

D2.1



This project has received funding from Horizon 2020, European Union's Framework Programme for Research and Innovation, under grant agreement No.831138



Deliverable D2.1

Initial version of system requirements and architecture design

SCENE Project

Grant Agreement No. 831138

Call H2020-EIC-FTI-2018-2020 "Fast Track to Innovation"

Topic EIC-FTI-2018-2020– Fast Track to Innovation (FTI)

Start date of the project: 1 December 2018

Duration of the project:24 months

Disclaimer

This document contains material, which is the copyright of certain SCENE contractors, and may not be reproduced or copied without permission. All SECENE consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information. The reproduction of this document or of parts of it requires an agreement with the proprietor of that information. The document must be referenced if used in a publication.

The SCENE consortium consists of the following partners.

| No. | Name | Short Name | Country |
|-----|--|------------|---------|
| 1 | VISIONWARE - SISTEMAS DE INFORMAÇÃO, SA | VISIONWARE | PT |
| 2 | JCP-CONNECT SAS | JCP-C | FR |
| 3 | ALMAVIVA - THE ITALIAN INNOVATION COMPANY SPA | ALMAVIVA | IT |
| 4 | COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES | CEA | FR |
| 5 | AZIENDA METROPOLITANA TRASPORTI CATANIA SPA | CAT | IT |

Document Information

| | |
|--|--|
| Project short name and number | SCENE (AMD-831138-1) |
| Work package | WP2 |
| Number | D2.1 |
| Title | Initial version of system requirements and architecture design |
| Version | V1 |
| Responsible partner | VISIONWARE |
| Type¹ | R |
| Dissemination level² | PU |
| Contractual date of delivery | 28.02.2019 |
| Last update | 07.03.2019 |

¹**Types.R:** Document, report (excluding the periodic and final reports); **DEM:** Demonstrator, pilot, prototype, plan designs; **DEC:** Websites, patents filing, press & media actions, videos, etc.; **OTHER:** Software, technical diagram, etc.

²**Dissemination levels.PU:** Public, fully open, e.g. web; **CO:** Confidential, restricted under conditions set out in Model Grant Agreement; **CI:** Classified, information as referred to in Commission Decision 2001/844/EC.

Document History

| Version | Date | Status | Authors, Reviewers | Description |
|----------------|-------------|---------------|-------------------------------|--|
| v0.1 | 14.02.2019 | Draft | JCP, JCP | Initial version, definition of a structure |
| V0.2 | 01.03.2019 | Draft | JCP, ALM, CEA, VIS | Completion and correction of the document from 14.02 till 1.03 |
| V0.3 | 06.03.2019 | Draft | ALM, CEA, VIS, JCP | review |
| V0.4 | 06.03.2019 | Draft | JCP | Implementation of review comments |
| V1.0 | 07.03.2019 | Final | VIS | Final Review |

Acronyms and Abbreviations

| Acronym/Abbreviation | Description |
|-----------------------------|---|
| API | Application Programming Interface |
| BOM | Bill Of Material |
| GUI | Graphical User Interface |
| IGW | Intelligent Gateway |
| IoT | Internet of Things |
| KPI | Key Performance Indicators |
| LoRa | Long Range |
| PM | Person Month |
| PMC | Project Management Committee |
| QoE | Quality of Experience |
| SCENE | Smart City on the Edge Network Enhancements |
| SP | Service Platform |
| UI | User Interface |
| UC | Use Case |
| VQM | Video Quality Metric |

Contents

- 1 INTRODUCTION8
- 2 TERMINOLOGY 10
- 3 USE CASES 12
 - 3.1 Use case 1: Monitoring Critical Infrastructures and Buildings 12
 - 3.1.1 The problem to be addressed 12
 - 3.1.2 The proposed Use Case 12
 - 3.2 Use case 2: Monitoring High capacity sensors in the city 13
 - 3.2.1 The problem to be addressed 13
 - 3.2.2 The proposed Use Case 14
 - 3.3 Use case 3: Double parking in city environments 14
 - 3.3.1 The problem to be addressed 14
 - 3.3.2 The proposed Use Case 15
 - 3.4 Use case 4: Content delivery 16
 - 3.4.1 The problem to be addressed 16
 - 3.4.2 The proposed Use Case 16
- 4 REQUIREMENTS 17
 - 4.1 Business requirements 17
 - 4.2 General Requirements 17
 - 4.3 Use Cases Requirements 18
 - 4.4 System Requirements 21
 - 4.4.1 General Platform Requirements 21
 - 4.4.2 Service Platform Requirements 22
 - 4.4.3 Dashboard Requirements 24
 - 4.5 Intelligent Gateway Requirements 25
- 5 VERIFICATION METHODS 28
 - 5.1 Modules validation 28
 - 5.2 Pre-qualification 28
 - 5.3 Usage testing (pilots and field tests) 28
- 6 KEY PERFORMANCE INDICATORS 29
- 7 PRELIMINARY SYSTEM Architecture 31



D2.1

| | | |
|-----|--------------------------------------|----|
| 7.1 | Preliminary System Architecture..... | 31 |
| 8 | CONCLUSION..... | 33 |

1 INTRODUCTION

Security, utility management (water, electricity, etc.), transportation, smart communities, smart cities and many other sectors are influenced by the technology evolution in data analytics and its various interesting applications. However, the availability of data itself in real-time is dependent on the communication technology and its underlying infrastructure.

