Multi-layered Security Technologies

for hyper-connected smart cities

D2.7: Integrated Prototype – final release

June 2021

Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, BigData, Cloud and IoT

Project acronym	M-Sec
Deliverable	D2.7 Integrated Prototype – final release
Work Package	WP2
Submission date	June 2021
Deliverable lead	Xavier Cases (WLI)
Authors	Xavier Cases (WLI), Alberto Puras (TST), Keio team (KEIO), Orfeas Voutyras (ICCS), Aránzazu Sanz (TST)
Internal reviewer	Aamir Bokhari (YNU) / Alberto Puras (TST)
Dissemination Level	Public
Type of deliverable	DEM

The M-Sec project is jointly funded by the European Union's Horizon 2020 research and innovation programme (contract No 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No. 19501).

Version history

#	Date	Authors (Organization)	Changes
v0.1	16 April 2021	Xavier Cases (WLI)	Full ToC and assignments
v0.2	30 April 2021	Xavier Cases (WLI)	Reviewed diagrams
v0.3	14 May 2021	Xavier Cases (WLI)	Reviewed Integration readiness levels
v0.4	28 May 2021	Xavier Cases (WLI)	Reviewed technology readiness levels
v0.5	11 June 2021	Xavier Cases (WLI)	Final diagrams and integration points matrixes
v0.6	15 June 2021	Xavier Cases (WLI)	Use Case 2 review
v0.7	18 June 2021	Alberto Puras (TST)	Use Case 1 review
v0.8	22 June 2021	Keio team (KEIO)	Use Case 3 and 4 review
v0.9	25 June 2021	Orfeas Voutyras (ICCS)	SRL Calculations
v0.10	28 June 2021	Aamir Bokhari (YNU)	Internal Review
v0.11	29 June 2021	Aránzazu Sanz (TST)	Internal Review
v1.0	30 June 2021	Xavier Cases (WLI)	Final version
V1.1	1 July 2021	Xavier Cases (WLI)	Reviewing some last minute comments

Table of Contents

List of Tables

List of Figures

Glossary

Acronym	Description	Acronym	Description
AI	Artificial Intelligence	OS	Operating System
API	Application Programming Interface	P2P	Peer-to-peer
APP	Application	QoL	Quality of Life
CCDB	Crypto Companion Database	SDK	Software Development Kit
Dx.y	Deliverable y of WP x	SRA	System Readiness Level
EU	European Union	SRL	System Readiness Level
FG	Functional Group	TRL	Technology Readiness Level
ID	Identifier	T&R	Trust and Reputation
IoT	Internet of Things	Tx.y	Task y of WP x
IRL	Integration Readiness Level	UC	Use Case
NASA	National Aeronautics and Space Administration	VPN	Virtual Private Network
NDA	Non-Disclosure Agreement	WP	Work Package

1. Introduction

1.1 Scope of the document

This deliverable is the outcome of Task 2.3 “Overall Integration”, which focuses on the overall integration of all components and modules developed and deployed in WP4. It generates the integrated system providing the M-Sec functionalities as they have been specified in WP3.

Following the methodology together with a series of best practices, work-plans and testing schemes, an overall integration of all components and modules have been accomplished.

For clarity, the integration points between assets are being presented per Use Case (UC), as each of them has its own interaction with the assets in Secition3. A Global overview can be seen in Section2.

In Section 3, all subsections include:

- A short description of the Use Case and a summary of requirements.
- An interaction diagram showing the integration points in a functional view.
- An interaction matrix with all the integration points between the assets used in the UC.
- A Use Case System Readiness Level (SRL)
- A subsection to identify the type of each interaction.

Finally, in Section 4 the conclusion extracted from all the work done is provided.

1.2 Relationship to other work packages and tasks

Deliverable D2.7 “Integrated Prototype – final release”, uses as input the M-Sec requirements and architecture from deliverables D3.2 “M-Sec requirements” and D3.4 “M-Sec architecture”, as well as the developments performed in the WP4 and the methodology written in the deliverable D2.5 “Integration Plan”. As a result, the following deliverables are taken into account:

- Deliverable D2.5 about Integration Plan from Task 2.3.
- Deliverable D2.6 about Integrated Prototype - First release from Task 2.3.
- Deliverable D3.2 about M-Sec requirements from Task 3.1.
- Deliverable D3.4 about M-Sec architecture from Task 3.2.
- Deliverable D4.2 about IoT Security from Task 4.1.
- Deliverable D4.4 about cloud and data level security from Task 4.2.
- Deliverable D4.6 about P2P level security and blockchains from Task 4.3.
- Deliverable D4.8 about application level security from Task 4.4.
- Deliverable D4.10 about end-to-end security from Task 4.5.

2. Global overview of platform integration

2.1 Overall interaction diagram

The expected interaction in this diagram will focus on all the assets involved in M-Sec.

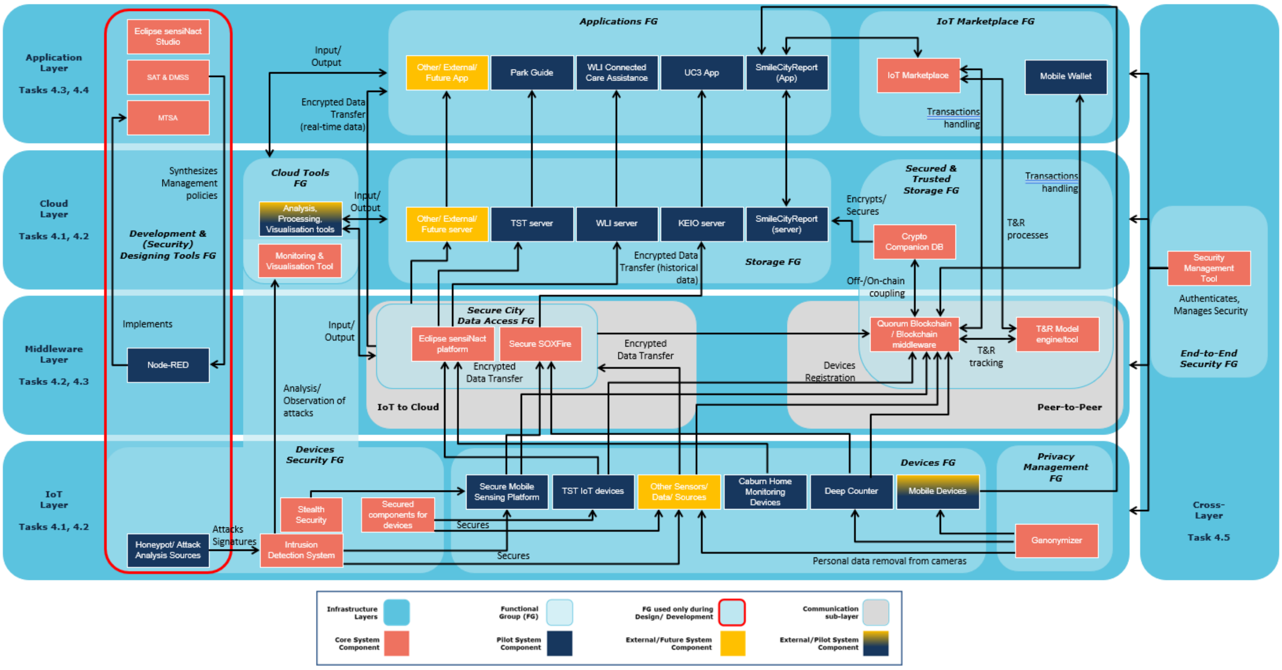
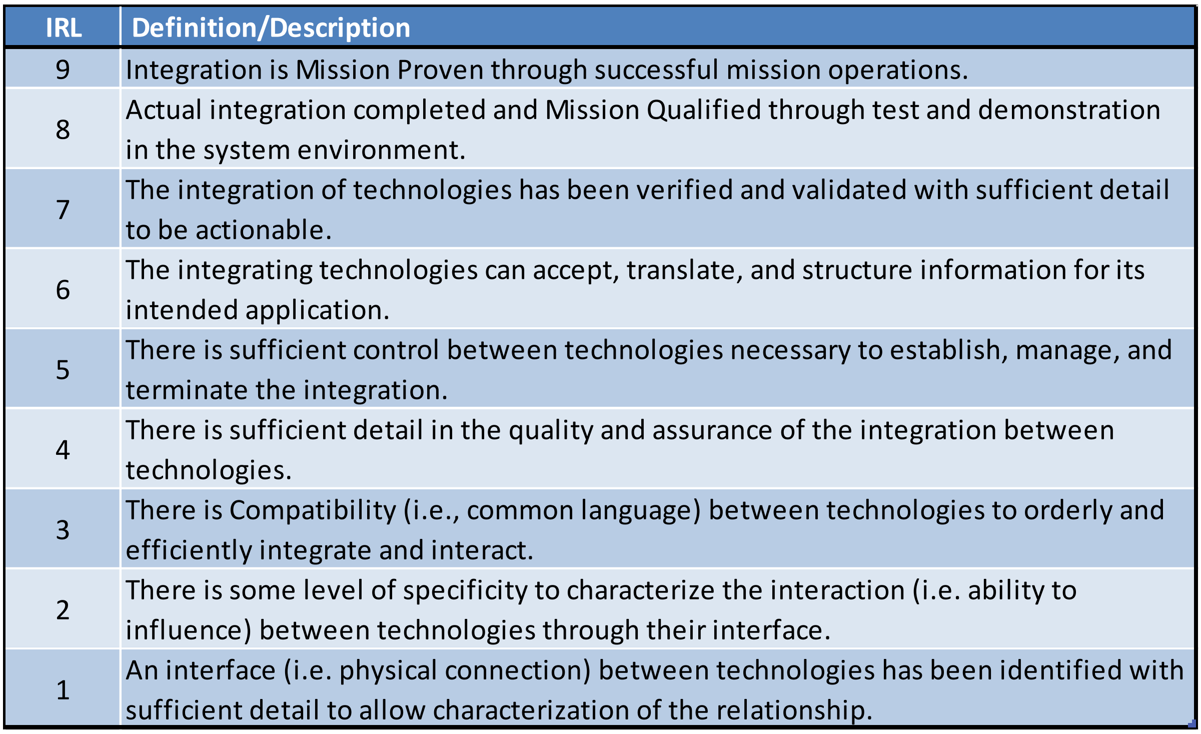


Figure 1. Architectural diagram with all interaction points of M-Sec.

2.2 IRL matrix

The values and descriptions used in this document for the Interface Readiness Level (IRL) matrixes are shown in Table 1.

Table 1. Interface Readiness Level definitions.



IRL	Definition/Description
9	Integration is Mission Proven through successful mission operations.
8	Actual integration completed and Mission Qualified through test and demonstration in the system environment.
7	The integration of technologies has been verified and validated with sufficient detail to be actionable.
6	The integrating technologies can accept, translate, and structure information for its intended application.
5	There is sufficient control between technologies necessary to establish, manage, and terminate the integration.
4	There is sufficient detail in the quality and assurance of the integration between technologies.
3	There is Compatibility (i.e., common language) between technologies to orderly and efficiently integrate and interact.
2	There is some level of specificity to characterize the interaction (i.e. ability to influence) between technologies through their interface.
1	An interface (i.e. physical connection) between technologies has been identified with sufficient detail to allow characterization of the relationship.

