Pilot_Scenario_2
Priority	Must

3.3.5 User Engagement and Feedback

The involved users in this pilot will be the DSO operator, the fleet manager and the EV user.
User engagement will be determined by the benefits provided by the platform:

- DSO operator: will benefit from the increase of local energy consumption within the micro-grid, reducing the reverse power flow.
- Fleet manager: will reduce the total cost of fleet recharging, due to the provided incentives.
- EV User: probably can be rewarded with a fraction of the incentive tokens collected by the fleet manager, or can benefit directly from incentives in the "push" scenario.

Regarding feedback collection we will offer questionnaires that the EV users will fill aiming to identify the following:

- The compatibility of its charging plans with the provided incentives.
- The user-"friendliness" of the displayed information, how easy it was to understand the information presented and how well it was presented.

3.4 Mobile Gaming Pilot (Finland)

3.4.1 Pilot Objectives

The focus of this pilot will be on leveraging DLT to provide new gaming features for players with alongside seeking validation of potential location and IoT use cases. It will seek to overcome known technical issues; in principle the ability of DLTs to scale so as to cost-effectively support millions of active users per day with thousands of transactions per second. The pilot will also seek to investigate business issues, namely:

- **Game discovery**: how to reach mass market - given mobile app ecosystem (Apple / Google) access restriction on cryptocurrencies.

- **IoT device scale**: devices fit for gaming use cases that can easily provide global scale so players can engage in their locality.

3.4.2 Actors

The actor roles that will appear in the pilot are:

1. **Player:** this actor is the consumer playing the game. A critical requirement for the player is that the game should meet the motivation needs - achievement, social and immersion. The player should be able to own and trade content within the game and interact with IoT devices.
2. **Game Developer:** this actor is responsible for development and operation of the game. Expectations for this role include the continuous development ('live operation') of the game - 'game as a service'. Core game and mini-games could be developed by different game developers.

3. **Location owner:** this actor provides the IoT device used for interaction with the game. This for example could be a beacon that the player interacts with at a location via the game.

3.4.3 Scenarios

3.4.3.1 Collection and Trading scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	David Mason - v1.0 - First scenario description
Scenario ID	Game Pilot Scenario 1
Scenario Name	Collect + Trade
Key Actors	Game Developer Player
Assumptions / Dependencies	DLT used to publish core game content 'DNA'. DLT enables transfer of ownership of game content.
Objective(s)	Player can collect 'own' and trade 'transfer ownership' of in game content.
Description	Enable players to collect and trade in-game content swapping or buying with other players (e.g. characters, weapons, equipment, parts) leveraging DLTs to provide player ownership of the asset, an open market for trading transactions, transparency and consistency of asset attributes and transactions. Attributes 'DNA' of the in-game assets would be published on the blockchain.
Services	SOFIE supported DLT used to store game content
Metrics	1,000's of transaction per second to support millions of daily active users

3.4.3.2 Mini-game scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	David Mason - v1.0 - First scenario description
Scenario ID	Game Pilot Scenario 2
Scenario Name	Mini-game
Key Actors	Game Developer Player
Assumptions / Dependencies	DLT used to publish game content 'DNA' so that mini-games can leverage core game content
Objective(s)	Game developer can build mini-games on top of core game content
Description	To enable extension games "mini-games" to be built on top of the assets

	published on top of the blockchain. This will enable innovation potentially by other developers and extension of the original core game providing players with increased game depth. Leverage attributes 'DNA' of the core game assets via the blockchain.
Services	SOFIE supported DLT used to store game content
Metrics	1,000's of transaction per second to support millions of daily active users

3.4.3.3 IoT mini-game scenario

SCENARIO	
FIELD	**DESCRIPTION**
History	David Mason - v1.0 - First scenario description
Scenario ID	Game Pilot Scenario 3
Scenario Name	IoT Mini-game
Key Actors	Location Owner Game Developer Player
Assumptions / Dependencies	DLT used to publish game content 'DNA' so that mini-games can leverage core game content Location interaction via IoT device
Objective(s)	Game developer can build IoT mini-games on top of core game content with location owner providing IoT device for location interaction.
Description	Extension games would enable IoT games to be built around the core game. Game(s) to leverage IoT devices via the SOFIE platform to provide game experiences, for example using Beacons for a scavenger hunt completing 'collection' missions built on the assets from the core game potentially providing a reward in the game of from the locations - Location Owner (e.g. retailer)
Services	SOFIE federated IoT devices
Metrics	1,000's of transaction per second to support millions of daily active users with real-time interaction with IoT devices

3.4.4 Use Cases

3.4.4.1 Game content DNA

USE CASE	
FIELD	**DESCRIPTION**
ID	MG_1
Name	Game Content DNA
Actors	Game Developer Player
Storyline	DLT used to publish core game content 'DNA'. DLT enables transfer of ownership of game content and mini-games.
Trigger events	New content created and published by game developer or by player.
Pre-conditions	Timed publication of new content with transparent content DNA
Post-conditions	Content can be collected, owned, traded and used within mini-games
Data	Attributes of content DNA defined by game
Related scenario(s)	Game Pilot Scenario 1, Game Pilot Scenario 2, Game Pilot Scenario 3
Priority	Must

3.4.4.2 Game-IoT interaction

USE CASE	
FIELD	**DESCRIPTION**
ID	MG_2
Name	Game IoT interaction
Actors	Location Owner Game Developer Player
Storyline	Player interacts with IoT device in location via the mini-game
Trigger events	Interaction of player with location IoT device
Pre-conditions	IoT device location and interactions are known by the game
Post-conditions	Real-time interaction with IoT device so game play is real-time
Data	Interaction data to be defined by mini-game design e.g. Scavenger game and IoT devices used for location interaction e.g. Beacon
Related scenario(s)	Game Pilot Scenario 3
Priority	Must

3.4.5 User Engagement and Feedback

User engagement takes into account both acquisition of users and then retention of the lifetime of the game. The factors that will drive this will be dependent on multiple factors including the accessibility of the game - can I readily download and play, is the game fun - do I want to play this game, and is the game deep enough for repeated play - do I want to play this game again and again.