To overcome the challenge of high initial investment in traditional communication systems that allows to collect data for smart environments (cities, communities, groups, services, etc.) the Internet of Things (IoT) is introduced as a low-cost solution. The low cost of sensors and the wide variety of supported applications encouraged the adoption of the technology in several cases.

Collecting and processing secured data in real-time is a major challenge, but not the only one. Data analysis and consequential response reactions - which varies from simple signalling up to huge content delivery - are other major challenges that need processing power for analytics and transmission bandwidth for potential content. In many cases the response reaction may involve configuration setup, documents/multimedia transmission, etc. that might be beyond the capacity of the used IoT systems, and as a result complementary systems/implementations should be deployed to perform this transmission tasks.

SCENE (Smart City on the Edge Network Enhancement) is proposing an integrated solution based on vehicular networks for a secured environment that securely collects, and processes sensor data based on IoT technologies. This data is transmitted centrally to be analysed and processed by smart-city applications. On the other direction, the system also supports a content delivery platform that deploys suitable protocol stack for secured content delivery. With this functionality, SCENE is building an integrated security system for both IoT based data collection as well as multimedia secured content delivery. The content delivery platform is intelligent enough to be deployed in both IoT mode and in the stand-alone mode to deliver contents to subscribed smart applications.

This deliverable presents the Use Cases that will guide the definition of the system. The derived Pilots will constitute the test bench for the validation of the SCENE Platform (to be implemented in WP6).

Further to the validation Pilots, additional demonstration Field Tests will be defined and conducted in the cities targeted by the final Platform. Additional cities will be potentially added during the project. These tests will each show a specific use case of SCENE. The goal will be to assess users and stakeholders experience (smart cities, IoT service provider). The results of these tests are crucial to prove that the innovations that will be introduced by the SCENE platform have a great and valuable commercial potential.



D2.1

The first 3 Use Cases introduced in this document address a possible user need that can be solved by using an IoT solution. The 4th use case presented is a typical scenario of a content delivery systems. The SCENE Platform will be designed and implemented such that content delivery and IoT functionalities can be activated either separately, or together. The requirements that follow are consequently targeting either of the 2 functionalities.

This document also presents the initial version of the Requirements of the project and a general architecture of the SCENE Platform in functional modules. This initial schema will be further investigated and described in a following Deliverable, D2.2, in which the System Architecture at a higher level of detail will be presented.

2 TERMINOLOGY

The following definitions are considered crucial for the proper understanding of the rest of this document.

A “Requirement” is a singular documented physical and functional need that a particular design, product or process must be able to perform. It is a statement that identifies a necessary attribute, capability, characteristic, or quality of a system for it to have value and utility to a customer, organization, internal user, or other stakeholder.

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST" This word means that the item is an absolute requirement of this specification.

"MUST NOT" This phrase means that the item is an absolute prohibition of this specification.

"SHOULD" This means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.

D2.1



Figure 2.1 SCENE Data Flow Diagram

3 USE CASES

3.1 Use case 1: Monitoring Critical Infrastructures and Buildings

This section describes the ITALY Use Case (UC1) for testing the SCENE platform. Starting from the relevant problem to be addressed for AMT Catania, the UC is defined and described, including which data is to be collected. Type of sensors needed are also included in this document.

3.1.1 The problem to be addressed

The territory of the city of Catania and of its suburbs, a wide area, is affected by earthquakes, due to the presence of the Etna volcano. Further, the traffic – as for all the modern cities – has also a negative effect on roads, buildings, critical infrastructures, etc. Monitoring this wide area is a critical issue.

Urban and rural roads constitute a network system characterized by a wide extension in the territory, but monitoring road status and performance is very difficult, due essentially to high costs to equip the infrastructures with automatic monitoring systems, capable of measuring quantities, representative of the characteristics to be monitored and transferring relevant data.

Nowadays, monitoring is carried out using special vehicles, equipped with a series of detection systems, also with video cameras and image interpretation, which give a very detailed picture of the infrastructure status, especially with regards to the pavement, high costs are the most critical obstacle to this kind of approach, along with the impossibility of evaluating the structural components of road main body or infrastructure parts (viaducts, bridges, tunnels, etc.), which are critical parts of the infrastructure.

3.1.2 The proposed Use Case

The proposed ITALY Use Case is focused on the need to have an “intelligent” monitoring system of some specific parameters of urban infrastructures, both structural and functional, (e.g. useful to evaluate the effects of an earthquake on the usability of the infrastructure or to gather specific parameters on the state of the art of ancient and artistic buildings/monuments due to traffic vibrations, earthquake, etc.) A possible extension of use case for monitoring traffic with origin/destination and vehicle type detection may be evaluated.