An interaction point shows the readiness level of an integration between the assets. The interaction matrix expected to take place between the assets in M-Sec is shown in Table 2.

Table 2. Overall interaction matrix.

M-Sec	Park guide	TST Server	IoT Marketplace	Eclipse sensiNact platform (and Studio)	Security Management Tool	TST IoT crowd-counting devices	TST IoT environmental devices	Secured components for devices and gateways	Quorum Blockchain framework	Honeypot (IoTPOT)	T&S FG API	Crypto Companion Database	Worldline Connected Care Assistance	Worldline Server	Caburn Home Monitoring Devices	Secure SOXFire	Node-RED	Modal Transition System Analyser (MTSA)	Visualization Tool	Deep Counter (Garbage Identification AI)	Secure Mobile Sensing Platform	Ganonymizer	Intrusion Detection System (IDS)	Honeypot (IoTPOT)	Stealth Security Componentç	SmileCityReport (App)	SmileCityReport (Server)	Security Analysis tool + Development Method for secure Services	T&R Model engine/tool	Mobile Wallet
Park Guide	9	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TST Server	9	9	0	7	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IoT Marketplace	0	0	9	5	2	0	0	0	7	0	0	0	0	7	0	5	9	0	0	0	0	0	0	0	0	5	5	0	3	1
Eclipse sensiNact platform (and Studio)	0	7	5	9	7	7	7	0	5	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Security Management Tool	0	0	2	7	9	0	0	0	2	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TST IoT crowd-counting devices	0	0	0	7	0	9	0	7	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TST IoT environmental devices	0	0	0	7	0	0	9	7	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Secured components for devices and gateways	0	0	0	0	0	7	7	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Quorum Blockchain framework	0	0	7	5	2	0	0	0	9	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	1
Honeypot (IoTPOT)	0	0	0	0	0	7	7	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T&S FG API	0	7	0	0	7	0	0	0	0	0	9	7	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Crypto Companion Database	0	0	0	0	0	0	0	0	7	0	7	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Worldline Connected Care Assistance	0	0	0	0	0	0	0	0	0	0	0	0	9	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Worldline Server	0	0	7	7	0	0	0	0	0	0	7	0	9	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Caburn Home Monitoring Devices	0	0	0	7	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Secure SOXFire	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	9	7	7	0	7	7	0	0	0	0	7	7	0	0	0
Node-RED	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	7	9	7	0	0	0	7	0	0	0	0	0	0	0	0
Modal Transition System Analyser (MTSA)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	7	9	0	0	0	0	0	0	0	0	0	0	0	0
Visualization Tool	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	7	0	0	0	0	0	0	0
Deep Counter (Garbage Identification AI)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	9	7	0	0	0	0	0	0	0	0	0
Secure Mobile Sensing Platform	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	7	9	7	0	0	5	0	0	0	0	0
Ganonymizer	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	7	9	0	0	0	7	0	0	0	0
Intrusion Detection System (IDS)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	9	9	0	0	0	0	0	0
Honeypot (IoTPOT)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	9	0	0	0	0	0	0
Stealth Security Componentç	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	9	0	0	0	0	0
SmileCityReport (App)	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	7	0	0	0	9	9	0	0	0
SmileCityReport (Server)	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	9	9	0	0	0
Security Analysis tool + Development Method for sec	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0
T&R Model engine/tool	0	0	3	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0
Mobile Wallet	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9

2.3 Integration descriptions and details

Although all integration points have been started not all of them are completed. A lot of work has been put in the integrations in order to have a robust and trusted platform. Following can be found a list of the most relevant integrations with a short description about what has been accomplished. Some of the integrations expected, finally were discarded or delayed because of various reasons: time in order to perform proper testing due to COVID-19 pandemic, not meeting the needed functionality, prioritization of core integrations, and others. At the date of this writing the integrations are still being developed/tested in order to stay on track for the Pilots.

Crypto Companion Database – Quorum Blockchain framework/Blockchain middleware

This integration has been completed. The integration between the Crypto Companion Database and the Quorum Blockchain framework / Blockchain middleware relies on the need to create a transaction each time some data needs to be stored. The Crypto Companion Database together with the blockchain help to be tampered proof and GDPR compliant at the same time.

Worldline Connected Care Assistance – Secured & Trusted Storage Functional Group API

This integration has been completed. The integration between these two assets has been performed adding a module in the Connected Care Assistance asset in order to have the usual connection to the database of the application and a new connection that will provide extra security and encryption for the sensitive data. This integration point has been switched from Crypto Companion Database to the Functional Group API.

Worldline Connected Care Assistance – Eclipse sensiNact platform (and Studio)

This integration has been completed. Connected Care Assistance connects to the Eclipse sensiNact platfrom from a provided API in order to retrieve the data from the devices.

Eclipse sensiNact platform (and Studio) – Caburn Home Monitoring Devices

This integration has been completed. Eclipse sensiNact connects to the broker and serve the data needed exposing an API.

Secured & Trusted Storage Functional Group API – Security Management Tool

This integration has been completed. The Security Management Tool authenticates the users that want to use the API and ensures no external calls are made.

Worldline Connected Care Assistance – IoT Marketplace

The integration has been completed. The Connected Care Assistance is connected to the IoT Marketplace, registering and providing raw data to be sold.

Secure SOXFire - Eclipse sensiNact platform (and Studio)

The integration has been completed. Sensor data sent to Secure SOXFire can be forwarded to the Eclipse sensiNact platform (and Studio) through the integration point.

Secure SOXFire - Secure Mobile Sensing Platform

The integration has been completed. The IoT devices included in the Secure Mobile Sensing Platform can transmit all the sensor data through Secure SOXFire.

Secure SOXFire – SmileCityReport (App & Server)

The integration has been completed. SmileCityReport (Server) is built atop Secure SOXFire. Pictures taken by SmileCityReport (App) software on a smart phone can be transmitted to subscribers through Secure SOXFire.

Secure SOXFire - Deep Counter (Garbage Identification AI)

The integration has been completed. Deep Counter (Garbage Identification AI) data is transmitted to Secure SOXFire through the Secure Mobile Sensing Platform, then can be forwarded to other platforms including Node-RED and Eclipse sensiNact platform (and Studio).

Secure Mobile Sensing Platform - Deep Counter (Garbage Identification AI)

The integration has been completed. Deep Counter (Garbage Identification AI) data is transmitted to Secure SOXFire through the Secure Mobile Sensing Platform, then can be forwarded to other platforms including Node-RED and Eclipse sensiNact platform (and Studio).

Ganonymizer – SmileCityReport (App & Server)

The integration has been completed. The images taken by SmileCityReport (App), installed in diverse smartphones running different Operating Systems (OS), are anonymized by Ganonymizer. To do that, Ganonymizer has been implemented to export a web API and SmileCityReport (Server) sends the images to that API.

Ganonymizer - Deep Counter (Garbage Identification AI)

The integration has been completed. The images taken by Deep Counter (Garbage Identification AI), running at the garbage truck side, are anonymized by Ganonymizer. To do that, Ganonymizer has been implemented to export a web API and SmileCityReport (Server) sends the images to that API.

IoT crowd-counting and environmental devices - Secure components for devices and gateways

The integration among the IoT devices and the secure components for devices and gateways is currently ongoing. As a starting point, both the crowd counting devices and the environmental ones test their operation sending data to a standard ST-TPM-RASPI. This data is encrypted in the RASPI module and forwarded again to the micro-controller in the IoT device that in turn sends the information encrypted via wireless technology to the other end of the communication link, where it is de-encrypted. Once this process is validated, the interaction with the complete secured component ensues, thus achieving the goal of incorporating extended security for these IoT devices.

IoT crowd-counting and environmental devices - Honeypot (IoTPOT)

Honeypot (IoTPOT) has been used for testing purposes of the IoT devices, cyber-attack patterns and signatures have been extracted and analysed.

IoT crowd-counting and environmental devices – Eclipse sensiNact platform (and Studio)

A similar approach applies to the interaction with the Eclipse sensiNact platform (and Studio). In this particular case, the first step consists in having a NDA ready among the involved parties. Afterwards, the data produced by the IoT devices will adjust to the format accepted by Eclipse sensiNact platform (and Studio).

Park Guide - TST IoT crowd-counting and environmental devices

The Park Guide application developed in the context of Use Case 1 receives the decrypted information provided by the sensors integrated in the IoT devices and put it into the user interface to allow the visualization of measurements in tables and linecharts.

Park Guide – Secured & Trusted Storage Functional Group API

The Park Guide application specifically devised for this Use Case will receive from the Crypto Companion Database (through S&T Storage FG API) the information generated by the sensors deployed in the Las Llamas Park.

SmileCityReport (App & Server) – Secure SOXFire, Companion Database and IoT Marketplace

The main interaction in this case involves the mobile application SmileCityReport dubbed “SushiRepo” (that will be the one employed by users active in this use case), feeding Secure SOXFire tool and providing data to both the Companion Database and the IoT Marketplace. The stakeholders external to the consortium will have the chance of taking a look into this data through the marketplace and decide whether they find it useful when preparing their very own solutions or prefer to opt out for other alternatives in the marketplace.

Mobile Wallet – Quorum Blockchain framework/Blockchain middleware

The integration of Mobile Wallet with Quorum Blockchain framework/Blockchain middleware was based on Metamask[1] (see Figure 2). Using it as a browser extension, the user is able to connect to the Blockchain. Other features of Metamask and Web3 library have been exploited in order to authenticate and verify the identity of a user offering more transparency and security. This way, the user can complete a transaction (e.g., transfer of M-Sec tokens) only if he/she has the private/public key of the account and a message/transaction can be signed by a specific user.

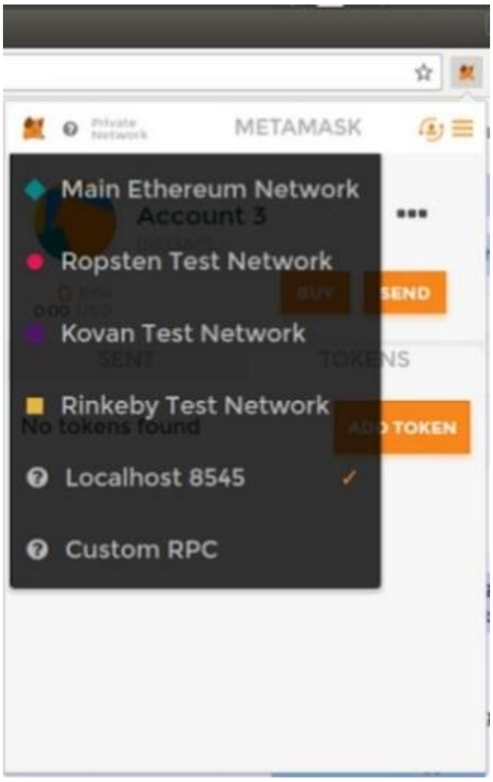


Figure 2. Metamask screenshot.