Feedback will be collected through play-testing - where a gamer is monitored in person, and through surveys - where players are asked in-game to complete a feedback survey.

4   Captured Data and Retention

This section summarizes the data that will be collected during the pilots and the methodologies that will be applied in order to achieve that. However, no detailed description is provided in this document; the reader is encouraged to find more detailed descriptions in deliverable D6.5 - Data Management Plan.

4.1   Food Chain Pilot (Greece)

4.1.1   Data to be collected

The Food Supply Chain pilot will collect data from all the IoT platforms involved along the path from-field-to-fork. That includes sensor data from the various sensors as well as user data for all the actors that will be involved in the pilot. The data from all IoT platforms will be in JSON format leading to easy integration. The data will be stored in each IoT platform storage infrastructure (subset of them will also be stored in each platform's DLT), and will be private. Access to the pilot participants will be provided through the BP. The data that will be generated will be related to commercial products and companies; therefore, it will not be open to access outside the pilot participants. However, we plan to make a dataset publicly available. That dataset will have been created for testing and repeatability purposes and will resemble data collected for the scenarios described in section 3.1.3.

4.1.2   Data collection methodologies

For this pilot two main data collection methodologies will be utilized:

1. Data logging from sensor devices
2. Questionnaires

All sensor devices that will be deployed along the path from-field-to-fork will provide data to the involved IoT platforms. This data will then be stored and processed according to the business logic of each platform.

In order to get end user feedback (as mentioned in section 3.1.5), questionnaires will be used. Those will be used mainly as a means of evaluation of the usefulness of the Food Chain pilot services as a whole. As mentioned earlier, these questionnaires will be anonymous.

4.2   Energy Pilot (Estonia)

4.2.1   Data to be collected

The data that is collected during the Estonian Energy pilot can be split in three categories:

1) The energy consumption data from the smart meters. That includes both the readings and the metadata about the smart meter, authentication process. Input from smart meters creates the largest data volume and it is essential that the scalability issues as well as the integrity of data are covered.
2) The verification and agreement data together with data transactions. This is the core part of the Estonian energy pilot to be able to fulfil the goals that have been set.
3) System log files that are needed for agreeing on the data import-export side.

More detailed view of data and processes are described in Deliverable 6.5 (Data Management Plan)

As Estonian energy pilot is using other platforms for input (like Estfeed platform operated by Elering), there are also datasets that are relevant to pilot use-case and scenario but are

handled as a constant from pilot perspective. These include the data processing inside the Estfeed (and other) platforms, the customer request management system and customer data.

4.2.2 Data collection methodologies

For Estonian energy pilot the main data collection methodologies will be data received from existing smart meter platforms and smart meter microgrid.

4.3 Energy Pilot (Italy)

4.3.1 Data to be collected

The Italian Energy Pilot, will collect data from EV charging stations (out of service, number of sockets in use, current vehicle ID attached, energy data), voltmeters, current meters, log and access data from servers, regarding power exchange, demand/response, PV power generation and EV data (battery State-of-Charge (%), residual autonomy (Km), minutes to full charge (m), geographic location, doors car state, engine car state). Collected data will be in CSV, XLS, JSON or raw format while their volume will be around some KBs.

Access for partners will be provided, if needed for the project objectives. However, the data will not be made public.

Data will be collected from IoT platforms; relevant data will be stored using the platform's blockchain infrastructure.

4.3.2 Data collection methodologies

EV data will be collected each 25 seconds, using the communication between EMOT OBD device and EMOT TCP/IP server, and EVSE data will be collected each 15 seconds, using communication between EMOT charging station single board computer and EMOT OCPP TCP/IP server.

All the smart meters, electric vehicles and charging stations will provide data to the involved IoT platforms. This data will then be stored and processed according to the business logic of each platform.

4.4 Mobile Gaming Pilot (Finland)

4.4.1 Data to be collected

Mobile Game Analytics

Session data collected from the consumer playing the game, used to understand player behaviours to improve and tune the game. This data will be collected from game's smartphone client, game server and game services (payment etc.). Data collection and storage process will utilize Rovio's data analytics pipeline. This data will be in JSON format, MB in size, with the potential for billions analytic events.

IoT device data

Data collected from IoT devices used to as part of IoT mini-game(s). These game(s) would leverage IoT devices via the Sofie platform to provide game experiences, for example using Beacons for a scavenger hunt completing 'collection' missions built on the assets from the core game potentially providing a reward in the game of from the locations (e.g. retailer). This data will be JSON format, KB in size with the potential for millions of devices.

4.4.2 Data collection methodologies

For this pilot two main data collection methodologies will be utilized:

- Analytic events logging from game client (smartphone) and IoT device data
- In-game surveys of players.