Referring to the structural characteristics and taking into account the static nature of the road main body and of the other infrastructure parts, sensors should be essentially composed by accelerometers, which can measure displacements and vibrations for both buildings and infrastructures.

D2.1

Other types of sensors can be used to detect hidden cracks inside the pavement layers; in this case the sensors must be embedded in the road pavement (they can also be positioned during the reconstruction of the road surface, before laying the most superficial layers of the pavement, or, later, through drilling and overcoating).

As regards the functional characteristics, the irregularities of the road surface are generally measured with accelerometers mounted on board vehicles. Greater irregularities (holes, cracks), as well as the state of maintenance of the road markings, can also be detected through image interpretation techniques (possibly - in the city context - also exploiting cameras used to detect the parking lane occupancy).

The US Federal Highway Administration publishes a report about innovative pavement monitoring systems, mainly oriented to rural roads, which can give useful indications on the quantities to be detected in order to implement a road network monitoring system:

<https://www.fhwa.dot.gov/publications/research/infrastructure/pavements/12072/12072.pdf>

The same system could also be used to monitor the structural state of buildings, especially those that have less chance of being connected to the internet for their historical worth (churches, historic buildings and monuments). For this last type of implementation, it's necessary to verify the distance constraints between the road (where vehicles equipped with the gateway device pass) and the various points of the building where the sensors should be positioned.

Data gathered by sensors are sent through the wireless sensors network, installed on AMT Catania buses, to the IoT Platform for the suitable elaboration and the dispatching of the useful information to end-users (AMT, Public Administration, citizens, etc...).

3.2 Use case 2: Monitoring High capacity sensors in the city

This section describes the FRANCE Use Case (UC2) for testing the SCENE platform. Starting from the problem to be addressed according to discussions with Rennes Metropole and Turk Telecom.

3.2.1 The problem to be addressed

It is very expensive to deploy high capacity sensors all along the city especially in less dense and sub-urban areas. It is over-expensive to install dedicated infrastructure in these areas and current IoT networks are not always well dimensioned to handle the flow of data generated by these sensors. The types of situations which are detected by the sensors are real time or non-real-time situations.

D2.1

3.2.2 The proposed Use Case

The proposed use case concerns the possibility to use the bus (and taxis, cars) to collect the necessary information to detect real time and non-real time events triggering a high upstream flow of data.

The situations are detected by different sensors:

- camera in the bus, filming inside the bus: it takes pictures on a low rate as a basis and increases the resolution when an event requiring immediate action is detected;
- camera in the bus, filming the bus surrounding in the city: it takes pictures, in order to be able to identify the different “objects” or patterns with a sufficient resolution in order to recognise them (cars, trucks, people, etc.). The information is coupled with location information;
- fixed cameras: these cameras can be close to the bus line (a few tens of meters) or at a longer distance. (for short distances, BLE, or WIFI or Zigbee are used, for longer distance like up to 1 km, NB-IoT or others are used).

In the usual case, information is processed locally in the Intelligent Gateway and will be sent to the service platform whenever cheap connection (such as WiFi) is available. It may be that an immediate action is triggered either at the sensor level, or at the Intelligent Gateway level, or at the service platform level. If for instance an immediate action is triggered locally (sensor or Intelligent Gateway level), the Intelligent Gateway may decide to send the critical information on real time to the service platform via 4-5G network.

3.3 Use case 3: Double parking in city environments

This section describes the PORTUGAL Use Case (UC3) for testing the SCENE platform. Starting from the problem to be addressed, the UC is defined and described, including which data are to be collected.

3.3.1 The problem to be addressed

Double-parking is a problem in cities all around Europe, when cars use traffic lanes to park or for long stops. This hinders traffic, reduces visibility, and creates safety issues for both (other) drivers and pedestrians. Double parkers are hard to track for police forces due to the transient nature of the infraction and the need for oblivious law enforcement to take care of the more serious crimes.

Automatic monitoring of traffic infractions is done successfully across European cities in situations such as speeding and incursion into streets reserved for local inhabitants, so it is expected the

D2.1

system will be well accepted by the communities. The innovation of this system lies in the detection of a transient action which requires high capacity of processing.

Monitoring (and automatic fining) of double parkers can be used as a deterrent for drivers. By advertising the fact that double parking will not be tolerated and may lead to a traffic infraction without the presence of the municipal police, we believe drivers will restrain from this practice, using legal parking spots instead. In high density streets with insufficient parking spots, this will ultimately lead to the citizens using public transportation instead of their personal car, leading to less congested streets and a healthier environment.

3.3.2 The proposed Use Case

The proposed Use Case uses sensors and the gateway to report double parkers to authorities, who may then proceed to act on it.

Sensors placed in high places, such as light poles will detect a double parker, or any vehicle parked irregularly, on a traffic lane. Data, such as time, location, license plate number, and duration as well as photographic evidence, will be stored in the sensor and passed to the SCENE Gateway when a vehicle passes within range. The SCENE Network will then pass the information on to the proper authority for further action.