Intrusion Detection System (IDS) - Secure Mobile Sensing Platform

The IDS is developed for Linux operating system (OS) that is the same on which the Secure Mobile Sensing Platform runs. Therefore, the integration is automatic, and both runs side-by-side because of being built for the same version of OS.

Intrusion Detection System (IDS) - Visualization Tool

Visualization Tool is based on elastic search and its agent are installed in the IDS, where they collect logs from the IDS and uploads them to an elastic server in the cloud.

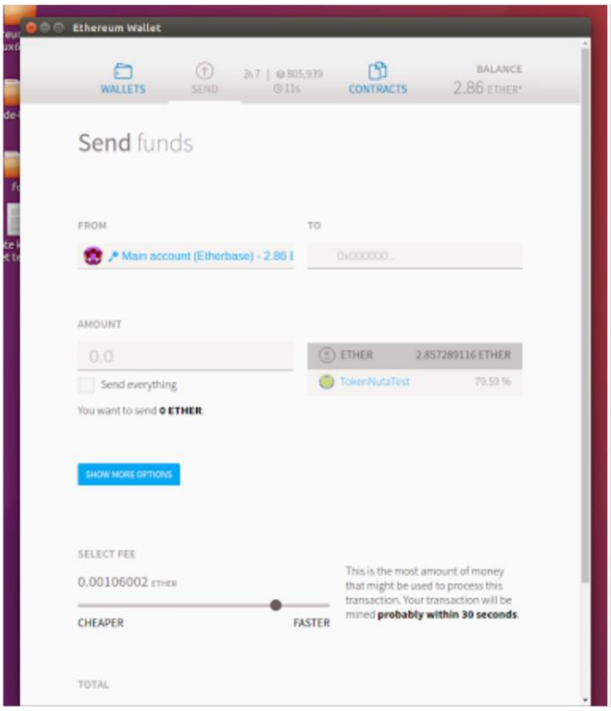
[1] https://metamask.io/

Intrusion Detection System (IDS) - Honeypot (IoTPOT)

The Honeypot (IoTPOT) is a standalone system that is used as a testbed for analysing attacks on various IoT devices during the designing and testing phase. The integration with IDS is manually conducted by writing the signature patterns observed by the Honeypot (IoTPOT) as signature rules in the IDS.

IoT Marketplace – Mobile Wallet

The integration of IoT Marketplace with Mobile Wallet that has already been accomplished allows the user to have access to the different smart contracts. An important aspect of this integration is the ability of a user to watch the M-Sec Token, which is a Solidity[2] smart contract running on blockchain. The use of different Wallets such as the Ethereum Wallet[3] (see Figure 3) have been explored, this enables watching, sending and transferring Tokens to other users. Using the wallet and logging in using his/her keys, the user can have a visual representation of the information stored in the blockchain (of specific smart contracts) and interact with it in a user-friendly manner.



Send funds

FROM: Main account (Etherbase) - 2.86 E

TO: 0x000000...

AMOUNT: 0.0

ETHER 2.857289116 ETHER

TokenNutaTest 79.59 %

□ Send everything

You want to send **0 ETHER**.

SELECT FEE: 0.00106002 ETHER

This is the most amount of money that might be used to process this transaction. Your transaction will be mined **probably within 30 seconds**.

TOTAL

Figure 3. Ethereum Wallet screenshot.

IoT Marketplace – T&R Model engine/tool

The Trust and Reputation Model Engine have been migrated to run on the Blockchain platform. An implementation based on Solidity smart contracts is integrated with the IoT Marketplace running on top of Quorum blockchain platform. This way the user can browse all the registered sensors in the respective smart contract and find information about them such as trust, reputation, and feedback from previous purchases.

[2] https://solidity.readthedocs.io/

[3] https://ethereum.org/wallets/

Additional features which ensure that operators of registered sensors will actually provide the data to buyers and data validation have also been considered.

Node-RED – IoT Marketplace

The implementation of M-Sec's IoT Marketplace has been based on Solidity smart contracts running on top of blockchain. Additionally, the integration with Node-Red and the development of respective Node-Red flows (see Figure 4) allowed the connection with different APIs, web services, IoT devices, sensors, and data sources. More than 10 flows have been implemented handling HTTP requests as well (e.g., search of purchases, search registered sensors, buy data, register sensors, transfer tokens etc.).

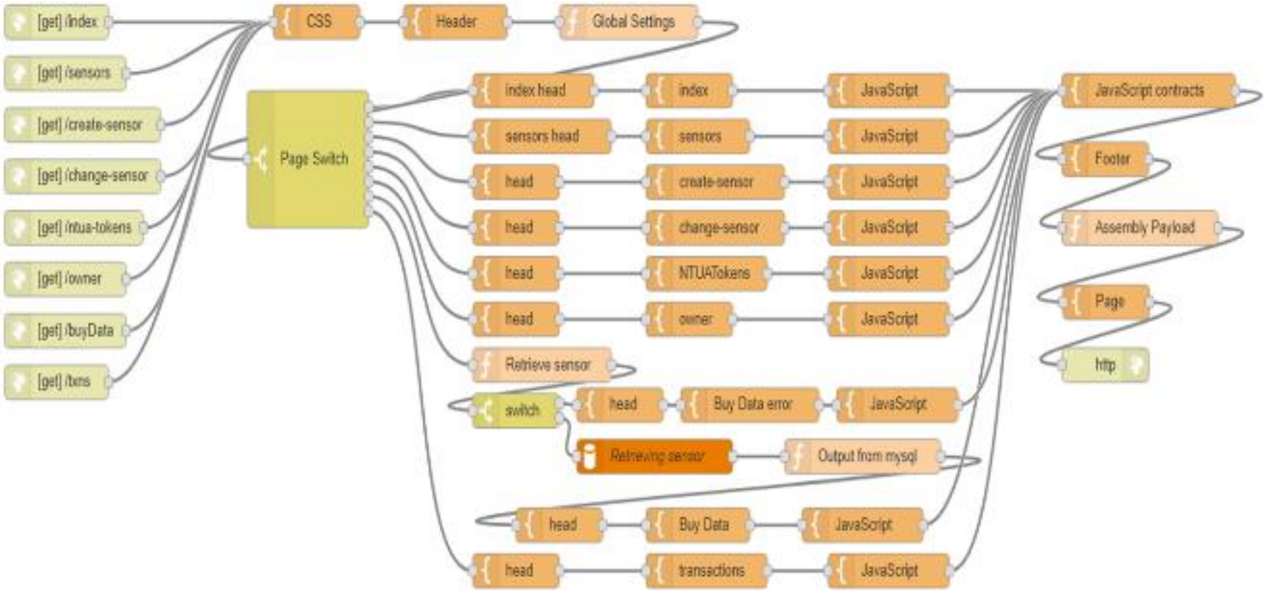


Figure 4. Node-Red flows.

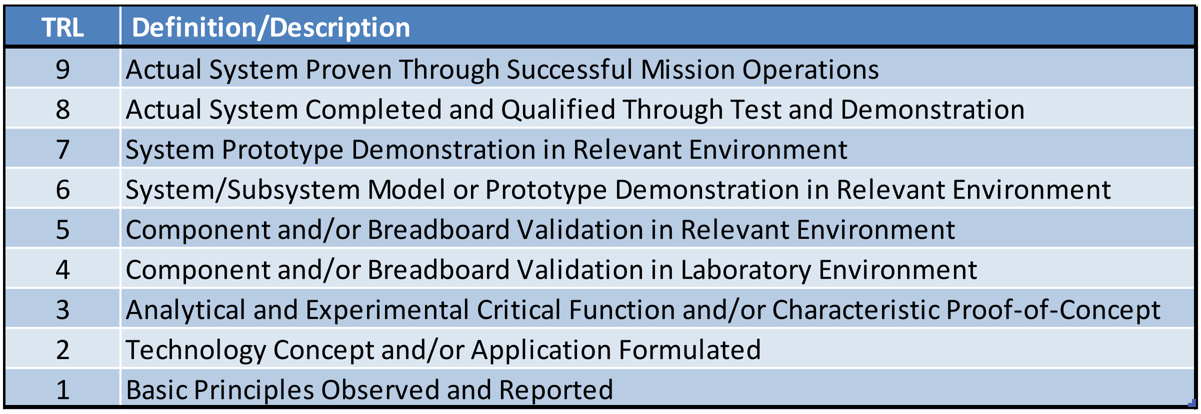
IoT Marketplace – Quorum Blockchain framework/Blockchain Middleware

An integration process among the IoT Marketplace and the Quorum Blockchain framework/Blockchain Middleware has been conducted. IoT Marketplace communicates with other smart contracts deployed on Quorum blockchain. Additionally, other services, which are part of the Middleware such as Handlers of On-chain/Off-chain data, uploads and accounts are important for the functionality of the Marketplace.

2.4 Components list and their TRL progress

In Table 3 readers can find a reference with values and descriptions, to understand the Technology Readiness Level (TRL) scale.

Table 3. Technology Readiness Level definitions.



TRL	Definition/Description
9	Actual System Proven Through Successful Mission Operations
8	Actual System Completed and Qualified Through Test and Demonstration
7	System Prototype Demonstration in Relevant Environment
6	System/Subsystem Model or Prototype Demonstration in Relevant Environment
5	Component and/or Breadboard Validation in Relevant Environment
4	Component and/or Breadboard Validation in Laboratory Environment
3	Analytical and Experimental Critical Function and/or Characteristic Proof-of-Concept
2	Technology Concept and/or Application Formulated
1	Basic Principles Observed and Reported

Table 4 recaps the TRL of all the components that are part of the M-Sec prototype. There are three columns in order to appreciate the evolution of them through the years. The TRL value in “Year Zero (Y0)” reflects the maturity level at which the asset was brought into the M-Sec project. The ones with a value of 1 are assets created specifically for the need of the M-Sec platform.

Table 4. Asset's Technology Readiness Level table.

Asset Name	TRL Y0	TRL Y1	TRL Y2	TRL Y3
Caburn Home Monitoring Devices	7	7	7	7
Crypto Companion Database	1	4	6	7
Deep Counter (Garbage Identification AI)	1	4	6	6
Eclipse sensiNact platform (and Studio)	3	4	5	7
Ganonymizer	1	3	6	7
Honeypot (IoTPOT)	5	6	6	7
Intrusion Detection System (IDS)	2	4	6	7
IoT Marketplace	2	4	7	9
Mobile Wallet	7	7	7	7
Modal Transition System Analyser (MTSA)	2	3	5	7
Node-RED	9	9	9	9
Park Guide	1	2	5	7
Quorum Blockchain framework	4	5	6	7
Secure Mobile Sensing Platform	2	3	6	6
Secure SOXFire	2	3	6	6
Secured components for devices and gateways	3	5	6	6
Security Analysis tool + Development Method for secure	1	2	4	4
Security Management Tool	1	3	4	5
SmileCityReport (App)	2	4	7	8
SmileCityReport (Server)	2	4	7	8
Stealth Security Component	0	0	2	5
T&R Model engine/tool	2	3	5	6
T&S FG API	0	0	0	7
TST IoT environmental devices	3	4	5	7
TST IoT crowd-counting devices	3	4	5	7
TST Server	1	2	5	7
Visualization Tool	2	3	6	6
Worldline Connected Care Assistance	3	4	5	7
Worldline Server	3	4	5	7

2.5 SRL table

In Table 5 readers can check a reference table, with value and description, to understand all values on System Readiness Level (SRL) as employed in this document.

Table 5. System Readiness Level descriptions.

SRL	Definition/Description
5	Operations & Support
4	Production & Development
3	System Development & Demonstration
2	Technology Development
1	Concept Refinement

Table 7 recaps the calculations performed to extract the Components SRL array for the overall M-Sec platform. The calculations have been made by the methodology written in deliverable D2.5 “Integration Plan” in section “2.2 Calculation”. As mentioned in that section, a Component SRL gives a picture of how well a specific component is integrated in the whole system (or subsystem, in the case of Use Cases), while the Composite SRL is the average of the Component SRLs and provides a metric for identifying the overall progress of the integration of all the components of the system (or subsystem). Composite SRLs are calculated on a scale from 0 to 1 (normalized value) and are then matched to a 5-levels scale (similar to the case of the TRL and IRL scales, which have 9 levels though). To translate the 0 to 1 scale to a 1 to 5 scale (the one presented in Table 5), an SRL Matching Model (Table 6) is used to map the decimal values to whole number values.

Table 6. SRL Matching Table.

SRL	Definition/Description	Composite SRL
5	Operations & Support	0,9 to 1,00
4	Production & Development	0,8 to 0,89
3	System Development & Demonstration	0,6 to 0,79
2	Technology Development	0,4 to 0,59
1	Concept Refinement	0,1 to 0,39

Table 7. M-Sec’s platform System Readiness Level.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Park Guide	7	2	126	1,56	0,78
TST Server	7	4	224	2,77	0,69
IoT Marketplace	9	11	440	5,43	0,49
Eclipse sensiNact platform (and Studio)	7	9	423	5,22	0,58
Security Management Tool	5	5	175	2,16	0,43
TST IoT crowd-counting devices	7	4	203	2,51	0,63
TST IoT environmental devices	7	4	203	2,51	0,63
Secured components for devices and gateways	6	3	152	1,88	0,63
Quorum Blockchain framework	7	7	269	3,32	0,47
Honeypot (IoTPOT)	7	3	161	1,99	0,66
T&S FG API	7	5	245	3,02	0,60
Crypto Companion Database	7	3	161	1,99	0,66
Worldline Connected Care Assistance	7	2	126	1,56	0,78
Worldline Server	7	5	287	3,54	0,71
Caburn Home Monitoring Devices	7	2	112	1,38	0,69
Secure SOXFire	6	8	407	5,02	0,63
Node-RED	9	5	302	3,73	0,75
Modal Transition System Analyser (MTSA)	7	3	168	2,07	0,69
Visualization Tool	6	2	103	1,27	0,64
Deep Counter (Garbage Identification AI)	6	3	138	1,70	0,57
Secure Mobile Sensing Platform	6	5	212	2,62	0,52
Ganonymizer	7	4	224	2,77	0,69
Intrusion Detection System (IDS)	7	3	168	2,07	0,69
Honeypot (IoTPOT)	7	2	126	1,56	0,78
Stealth Security Componentç	5	2	75	0,93	0,46
SmileCityReport (App)	8	5	280	3,46	0,69
SmileCityReport (Server)	8	4	231	2,85	0,71
Security Analysis tool + Development Method for secure Services	4	1	36	0,44	0,44
T&R Model engine/tool	6	3	130	1,60	0,53
Mobile Wallet	7	3	79	0,98	0,33

After doing the calculations, the Composite SRL for the overall M-Sec platform is 0,62, which is mapped to an SRL of level 3 – System Development & Demonstration.

3. Integration readiness level analysis

3.1 Use Case 1

Short description for Use Case 1 and summary of requirements

Use Case 1 is aimed at enriching the experience of visitors in Las Llamas park by providing them with useful information, as well as curiosities of its flora and fauna. In order to achieve this objective, five environmental monitoring IoT devices have been deployed throughout the park. These IoT nodes measure five different environmental variables: temperature, humidity, CO2, volatile organic compounds, and noise. Besides, an innovative people counter device was developed and installed in the park to provide an estimation of the number of visitors in the park. Finally, nine QR codes are scattered throughout the park to provide interesting information about the biodiversity.

The information provided by the deployed IoT devices is relevant not only for citizens and tourists, but also for the Santander Municipality, since it can be used for programming actions in a more effective way.

Users will have access to all the information, including the data provided by the deployed sensors, through the Park Guide application (see Figure 5). This is a web application that has been especially designed to facilitate the visualization of measurements. In this regard, measurements are presented in tables and in plots.

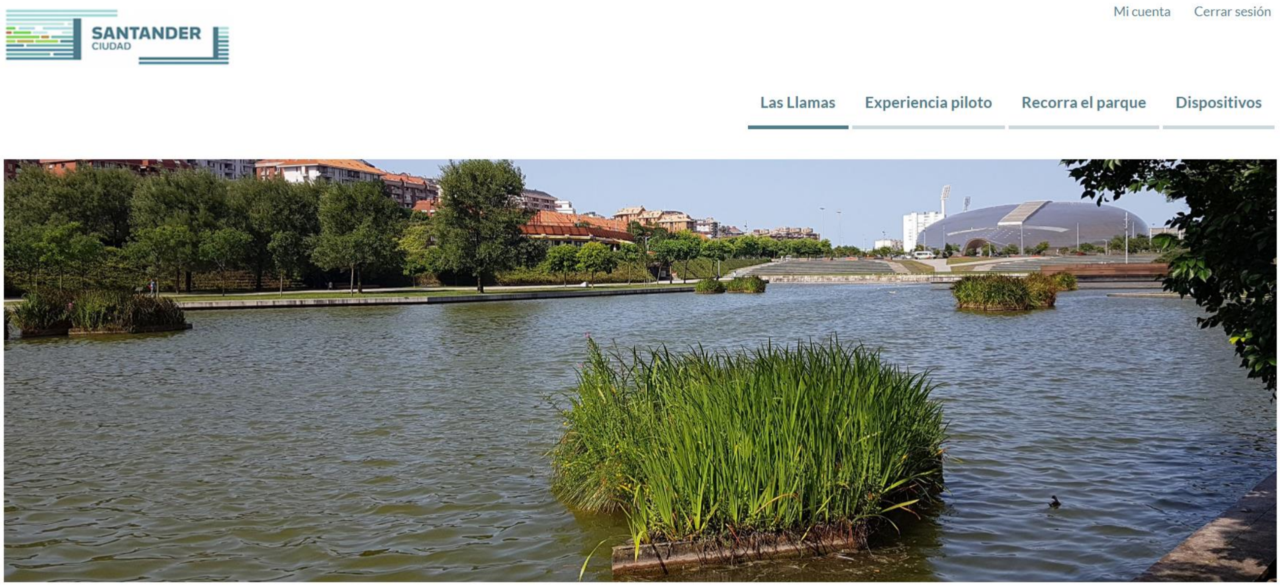


Figure 5. The Park Guide web application (Las Llamas Park – Use Case 1)

The design of the deployed infrastructure at Las Llamas park was accomplished to meet a set of specific requirements. The most relevant aspects that were considered were the following:

1) **Impact on the daily operations**. In this regard, the developed IoT devices are self-content sensors that do not require access to power/communication cables. To achieve this goal, IoT devices were

endowed with batteries and wireless communication. As a result, the sensors could be easily deployed (see Figure 6 and Figure 7) and do not difficult daily operation of the park, from both user and maintenance points of view.

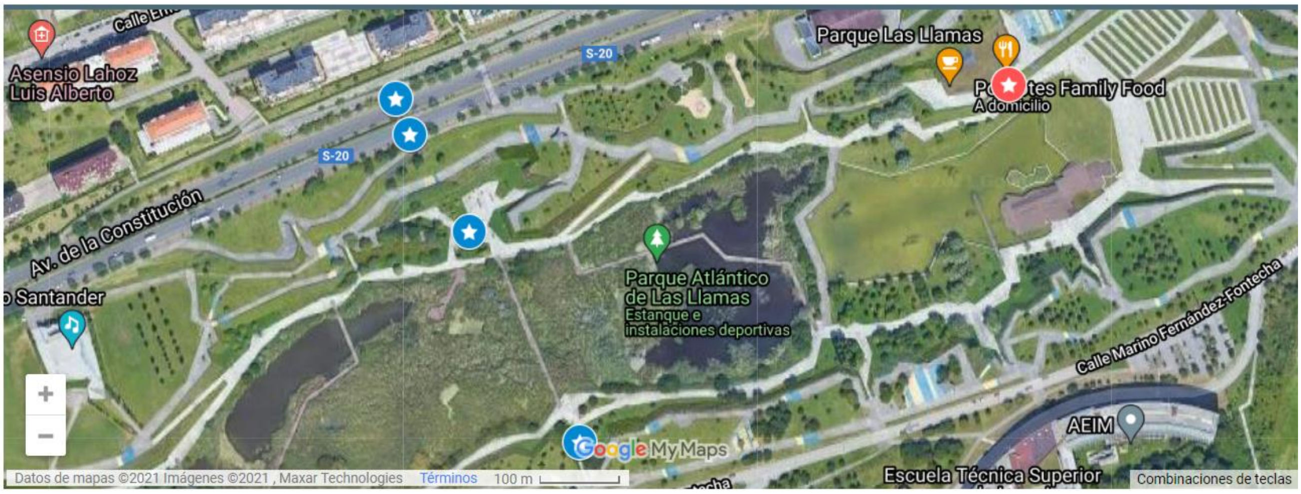

Calle Er
Asensio Lahoz Luis Alberto
S-20
S-20
Av. de la Constitución
o Santander
Parque Las Llamas
P tes Family Food
A domicilio
Parque Atlántico de Las Llamas
Estanque e instalaciones deportivas
Calle Marino Fernández-Fontecha
AEIM
Escuela Técnica Superior
Google My Maps
Datos de mapas ©2021 Imágenes ©2021 , Maxar Technologies
Términos
100 m
Combinaciones de teclas

Figure 6. Placement of the sensors. Blue icons represent the environmental sensors, while the red one is for the people counter device.