Photos will be carefully processed to protect the privacy of citizens, as displayed in the following example:



All processing will be done on the sensor, so the only data that is sent over the SCENE network are the two timestamped and georeferenced pictures. Final decision on whether to fine an infraction is always done by a human (law enforcement agent).

The sensor will communicate to the SCENE gateway over 802.11p, using MQTT to store & forward the data to a central application, operated by the city's law enforcement agency.

3.4 Use case 4: Content delivery

This section describes the Content Delivery Use Case (UC4) for testing the SCENE platform. Starting from the problem to be addressed, the UC is defined and described, including which data is to be collected.

3.4.1 The problem to be addressed

The proliferation of mobile devices and the development of alternative digital media platforms increase exponentially the consumption of digital contents, especially in the public transport when people commute to work or travel for leisure or business.

In areas where the network coverage is not satisfactory, users are cut from useful data regarding their travel, tourist information or local news.

3.4.2 The proposed Use Case

The proposed Use Case is based on the SCENE solution on the content delivery side, which JCP already prototyped. SCENE has in addition of its IoT function a content delivery functionality which uses the caching technology to preload contents and deliver them to users even when there is no available Wi-Fi connection. The solution can deliver two types of contents:

- Digital contents that have been prefetched on the cache according to users' interests;
- Digital contents that have been preloaded on a dedicated portal.

The idea of the use case is the following: when a vehicle on which the IGW is installed is moving, the IGW caches and preloads content according to i) the vehicle movement ii) the users' interests. Real time content download can of course be performed via 4G network but is expensive and not necessary as users consume many identical contents. SCENE system will act such a way that instead of interacting with Internet, the user will interact with the interactive gateway as content of interest to the user has been preloaded or cached already in the IGW.

2 main situations can exist:

1) users have some similar behavior i) between them ii) over time. This means that content can be downloaded in the IGW according to these 2 parameters.

2) the vehicles are moving towards predicted places in the case of public transport; in the more general case (which is not investigated here) the vehicle movement can be anticipated. This means that content can be pre-loaded in the next IGW to which the vehicle will connect to. Another fact is that when users initiate long streaming sessions, the average session time is in general order of magnitude higher than the time between 2 IGW access point.

The system will cache and prefetch content in the IGW within the bus so the the QoE of the user is maximized and the traffic in the 4-5G network is minimized.

4 REQUIREMENTS

This section presents the User Requirements and an initial set of System Requirements.

Both Functional and non-Functional (quality of service related) requirements are presented.

Requirements represent the foundation for the following phases of the project. Starting from them, the architecture of the system, both hardware and software, will be defined, and will be described in detail in the Deliverable D2.2.

4.1 Business requirements

| Id | Requirement | Remarks |
|------|---|--------------------------|
| BR.1 | SCENE MUST offer an affordable IOT Open platform for developing high security IOT Services | |
| BR.2 | SCENE MUST drop costs for deploying IOT infrastructures in Small Towns | |
| BR.3 | SCENE MUST support External Partners to produce IOT solution with smaller costs | |
| BR.4 | SCENE MUST offer services with highest security levels | |
| BR.5 | SCENE SHOULD integrate IoT services and Content Delivery Services | IoT and content delivery |
| BR.6 | IoT and content delivery services MUST be offered together on the same platform, or separately | |
| BR.7 | SCENE SHOULD offer an affordable Content Delivery System to allow Content Providers and/or Transport Operators to make available their content through SCENE platform | Content delivery |

4.2 General Requirements

| Id | Requirement | Remarks |
|------|---|---------|
| GR.1 | SCENE MUST be accessible by Users through Graphical User Interface (GUI) | |
| GR.2 | SCENE MUST be accessible by Users through an Interface layer based on Application Programming Interface (API) | |
| GR.3 | SCENE MUST have the capability to be interfaced with standard protocols and technologies | |
| GR.4 | SCENE MUST manage and control user access to the platform, both from GUI and API | |
| GR.5 | SCENE MUST guarantee Security and Data Protection | |

D2.1

| | | |
|-------|---|---|
| GR.6 | SCENE MUST collect and process IOT data as soon as they are provided by the sensors to the SCENE platform | |
| GR.7 | SCENE MUST persist and retain received IOT data according to timeframe required by user’s business case | |
| GR.8 | SCENE MUST provide IOT collected data to its Users (Public administration, citizens, companies, Smart City Service Providers, etc.) | |
| GR.9 | SCENE SHOULD enable simple automatic alarm or notification mechanisms on receiving IOT Data if specific conditions are verified | |
| GR.10 | SCENE MUST provide statistics and metrics about platform usage and activities | |
| GR.11 | SCENE SHOULD be able to receive from User configuration information to be sent to sensors | It will depend upon features and capabilities of sensors identified for UC implementation |
| GR.12 | SCENE MUST be able to receive and manage App-packages to be installed in the SCENE Edge module | |
| GR.13 | SCENE MUST be able to receive and manage information to be sent to App-packages installed on SCENE Edge module | |
| GR.11 | SCENE MUST be able to process separately IoT and content delivery services, or to integrate the 2 services together | |

4.3 Use Cases Requirements

Use Case 1 Requirements – City Infrastructures monitoring

| ID | Requirement | Remarks |
|--------|--|---------|
| UC1.01 | The system MUST collect measures of displacements and vibrations from sensors positioned on buildings and road infrastructures (bridges, viaducts, tunnels, retaining walls, etc.) | |
| UC1.02 | The measures MUST be persisted in the system for the required time period; the effective period length will be defined at business case refinement | |
| UC1.03 | Each persisted record MUST contain, besides the measure, also the sensor identifier and the related timestamp | |
| UC1.04 | In addition, each persisted record SHOULD contain the sensor position | |
| UC1.05 | The system SHOULD keep the list of monitored infrastructures; each infrastructure is identified by a unique identifier | |

D2.1

| | | |
|--------|---|---|
| UC1.06 | The system MUST keep the list of data owner customers (for example the external Smart City Services) where each customer is identified by a unique identifier. This identifier will be the key for the correct assignment of the stored data to the correct organization data owner | |
| UC1.07 | The system SHOULD enrich the persisted measures with additional attributes (for example sensor family, identifier of monitored infrastructure, identifier of the owner organization, city area, ...) that are required for analytic functions | Sensor data is configured at on-boarding time |
| UC1.08 | The system SHOULD detect, as soon as the data is processed, values of collected measures that could indicate critical situation | Thresholds will be defined in the specific use cases for critical value detection |
| UC1.09 | The system SHOULD notify the users in case of critical values detection | |
| UC1.10 | The system SHOULD be able to produce tables, reports and/or diagrams that report historical trends of collected measures based on time intervals, additional attributes etc. | |

Use Case 2 Requirements – High capacity sensor

| Id | Requirement | Remarks |
|--------|---|---|
| UC2.01 | System MUST guarantee anonymity unless a competent authority intervenes. | |
| UC2.02 | Sensors MUST capture evidences, e.g. in form of a photography | |
| UC2.03 | Sensor MUST collect hour, date and location | |
| UC2.04 | Information MUST be sent to the authorities in a useful time frame. | |
| UC2.05 | Sensors MUST be able to capture SD and HD related content | |
| UC2.06 | Sensors MUST have communication capabilities to support SD and HD content transmission | |
| UC2.07 | Sensors SHOULD be able to buffer information | Should be precise when the use case is more precise |
| UC2.08 | Sensors SHOULD detect defined pattern or sequences of patterns | |
| UC2.09 | Sensors MUST be able to securely and quickly communicate with the Intelligent Gateway when it's passing by | |
| UC2.10 | Sensors MUST be physically and digitally secure | |
| UC2.11 | Sensors MUST be able to work continuously or through batteries, respectively, when its location is fixed or temporary | |
| UC2.12 | Sensors SHOULD have the ability to be externally audited | |

Use Case 3 Requirements – Double Parking Control

| Id | Requirement | Remarks |
|--------|---|---------|
| UC3.01 | Sensors MUST be able to identify 2nd line parking, specifically the automobiles in those circumstances | |
| UC3.02 | Sensors MUST be able to distinguish 2nd line parking from other, considered regular as, for example, cars stopped due to traffic, cars correctly parked and moving cars | |
| UC3.03 | Sensors MUST be able to capture the evidence of an unusual event, in particular through a photography | |
| UC3.04 | Sensors MUST be able to capture the hour, date and must store a location (GPS or ID) | |
| UC3.05 | The evidence collected MUST be sent to the authorities in a useful time frame | |
| UC3.06 | The evidence collected MUST be exclusively related to the double-parking situation | |
| UC3.07 | The evidence collected SHOULD be available only for a short period of time | |
| UC3.08 | The evidence collect MUST have all non-essential elements obfuscated | |
| UC3.09 | The evidence collect MUST be retained for sufficient time to be confirmed at the destination | |
| UC3.10 | Sensors MUST have sufficient internal storage in order to keep the evidence until the passage of the Intelligent Gateway | |
| UC3.11 | Sensors MUST be able to securely and quickly communicate with the Intelligent Gateway when it's passing by | |
| UC3.12 | Sensors MUST be physically and digitally secure | |
| UC3.13 | Sensors MUST be able to work continuously or through batteries, respectively, when its location is fixed or temporary | |
| UC3.14 | Sensors SHOULD have the ability to be externally audited | |

Use Case 4 Requirements – Content Delivery

As there is only one generic use case defined for content delivery (by contrast with the 3 use cases defined for IoT), there is no need to detail content delivery requirements related to use case 4 specifically. In consequence, content delivery use case 4 requirements are in the different requirements pertaining to the system, SP, and IGW.

D2.1

4.4 System Requirements

In this section general initial System Requirements are presented.