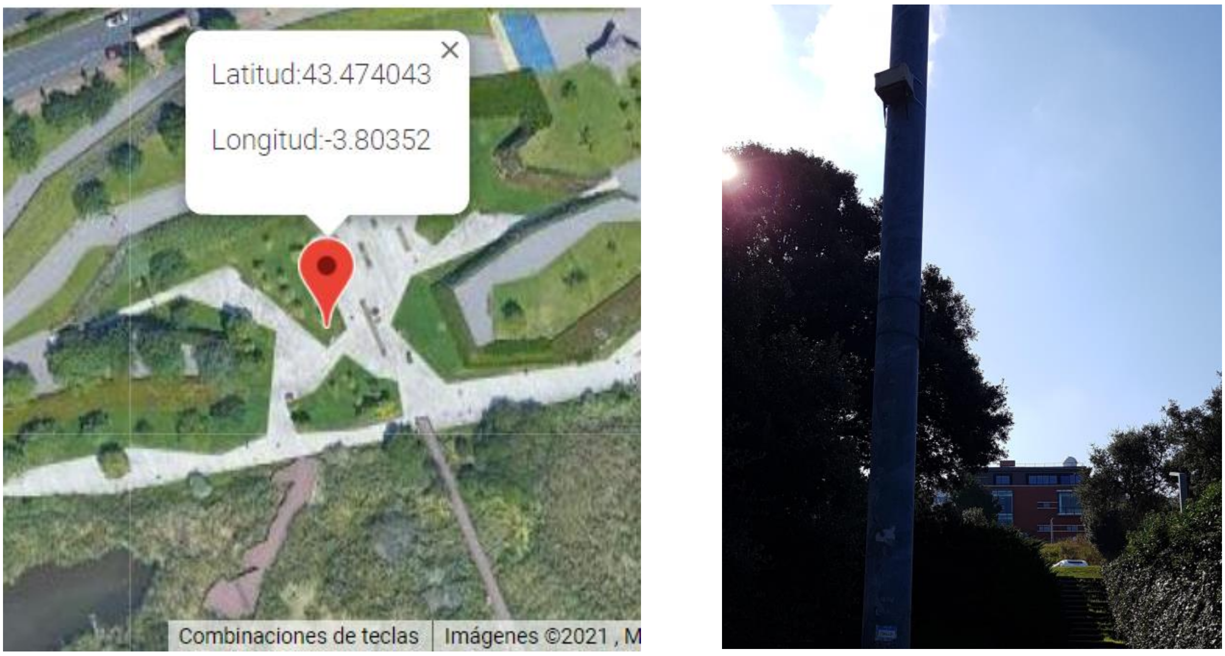


Figure 7. Global coordinates of one of the sensors obtained through the web application (left). Environmental sensor installed on a streetlight.

2) **Data access and visualization**. The localization of the sensors can be visualized in a satellite view of the park. By clicking on the different icons (i.e., blue: environmental sensors and red: people counter) the related measurements can be accessed. Since the sensors send new measurements every hour,

data presented in the web application is hourly updated. The last measurements are shown in tables, while historic data from the last month, week and 48 hours are presented in a graphical way with plots. Data time-histories are the basis for the city economic development division and event organisers statistical analysis.

Figure 8, Figure 9, and Figure 10 depict how the measurements are presented in the Use Case 1 related web page.

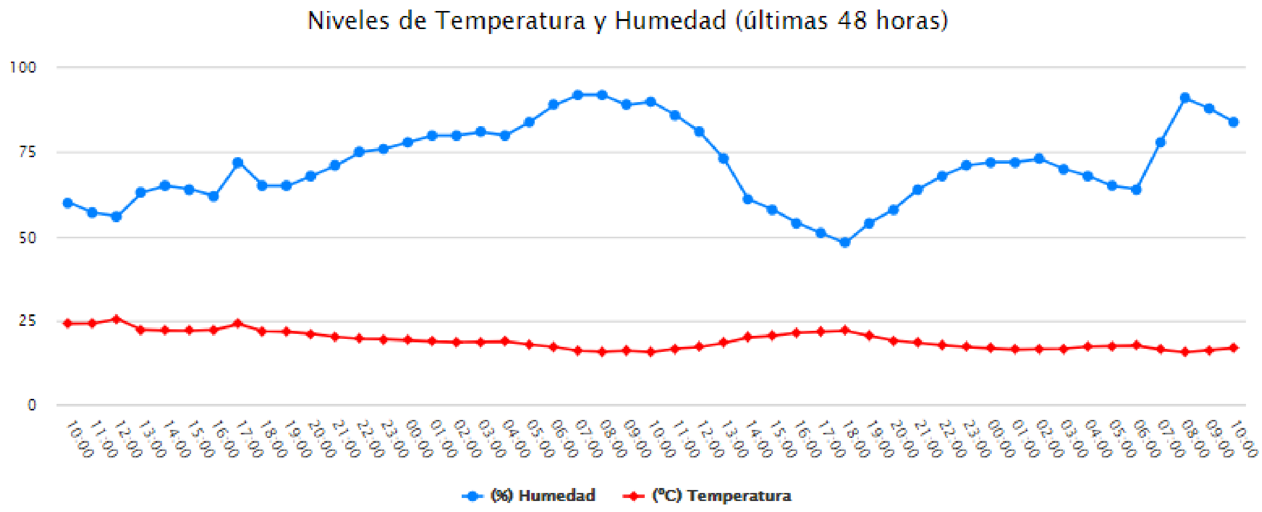


Figure 8. Temperature (red) and humidity (blue) plots to inform about their evolution during the last 48 hours.

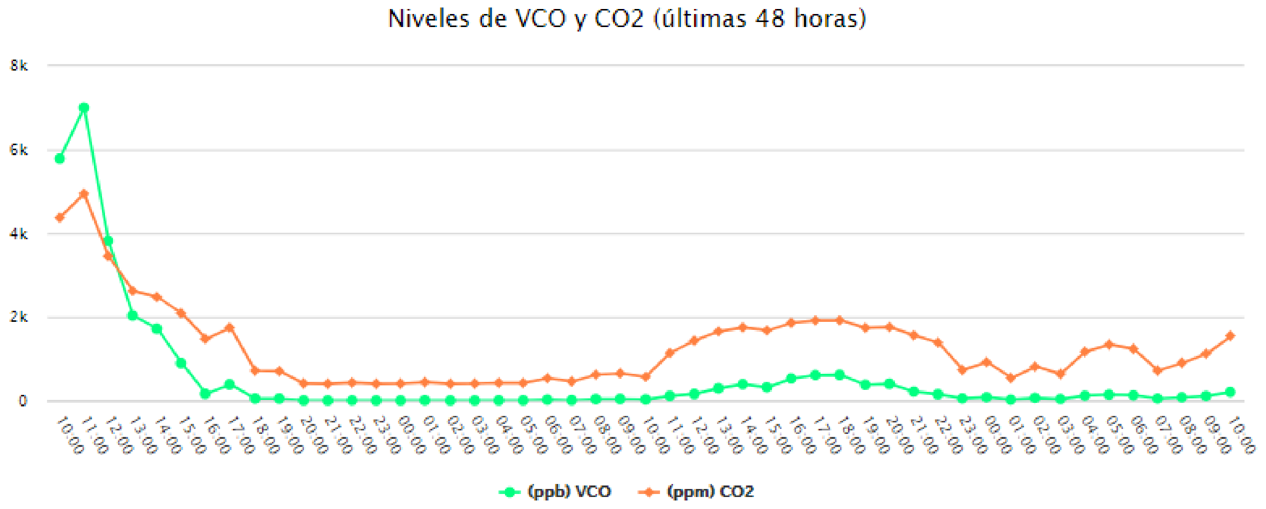


Figure 9. CO2 (orange) and Volatile Organic Compounds (green) plots to inform about their evolution during the last 48 hours.

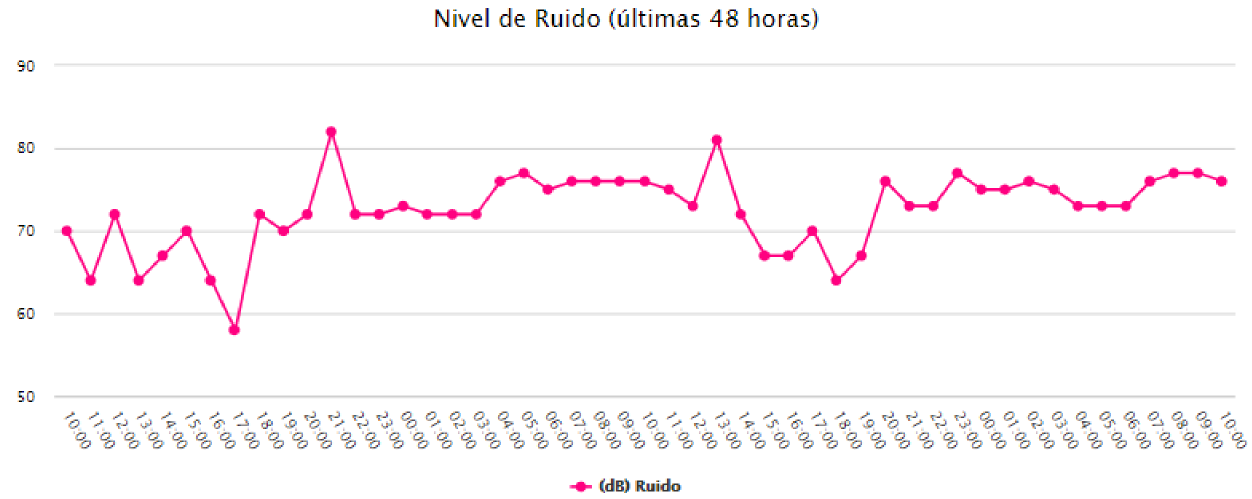


Figure 10. Noise level plot for the last 48 hours.

In addition to the environmental data, the Use Case 1 provides estimations on the number of visitors. Figure 11 shows the identified number of devices with active Wi-Fi connection during the last 48 hours.

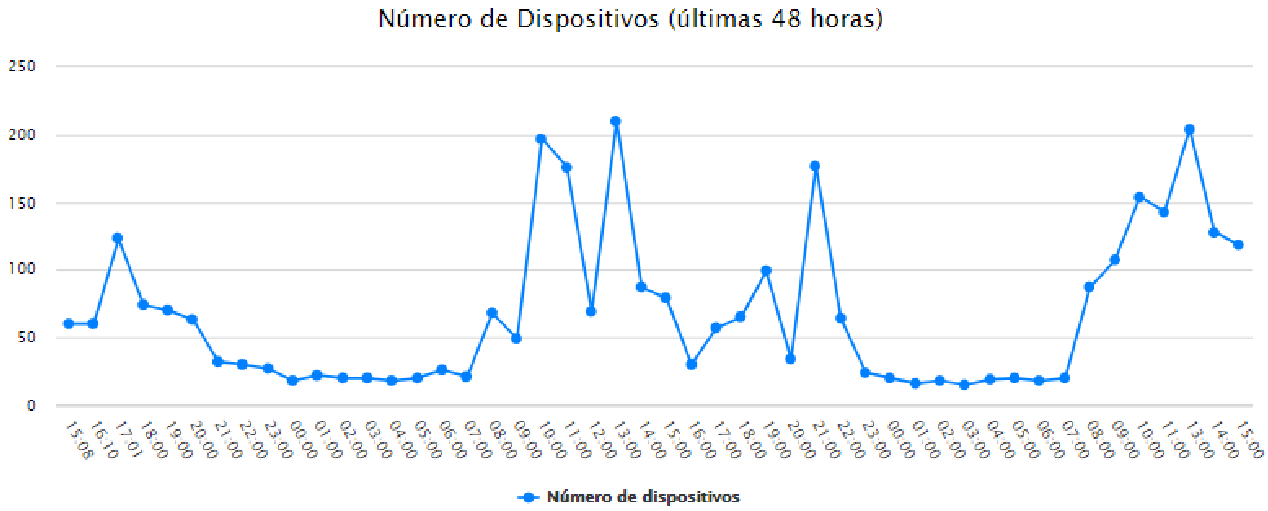


Figure 11. Number of devices with active Wi-Fi connection as an estimation of the number of visitors in the last 48 hours.