4.4.1 General Platform Requirements

| Id | Requirement | Remarks |
|-------|---|------------------|
| SR.01 | SCENE Platform MUST implement a central module named “Service Platform” (SP) to collect IOT data from sensors and made available processed data to the Users and to manage the whole system | |
| SR.02 | SCENE MUST implement mobile “Intelligent Gateway” capabilities (IGW) to reach the edge for interacting with IOT sensors remotely and to bring computation to the edge | |
| SR.03 | SCENE MUST enable the usage of IOT sensors with low range wireless communication capabilities | |
| SR.04 | SCENE MUST manage a wide range of network protocols to be able to connect with a wide range of IOT sensors | |
| SR.05 | SCENE MUST offer advanced statistic functions over the collected data | |
| SR.06 | SCENE MUST provide a “Dashboard” GUI built on web technologies to interact, manage and control the platform | |
| SR.07 | SCENE MUST provide “Analytics” component in charge of process data and inferring different metrics | |
| SR.08 | SCENE MUST provide an “API interface”, built on standard protocols, to dialogue with the rest of the Platform (i.e. Intelligent Gateway, services and other components) and with External Systems | |
| SR.09 | SCENE MUST implement a solution that assure high security standards | |
| SR.10 | SCENE MUST implement mobile “Intelligent Gateway” capabilities (IGW) to reach the edge to provide content delivery to the user | Content delivery |
| SR.11 | The SCENE solution MUST distribute a WIFI signal and grant users equipped with mobile device access to the network | Content delivery |
| SR.12 | User MUST have the possibility to login on the SCENE system to gain Internet access by using credentials | Content delivery |
| SR.13 | The SCENE platform MUST respect requirements of GDPR if applicable | |

D2.1

4.4.2 Service Platform Requirements

| Id | Requirement | Remarks |
|-------|---|---------|
| SP.01 | Service Platform MUST be able to ingest IoT sensor data from IGW | |
| SP.02 | Service Platform MUST be able to process ingested data applying filtering, enrichment, aggregation and analytics functions | |
| SP.03 | Service Platform MUST be able to send to all IGWs gateway configuration data | |
| SP.04 | Service Platform MUST be able to send to all IGWs sensor configuration data | |
| SP.05 | Service Platform MUST be able to send to all IGWs App-packages to be installed on the gateways | |
| SP.06 | Service Platform MUST be able to send to all IGWs App-packages configuration data | |
| SP.07 | Service Platform MUST be able to receive IGW-related telemetry data from IGWs | |
| SP.08 | Service Platform must be able to receive sensor-related telemetry data from IGWs | |
| SP.09 | Service Platform MUST be able to receive sensors status data | |
| SP.10 | Service Platform MUST be able to receive IGW status data | |
| SP.11 | Service Platform MUST be able to receive configuration data from Customers for IGW APPs | |
| SP.12 | Service Platform MUST be able to receive App-packages from External Partners to be sent to IGWs | |
| SP.13 | Service Platform MUST persist all data received in a data layer according to retention policies configuration | |
| SP.14 | Service Platform MUST produce statistics on data persisted in the data layer | |
| SP.15 | Service Platform MUST provide an API layer for interfacing with IGW | |
| SP.16 | Service Platform MUST provide an API layer for interfacing with Customers | |
| SP.17 | Service Platform MUST provide an API layer for interfacing with Dashboard | |
| SP.18 | Service Platform MUST provide an API layer for interfacing with Other management modules | |
| SP.19 | Service Platform MUST provide Analytics modules that allow analysis on the data persisted in the Data Layer module | |
| SP.20 | Service Platform MUST provide Analytics features which enable alerting and user notification on pre-defined case (deviation, thresholds etc.) detection | |
| SP.21 | Service Platform MUST persist all the data related to the service platform monitoring (for example logins of users, successful and wrong API calls, dimension of messages, ...) | |

D2.1

| | | |
|-------|--|--|
| SP.22 | Analytics module SHOULD support interactive analytics, near real-time analytics and batch analytics | |
| SP.23 | Service Platform SHOULD allow to schedule pre-defined jobs both for operational task and batch analytics processing | |
| SP.24 | Service Platform MUST provide capabilities to manage User configuration for identification and access management in SCENE platform | |
| SP.25 | Service Platform MUST interconnect with IGW and retrieve cache related information | |
| SP.26 | Service Platform MUST manage IGW caches using standard protocols | |
| SP.27 | Service Platform MUST deliver an API to content providers to manage caching and prefetching in IGWs | |

4.4.2.1 Non-functional requirements

| Id | Requirement | Remarks |
|--------|--|---------|
| SPN.01 | Service Platform MUST implement scalability features in order to foster the performance on transactions processed and response time on events, according with the performance KPI of the system | |
| SPN.02 | Service Platform SHOULD have capabilities to offer High Availability services | |
| SPN.03 | Service Platform MUST adopt security mechanisms to ensure respectively: <ul style="list-style-type: none"> • secure communication between internal components of Service Platform • secure communication between SP and external systems and to prevent: <ul style="list-style-type: none"> ○ unauthorised access of data (confidentiality) ○ unauthorised handling of data (integrity) ○ denial of service (availability) | |
| SPN.04 | Service Platform MUST implement vertical and horizontal scalability | |

D2.1

4.4.3 Dashboard Requirements

| Id | Requirement | Remarks |
|-------|---|---|
| DR.01 | Dashboard MUST be implemented as a web user interface to manage all SCENE platform components | |
| DR.02 | Dashboard MUST consent access only after sign-in with credentials and give the possibility to “Sign out” by clicking on the related button | |
| DR.03 | Dashboard MUST give access to dashboard functions and data based on specific User Roles the logged-in user belongs to | |
| DR.04 | Dashboard MUST display on all pages the Username and User Role | |
| DR.05 | Dashboard MUST allow user to access only to owned data | Data segregation in multi-entity context |
| DR.06 | User MUST be univocally identified through a unique user identifier | |
| DR.07 | Each access to the system via Web UI MUST be registered and logged. Even any attempt failed MUST be registered on the system with the necessary information to identify the origin of those accesses | |
| DR.08 | Each action performed by the user on the system via Web UI SHOULD be traced and logged | |
| DR.09 | Dashboard SHOULD have multi-language capability and give the possibility to select a language in the Login Form choosing among: English, Portuguese, French and Italian, clicking on the related flag | Predefined language will be associated to registered user |
| DR.10 | Dashboard SHOULD have GUI for Sensors Management | |
| DR.11 | Dashboard SHOULD allow configuration and setup of Sensors with their sensor identification attributes and geo-localisation information | Attributes can include type of device, device id, manufacturer etc.. |
| DR.12 | Dashboard SHOULD provide capabilities that allow to display sensors map | |
| DR.13 | Dashboard MUST provide GUI for User Management | |
| DR.14 | Dashboard MUST provide GUI for Customers (External Smart City Providers) management functions (registration, modification, etc..) | Registration of external provider entity in order to enable data and function segregation |
| DR.15 | Dashboard SHOULD provide GUI for IGW Management | Content management and IoT |
| DR.16 | Dashboard MUST provide GUI for Analytics functionalities | |
| DR.17 | Analytics dashboard SHOULD provide interactive features for ad-hoc data inquiring | |
| DR.18 | Analytics dashboard SHOULD provide features for graphical representation of calculated metrics | |

D2.1

| | | |
|-------|--|--|
| DR.19 | Analytics dashboard MUST provide capabilities for data drill-downs on data lake | |
| DR.20 | Analytics dashboard SHOULD enable users to save and share queries results | |
| DR.21 | Analytics dashboard SHOULD enable users to export results in a variety of formats such as excel, pdf, csv | |

4.4.3.1 Non-functional requirements

| ID | Requirement | Remarks |
|------------|---|---------|
| DRN.0 1 | Web UI MUST adhere to best-practice usability criteria (clear, homogeneous, simple, consistent, WYSIWYG) | |
| DRN.0 2 | Web UI MUST interact with Service Platform through API interface layer | |
| DRN.0 3 | Web UI MUST be designed and optimized for desktop user experience | |
| DRN.0 4 | Web UI MUST be implemented accordingly with the adopted security paradigm | |
| DRN.0 5 | The communication between Web UI and Service Platform MUST be secured with suitable mechanisms and protocols | |

4.5 Intelligent Gateway Requirements

| Id | Requirement | Remarks |
|--------|--|---|
| IGW.01 | Intelligent Gateway (IGW) MUST have an independent capability to connect to Internet for IoT part (for instance 4G interface) | Independent connection to Internet for IoT |
| IGW.02 | The IGW MUST integrate content delivery and IoT functionalities in one box | Independent connection to Internet for IoT |
| IGW.03 | The IGW MUST integrate content delivery and IoT functionalities in one box | NB: we'll have to see according to BOM requirement and customer requirement what the options are. |
| IGW.04 | The IGW MUST be able to host applications | Must be defined whether this should be virtualized, or container based |
| IGW.05 | The IGW MUST perform caching both for content delivery and IoT sensor communication | |
| IGW.06 | The IGW MUST manage communications with different sensors families/ coming from different external providers with full-service separation | |

D2.1

| | | |
|--------|--|--|
| IGW.07 | The IGW MUST send user requests to the Service Platform | SP (content delivery side) has to be aware of the content requested by the user to take caching/prefetching decisions |
| IGW.08 | The IGWs MUST send cache status information both for content delivery and IoT data | |
| IGW.09 | The IGWs MUST collect information from sensors on a synchronized way | Gateway are moving and sensors are fixed usually so the gateways must synchronize about the information to process; also, the applications have to be downloaded taking into account gateways mobility |
| IGW.10 | IGW MUST be able to prefetch content locally | Based on the SP (content delivery side) information, IGW must be able to download content on its local storage to fulfill potential future requests () from user. |
| IGW.11 | The IGW MUST communicate with the Service Platform to transmit content delivery related information (cache, topology,..) | SP (content delivery side |
| IGW.12 | The IGW MUST communicate with the Service Platform (IOT side) to transmit and receive IoT related information (cache, status, ...) | |
| IGW.13 | The IGW MUST have Ethernet Interface for Internet network connection | |
| IGW.14 | The IGW MUST have Wi-Fi Interface for Internet network connection | |
| IGW.15 | The IGW SHOULD have 4G Interface for Internet network connection | |
| IGW.16 | Secure application download MUST be possible | |
| IGW.17 | Application handover SHOULD be possible | Exact requirement has to be checked during the project life |
| IGW.18 | The IGW MUST collect sensors information via LoRA | |
| IGW.19 | The IGW MUST collect sensors information via WIFI | |