3) **Scalability**. The provided IoT solution can be up scaled to adapt to other scenarios and can be easily integrated with existing infrastructures and future implementations.

4) Privacy. The mobile devices IDs (MAC) of end-users interacting with the city spots where the pilot is carried out are anonymized. Besides, the Park Guide web application protects the privacy of end-user, propose several levels of management of personal data, and give the option of modifying the privacy parameters any time.

Interaction diagram

The expected interactions in this use case will focus on the ones happening among the IoT devices designed by TST to keep track of environmental measurements and provide a figure related to the number of people gathering in selected spots. The analysis of potential attacks to these devices will be carried out through the Honeypot (IoTPOT), as depicted in Figure 12 below:

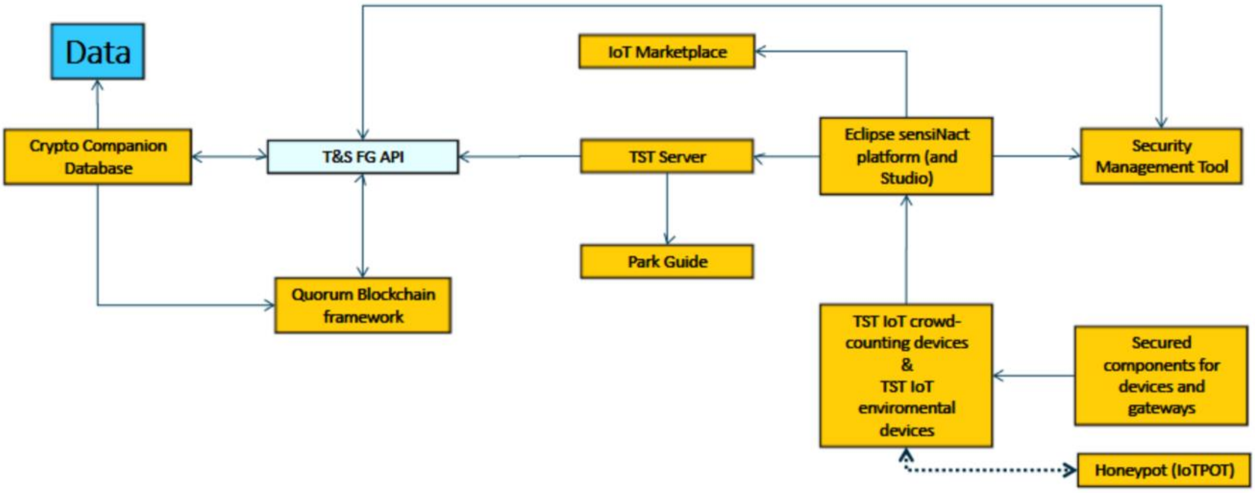

Data
Crypto Companion Database
T&S FG API
Quorum Blockchain framework
IoT Marketplace
TST Server
Park Guide
Eclipse sensiNact platform (and Studio)
Security Management Tool
TST IoT crowd-counting devices & TST IoT enviromental devices
Secured components for devices and gateways
Honeypot (IoTPOT)

Figure 12. Interaction diagram of Use Case 1.

Use Case IRL matrix

All interaction points that are expected to take place between all the assets of the Use Case 1 can be seen in the Table 8 interaction matrix. It should be noted that, as the assets are duplicated in Vertically/Horizontally (the matrix is a symmetric one, as described in previous deliverable D2.5), only the fields above the diagonal up (or only the ones below it) must be taken care of.

Table 8. Interactions matrix of Use Case 1.

Use Case 1	Park guide	TST Server	IoT Marketplace	Eclipse sensiNact platform (and Studio)	Security Management Tool	TST IoT crowd-counting devices	TST IoT environmental devices	Secured components for devices and gateways	Quorum Blockchain framework	Honeypot (IoTPOT)	T&S FG API	Crypto Companion Database
Park Guide	9	9	0	0	0	0	0	0	0	0	0	0
TST Server	9	9	0	7	0	0	0	0	0	0	7	0
IoT Marketplace	0	0	9	5	0	0	0	0	0	0	0	0
Eclipse sensiNact platform (and Studio)	0	7	5	9	7	7	7	0	0	0	0	0
Security Management Tool	0	0	0	7	9	0	0	0	0	0	7	0
TST IoT crowd-counting devices	0	0	0	7	0	9	0	7	0	7	0	0
TST IoT environmental devices	0	0	0	7	0	0	9	7	0	7	0	0
Secured components for devices and gateways	0	0	0	0	0	7	7	9	0	0	0	0
Quorum Blockchain framework	0	0	0	0	0	0	0	0	9	0	0	0
Honeypot (IoTPOT)	0	0	0	0	0	7	7	0	0	9	0	0
T&S FG API	0	7	0	0	7	0	0	0	0	0	9	7
Crypto Companion Database	0	0	0	0	0	0	0	0	0	0	7	9

Use Case SRL table

Table 9 recaps the calculations performed to extract the Component SRL array for Use Case 1.

Table 9. System Readiness Level of Use Case 1.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Park Guide	7	2	126	1,56	0,78
TST Server	7	4	224	2,77	0,69
IoT Marketplace	9	2	116	1,43	0,72
Eclipse sensiNact platform (and Studio)	7	6	290	3,58	0,60
Security Management Tool	5	3	143	1,77	0,59
TST IoT crowd-counting devices	7	4	203	2,51	0,63
TST IoT environmental devices	7	4	203	2,51	0,63
Secured components for devices and gateways	6	3	152	1,88	0,63
Quorum Blockchain framework	7	1	63	0,78	0,78
Honeypot (IoTPOT)	7	3	161	1,99	0,66
T&S FG API	7	4	196	2,42	0,60
Crypto Companion Database	7	2	112	1,38	0,69

After doing the calculations, the Composite SRL for Use Case 1 is 0,67, which is translated to an SRL of level 3 – System Development & Demonstration.

3.2 Use Case 2

Short description for Use Case 2 and summary of requirements

Use Case 2, “Home monitoring & Wellbeing Tele-assistance for active and independent aging people”, is based in the Worldline’s asset dubbed Connected Care, a solution designed to improve quality of life of elderly people by offering services based on monitoring their home activity and helping them to live independently at home while offering security and peace of mind to their families.

With Connected Care, users are monitored and looked after using home sensor devices such as a smart plug, bed occupancy sensor, window/door open sensor, and motion sensor. All data generated by these sensors are collected and analysed on an ongoing basis by tele-operators of the tele-assistance company in charge of taking immediate action if necessary.

The main added value and the objective of the use case and its associated pilot is to ensure through the M-Sec platform a trusted environment concerning all the sensitive data collected by these devices and privacy protection.

Therefore, the two main goals of the use case that will be probed during the execution of the pilot will be:

- Improvement of quality of life of elderly people who live alone and are not familiar with the use of new technologies.
- Improvement of data security and integrity through the use of M-Sec assets in the different elements that compound the service. For example, components (sensors, cloud systems) involved in the data stream dissemination need to be tamper-proof to prevent malicious attacks on devices.

The Scenario specific requirements for this use case are the following:

- The system should let users collect information about their home activity (e.g., windows open sensor).
- The system should store massive information (such as temperature per second) in an efficient way, taking into account that not all data are expected to be recorded/stored forever.
- The system should store information (such as access to data) in a way that ensures this information will not be forgotten, and with mechanisms that allow third parties to verify that this information is correct and true.

The Security/Privacy specific requirements for this use case are the following:

- The system should have an access control policy, binding the users with different profiles, each with different access privileges to data (the owner of the data, a person assigned by them to consult their data –family member or professional-, software administrator, technical support, security officer, etc.)
- The system should have several policies of access to the data, depending on the role of the user and the data the user is trying to access to. Anonymous users should be given no access to any data related to users.
- The system should have a dashboard for matching roles to policies and privileges of access.
- The system should support an easy-to-use mechanism that enables the owner of the data to grant privileges of access to other users in an understandable way.

- The system should support mechanisms for authentication and authorisation of the users, including updates of the users' proofs of access privileges.
- The system should include security measures that protect data transmitted over the network at the application level against eavesdropping (encryption and peer authentication).

Interaction diagram

The integration diagram in Figure 13 shows how each asset interacts with the others and which role takes each one versus the others.

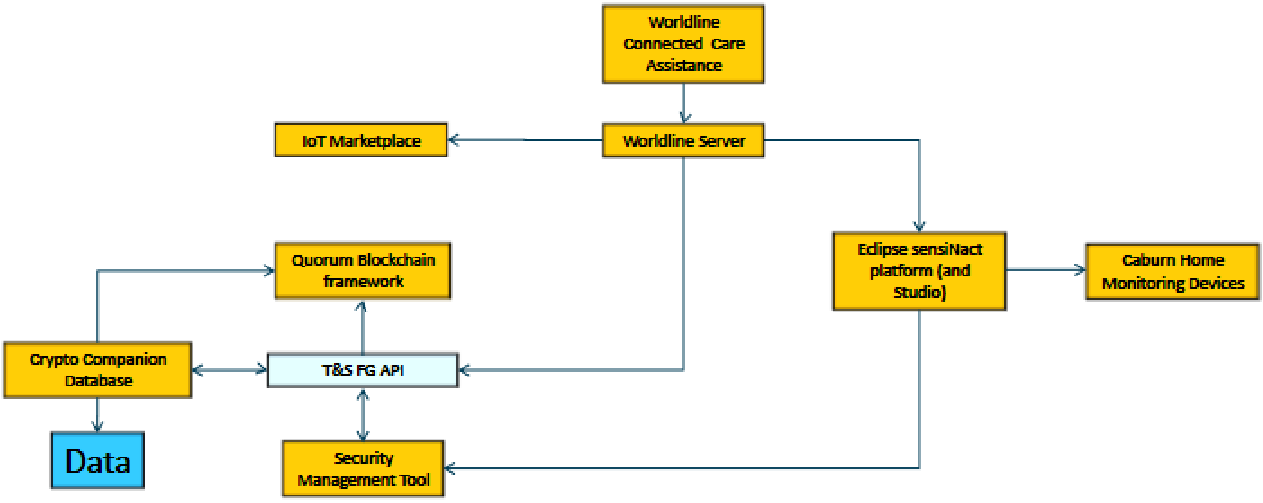

Worldline Connected Care Assistance
IoT Marketplace
Worldline Server
Quorum Blockchain framework
Eclipse sensiNact platform (and Studio)
Caburn Home Monitoring Devices
Crypto Companion Database
T&S FG API
Data
Security Management Tool

Figure 13. Interaction diagram of Use Case 2.

Use Case IRL matrix

In Table 10 all the interaction points between all the assets that the use case has can be seen. It should be noted that, as the assets are duplicated Vertically/Horizontally (the matrix is a symmetric one, as described deliverable D2.5), only the fields above the diagonal up (or only the ones below it) must be taken care of.

Table 10: Interactions matrix of Use Case 2.

Use Case 2	Worldline Connected Care Assistance	Worldline Server	IoT Marketplace	Eclipse sensiNact platform (and Studio)	Caburn Home Monitoring Devices	T&S FG API	Quorum Blockchain framework	Crypto Companion Database	Security Management Tool
Worldline Connected Care Assistance	9	9	0	0	0	0	0	0	0
Worldline Server	9	9	7	7	0	7	0	0	0
IoT Marketplace	0	7	9	0	0	0	0	0	0
Eclipse sensiNact platform (and Studio)	0	7	0	9	7	0	0	0	7
Caburn Home Monitoring Devices	0	0	0	7	9	0	0	0	0
T&S FG API	0	7	0	0	0	9	7	7	7
Quorum Blockchain framework	0	0	0	0	0	7	9	7	0
Crypto Companion Database	0	0	0	0	0	7	7	9	0
Security Management Tool	0	0	0	7	0	7	0	0	9

Use Case SRL table

Table 11 recaps the calculations performed to extract the Component SRL array for Use Case 2.

Table 11. System Readiness Level of Use Case 2.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Worldline Connected Care Assistance	7	2	126	1,56	0,78
Worldline Server	7	5	287	3,54	0,71
IoT Marketplace	9	2	130	1,60	0,80
Eclipse sensiNact platform (and Studio)	7	4	196	2,42	0,60
Caburn Home Monitoring Devices	7	2	112	1,38	0,69
T&S FG API	7	5	245	3,02	0,60
Quorum Blockchain framework	7	3	161	1,99	0,66
Crypto Companion Database	7	3	161	1,99	0,66
Security Management Tool	5	3	143	1,77	0,59

After doing the calculations, the Composite SRL for Use Case 2 is 0,364, which is mapped to an SRL of level 3 – System Development & Demonstration.

3.3 Use Case 3

Short description for Use Case 3 and summary of requirements

This use case enables a client application that allows urban environment monitoring entities (for example, local governments) to visualise spatially and temporarily dense environmental data. Using the application, the entities are enabled to serve their citizens with sophisticated environment monitoring better. In this scenario, an automotive sensing platform is used to generate real-time environmental sensor data streams from all over the city of Fujisawa, for example, leveraging hundred mobile sensing trucks.

This use case illustrates how the M-Sec platform secures such a mobile sensing platform.

The Scenario specific objectives/requirements are as follows:

- The system should collect environment sensor data.
- The system should be able to handle many data streams concurrently.
- The system should be able to transfer the data streams in real-time.
- The Security/Privacy specific requirements for this use case are the following:
    - The system needs to secure the heterogeneous components involved in the data stream dissemination, so that they are not hacked by malicious attackers.
    - The system needs to secure the data streams so that the data is not tampered in the network between their source and destination.
    - The system should protect the data streams from malicious attackers at the edge and distributed cloud platform.
    - The system should disseminate the environment data stream to citizens securely.
    - The system should not harm citizens' privacy; thus, an automated privacy protection mechanism should be provided.
    - The system should grant access only to those with valid access rights.

Interaction diagram

The integration diagram in Figure 14 shows how each asset interacts with others and which role takes each one versus the others.

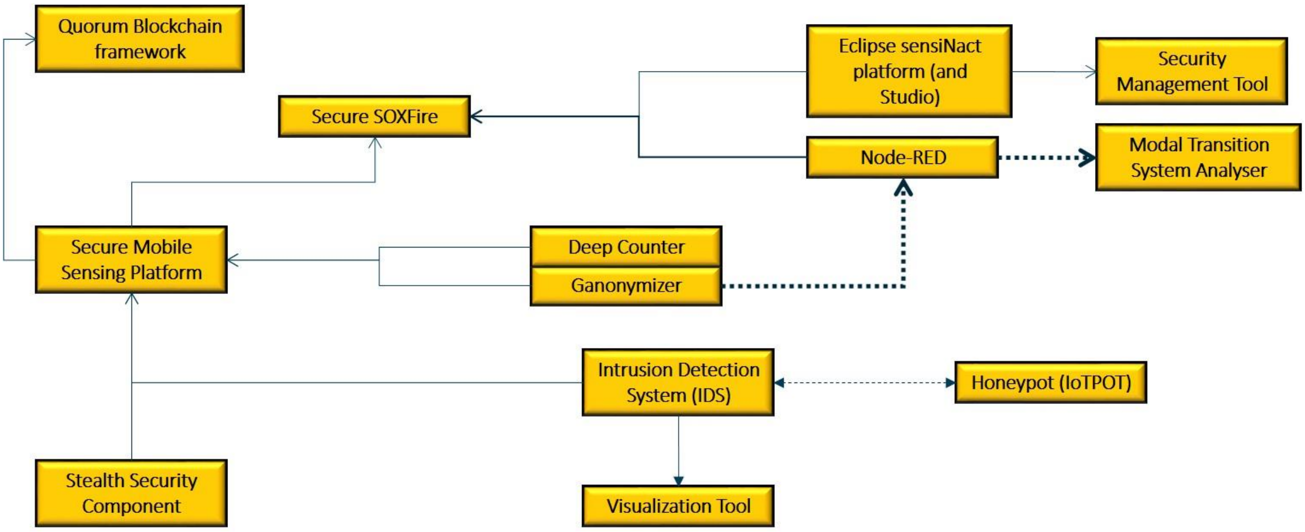

Quorum Blockchain framework
Eclipse sensiNact platform (and Studio)
Security Management Tool
Secure SOXFire
Node-RED
Modal Transition System Analyser
Secure Mobile Sensing Platform
Deep Counter
Ganonymizer
Intrusion Detection System (IDS)
Honeypot (IoTPOT)
Stealth Security Component
Visualization Tool

Figure 14: Interaction diagram of Use Case 3

Use Case IRL matrix

In Table 12 interaction matrix, can be seen all the interaction points between the assets that are expected to take place in the different stages of Use Case 3. It should be noted that, as the assets are duplicated in Vertically/Horizontally (the matrix is a symmetric one, as described in deliverable D2.5), only the fields above the diagonal up (or only the ones below it) have to be taken care of.

Table 12: Interactions matrix of Use Case 3

Use Case 3	Secure SOXFire	Eclipse sensiNact platform (and Studio)	Node-RED	Modal Transition System Analyser (MTSA)	Security Management Tool	Visualization Tool	Deep Counter (Garbage Identification AI)	Secure Mobile Sensing Platform	Quorum Blockchain framework	Ganonymizer	Intrusion Detection System (IDS)	Honeypot (IoTPOT)	Stealth Security Component
Secure SOXFire	9	0	7	7	0	0	7	7	0	0	0	0	0
Eclipse sensiNact platform (and Studio)	0	9	0	0	7	0	0	0	0	0	0	0	0
Node-RED	7	0	9	7	0	0	0	0	0	7	0	0	0
Modal Transition System Analyser (MTSA)	7	0	7	9	0	0	0	0	0	0	0	0	0
Security Management Tool	0	7	0	0	9	0	0	0	0	0	0	0	0
Visualization Tool	0	0	0	0	0	9	0	0	0	0	7	0	0
Deep Counter (Garbage Identification AI)	7	0	0	0	0	0	9	7	0	0	0	0	0
Secure Mobile Sensing Platform	7	0	0	0	0	0	7	9	0	7	0	0	5
Quorum Blockchain framework	0	0	0	0	0	0	0	0	9	0	0	0	0
Ganonymizer	0	0	7	0	0	0	0	7	0	9	0	0	0
Intrusion Detection System (IDS)	0	0	0	0	0	7	0	0	0	0	9	9	0
Honeypot (IoTPOT)	0	0	0	0	0	0	0	0	0	0	9	9	0
Stealth Security Component	0	0	0	0	0	0	0	5	0	0	0	0	9

Use Case SRL table

Table 13 recaps the calculations performed to extract the Component SRL array for Use Case 3.

Table 13. System Readiness Level of Use Case 3.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Secure SOXFire	6	5	250	3,09	0,62
Eclipse sensiNact platform (and Studio)	7	2	98	1,21	0,60
Node-RED	9	4	221	2,73	0,68
Modal Transition System Analyser (MTSA)	7	3	168	2,07	0,69
Security Management Tool	5	2	94	1,16	0,58
Visualization Tool	6	2	103	1,27	0,64
Deep Counter (Garbage Identification AI)	6	3	138	1,70	0,57
Secure Mobile Sensing Platform	6	5	212	2,62	0,52
Quorum Blockchain framework	7	1	63	0,78	0,78
Ganonymizer	7	3	168	2,07	0,69
Intrusion Detection System (IDS)	7	3	168	2,07	0,69
Honeypot (IoTPOT)	7	2	126	1,56	0,78
Stealth Security Component	5	2	75	0,93	0,46

After doing the calculations, the Composite SRL for Use Case 3 is 0,64, which is translated to an SRL of level 3 – System Development & Demonstration.

3.4 Use Case 4

Short description for Use Case 4 and summary of requirements

In this use case, "Hyper-connected citizen care applications" will be created for a range of different purposes and for different stakeholders. On one hand, a government officers' application will collect city-related data (such as urban waste generation per household, pedestrian flow or traffic flow data, etc.) through the M-Sec architecture and analyse the data to produce value-added data that affect citizens efficiently. Citizens' applications, on the other hand, will consume that value-added data to empower their decision on related topics towards better (physical, mental, or social) wellbeing or Quality of Life (QoL).

The Scenario specific requirements for this use case are the following:

- The system should collect heterogeneous data on citizens' life in real time.
- The system should be able to handle many data streams concurrently.
- The system should be able to transfer the data stream in real time.
- The local architecture should be scalable and can be integrated with others.
- Deployed devices will not impact negatively in the scenario nor affect the daily operations as they are before their deployment.
- The associated web application should provide and visualise environment information collected over the city.
- The application should provide a tool to analyse data and extract statistics in a simple and easily understandable way for the city environment division and citizens.
- The Security/Privacy specific requirements for this use case are the following:

- The system needs to secure the heterogeneous components involved in the data stream dissemination so that they are not hacked by malicious attackers.
- The system needs to secure the data streams, so that the data is not tempered in the network between their source and destination.
- The system should not harm citizens' privacy; thus, an automated privacy protection mechanism should be provided.
- The system should disseminate the data stream to municipalities and citizens securely
- The system should protect the data streams from malicious attackers at the edge and distributed cloud platform.
- The system should grant accesses from whom own a valid access right.
- The cloud system should store the data securely so that they are not disclosed to any party without permission.

Interaction diagram

The integration diagram in Figure 155 shows how each asset interacts with others and which role takes each one versus the others.

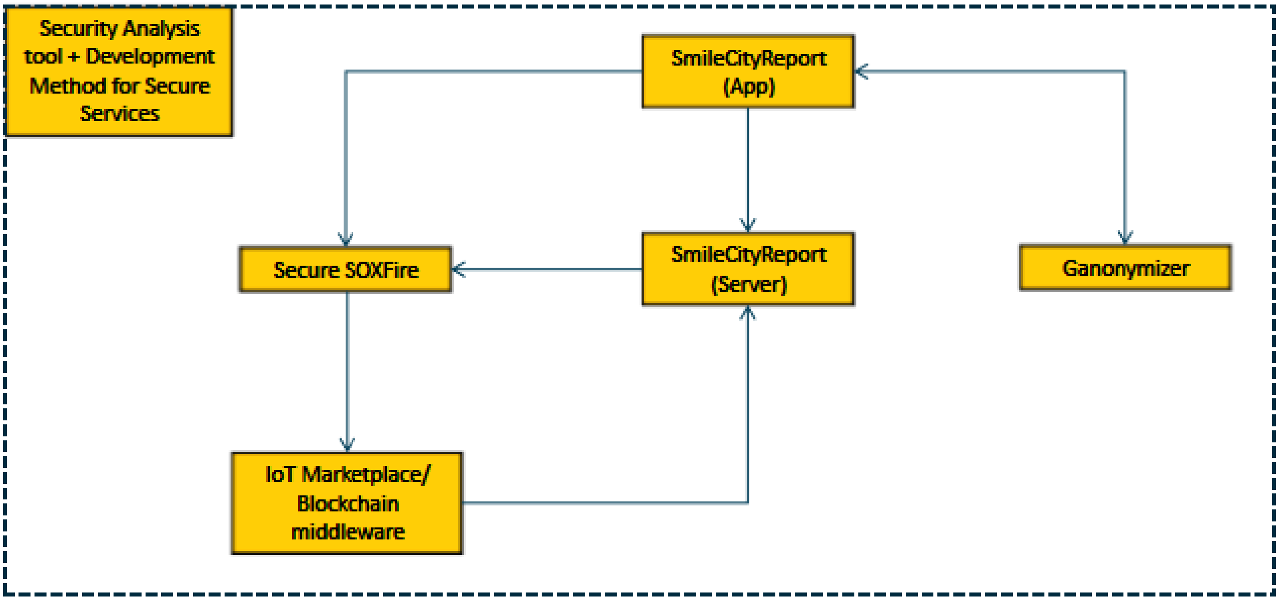

Security Analysis tool + Development Method for Secure Services
SmileCityReport (App)
Secure SOXFire
SmileCityReport (Server)
Ganonymizer
IoT Marketplace/ Blockchain middleware

Figure 15: Interaction diagram of Use Case 4

Use Case IRL matrix

In Table 14 all the interaction points between the assets that are expected to take place in the different stages of Use Case 4 can be seen.

Table 14: Interactions matrix of Use Case 4

Use Case 4	SmileCityReport (App)	SmileCityReport (Server)	Ganonymizer	Secure SOXFire	Security Management Tool	IoT Marketplace	Security Analysis tool + Development Method for secure Services
SmileCityReport (App)	9	9	7	7	0	5	0
SmileCityReport (Server)	9	9	0	7	0	5	0
Ganonymizer	7	0	9	0	0	0	0
Secure SOXFire	7	7	0	9	0	5	0
Security Management Tool	0	0	0	0	9	0	0
IoT Marketplace	5	5	0	5	0	9	0
Security Analysis tool + Development Method for secure Services	0	0	0	0	0	0	9

Use Case SRL table

Table 15 recaps the calculations performed to extract the Component SRL array for Use Case 4.

Table 15. System Readiness Level of Use Case 4.2.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
SmileCityReport (App)	8	5	280	3,46	0,69
SmileCityReport (Server)	8	4	231	2,85	0,71
Ganonymizer	7	2	119	1,47	0,73
Secure SOXFire	6	4	211	2,60	0,65
Security Management Tool	5	1	45	0,56	0,56
IoT Marketplace	9	4	191	2,36	0,59
Security Analysis tool + Development Method for secure Services	4	1	36	0,44	0,44

After doing the calculations, the Composite SRL for Use Case 4 is 0,63, which is translated to an SRL of level 3 – System Development & Demonstration.

3.5 Use Case 5

Short description for Use Case 5 and summary of requirements

This use case focuses on creating a marketplace to distribute data while ensuring confidentiality, integrity, availability, and privacy of data following GDPR/PIPA regulations so that people or organizations in EU and Japan can utilize the data more securely and effectively. Data to be exchanged in the marketplace are:

- Data from citizens and visitors: Purchase data, health data collected by pedometers, personal data collected by smartphones, data collected by questionnaires.
- Local government data: Statistic data, local information such as photos or reports collected by city staff.
- Web data: Any data automatically collected from the internet (environmental data, etc.).
- IoT data: Data collected from IoT devices (cameras, etc.) owned by companies or local governments.

Requirements:

- The local architecture should be processed securely.
- The cloud system should store the data securely and could be accessed from EU and Japan.
- The devices should be used to collect user's data, such as behaviour characteristic data.

The marketplace will be secured by using Blockchain technology.

Interaction diagram

The integration diagram in Figure 16 shows how each asset interacts with others and which role takes each one versus the others.

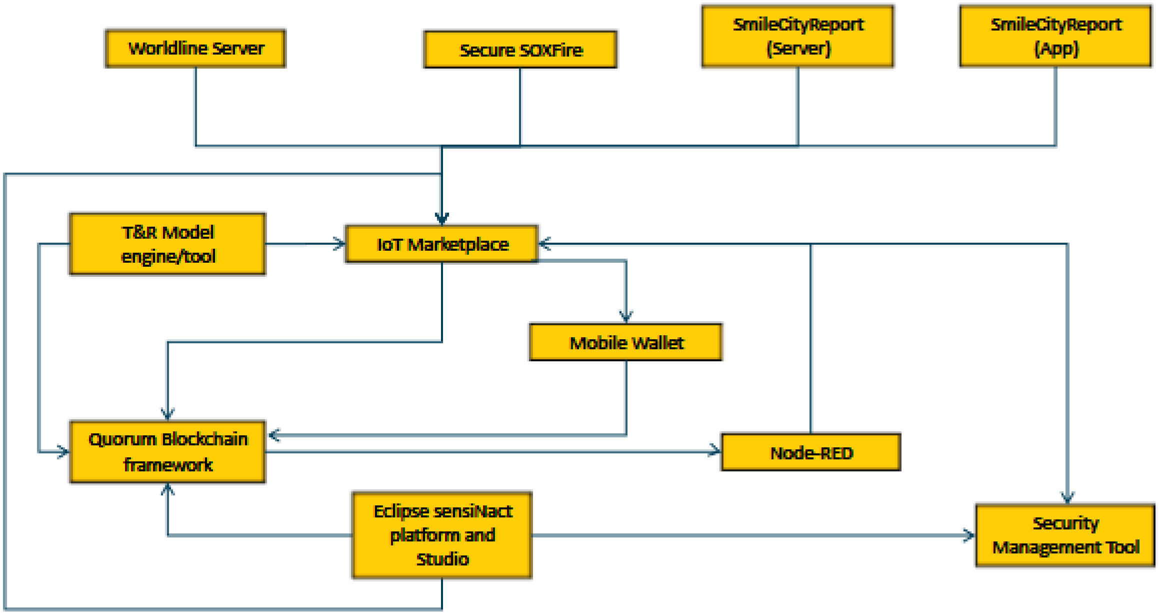


Figure 16: Interaction diagram of Use Case 5

Use Case IRL matrix

In Table 16 interaction matrix, can be seen all the interaction points between the assets that are expected to take place in the different stages of Use Case 3. It should be noted that, as the assets are duplicated in Vertically/Horizontally (the matrix is a symmetric one, as described in deliverable D2.5), only the fields above the diagonal up (or only the ones below it) must be taken care of.

Table 16: Interactions matrix of Use Case 5

Use Case 5	IoT Marketplace	Worldline Server	Secure SOXFire	SmileCityReport (App)	SmileCityReport (Server)	T&R Model engine/tool	Node-RED	Quorum Blockchain framework	Mobile Wallet	Eclipse sensiNact platform (and Studio)	Security Management Tool
Iot Marketplace	9	7	5	5	5	3	9	7	1	5	2
Worldline Server	7	9	0	0	0	0	0	0	0	0	0
Secure SOXFire	5	0	9	0	0	0	0	0	0	0	0
SmileCityReport (App)	5	0	0	9	0	0	0	0	0	0	0
SmileCityReport (Server)	5	0	0	0	9	0	0	0	0	0	0
T&R Model engine/tool	3	0	0	0	0	9	0	7	0	0	0
Node-RED	9	0	0	0	0	0	9	9	0	0	0
Quorum Blockchain framework	7	0	0	0	0	7	9	9	1	5	2
Mobile Wallet	1	0	0	0	0	0	0	1	9	0	0
Eclipse sensiNact platform (and Studio)	5	0	0	0	0	0	0	5	0	9	8
Security Management Tool	2	0	0	0	0	0	0	2	0	8	9

Use Case SRL table

Table 17 recaps the calculations performed to extract the Component SRL array for Use Case 5.

Table 17. System Readiness Level of Use Case 5.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Iot Marketplace	9	11	440	5,43	0,49
Worldline Server	7	2	126	1,56	0,78
Secure SOXFire	6	2	99	1,22	0,61
SmileCityReport (App)	8	2	117	1,44	0,72
SmileCityReport (Server)	8	2	117	1,44	0,72
T&R Model engine/tool	6	3	130	1,60	0,53
Node-RED	9	3	225	2,78	0,93
Quorum Blockchain framework	7	7	301	3,72	0,53
Mobile Wallet	7	3	79	0,98	0,33
Eclipse sensiNact platform (and Studio)	7	4	183	2,26	0,56
Security Management Tool	5	4	133	1,64	0,41

After doing the calculations, the Composite SRL for Use Case 5 is 0,60, which is translated to an SRL of level 3 – System Development & Demonstration.

4. Conclusions

The final release of the M-Sec platform has a good foundation. As shown in the document, the integrations between components have been performed and the majority are around 7, meaning that they are tested and working, and ready to be qualified in production alike environments.

All core assets are fully integrated and tested. Each pilot will start to be functioning in a production environment to fully test and validate the overall platform.

It should be noted that all the subsystems (Use Case ones) and the whole M-Sec system present a Composite SRL between 60% and 68% which corresponds to an SRL of level 3 – System Development & Demonstration. As stated in previous deliverables, for the project to be successful, it was planned for all subsystems and the whole system to reach a Composite SRL close to 70%, which is a typical level for successful Horizon 2020 projects, and it has been achieved and with some integrations already been improved it is expected to increase this percentage.