D2.1

| | | |
|--------|---|-----------------------------------|
| IGW.20 | The IGW MUST collect sensors information via 4/5G IoT | |
| IGW.21 | The IGW MUST ensure secure communication with sensors | |
| IGW.22 | The IGW MUST collect sensors information via BLE | |
| IGW.23 | The IGW MUST be manageable by the dashboard using standard interfaces | Define API and standard protocols |
| IGW.24 | a GUI SHOULD be available locally and on the service platform for management and configuration of the Gateway | |
| IGW.25 | Management of sensors SHOULD be possibly offloaded from the Service platform to the gateway | |
| IGW.26 | Any local change of configuration SHOULD be reflected to the service platform | |
| IGW.27 | The IGW MUST have a wifi AP capability to distribute content | |
| IGW.28 | The IGW SHOULD have a 4G client interface to communicate IoT information on real time to the SP | |
| IGW.29 | The IGW SHOULD have a 4G client interface to receive and transmit content. | Content delivery |
| IGW.30 | SCENE Intelligent Gateways MUST be able to connect to fixed Wi-Fi network transparently | Content delivery |
| IGW.31 | SCENE Intelligent Gateways MUST be able to connect to each other transparently | Content delivery |
| IGW.32 | SCENE Intelligent Gateways MUST have local storage capacity | Content delivery |
| IGW.33 | SCENE Intelligent Gateways SHOULD be aware of its location, direction and speed | Content delivery |
| IGW.34 | The IGW MUST contain a web portal allowing users to register | Content delivery |
| IGW.35 | The Portal MUST offer a selection of preloaded contents | Content delivery |
| IGW.36 | The Portal MUST include an easy-to-manage interface for administrators to upload and document the contents (metadata) | Content delivery |
| IGW.37 | The Portal MUST include a user-friendly interface for users to access to the contents | Content delivery |

4.5.1.1 Non functional requirements

| | | |
|--------|---|------------------|
| IGW.39 | The IGW SHOULD support the latency and delay requirements of IoT services | Content delivery |
| IGW.40 | The IGW SHOULD support the QoE requirements of content delivery services | Content delivery |

D2.1

5 VERIFICATION METHODS

5.1 Modules validation

A test plan will be produced for each SCENE module to verify the functionalities and performances of each modules and the whole system both in controlled environment and during the field trials. The test plan will take into account the list of requirements of D2.1 and will verify that they are fulfilled by the platform. Performances and functionalities will be deduced from D2.1 and D2.2. These test plans will be internal to the project.

Each module will be validated prior to integration according to the test plans defined in Task 6.1. results of tests and integration will be recorded in D6.1.

5.2 Pre-qualification

Test scenarios will be defined in Task 6.2, which will consider the use cases deployed in the pilot(s). The whole system performances will be assessed according to the metrics which are defined in T6.2 as well. Results of integration and testing will be listed in D6.2.

5.3 Usage testing (pilots and field tests)

Tests scenarios for pilots, field tests and pilot site(s) will be defined M12. The goal of the tests is also to evaluate users and stakeholders experience to assess the commercial value of SCENE innovations and understand eventual adaptations of the systems. This will be summarised in D6.3.

6 KEY PERFORMANCE INDICATORS

Here follows a first list of KPI for the system. The values of the KPIs will be further elaborated in D2.2.

| Services | Metrics | Description |
|------------------|--|---|
| Content delivery | QoE | The quality of experience (QoE) is the best metric to assess the quality of reception. It can be measured by tools like VQM (reference-based tool) |
| IoT | Sensor data latency | This KPI is intended to measure how timely and frequent is the sensor data capture. Value is determined by measuring the time gap among the time the sensor has detected a telemetry data and the time data is captured by one of the circulating Intelligent Gateway |
| IoT | SP Data Latency | This KPI is intended to measure the efficiency in Service Platform elaboration by detecting the gap between the time the gateway publishes data to the central server and the time the data is available, after filtering, transformation and enrichment, into the data layer available for inquiring and analytics functions |
| IoT | Sensor sample ratio | This KPI represent the ratio among the sensor telemetry sample captured and sent to SCENE Service platform and the expected gathered sample based on sensor measurement frequency, caching capability and estimated connection frequency with Intelligent Gateway |
| IoT | Listened Sensor ratio | KPI to measure the ratio among the number of sensors from which IoT data has been collected in a defined timeframe (day, week etc...) and the total number of sensors distributed in the smart city |
| Caching | Miss/Hit ratio | Represents the total number of data requests for a content, which is "not present"/present (miss/hit) in the cache. |
| | Path length (hops count, Access delay) | This can be measured by counting the delay or the number of hops between the source of the request and the cache/server containing the requested data. |

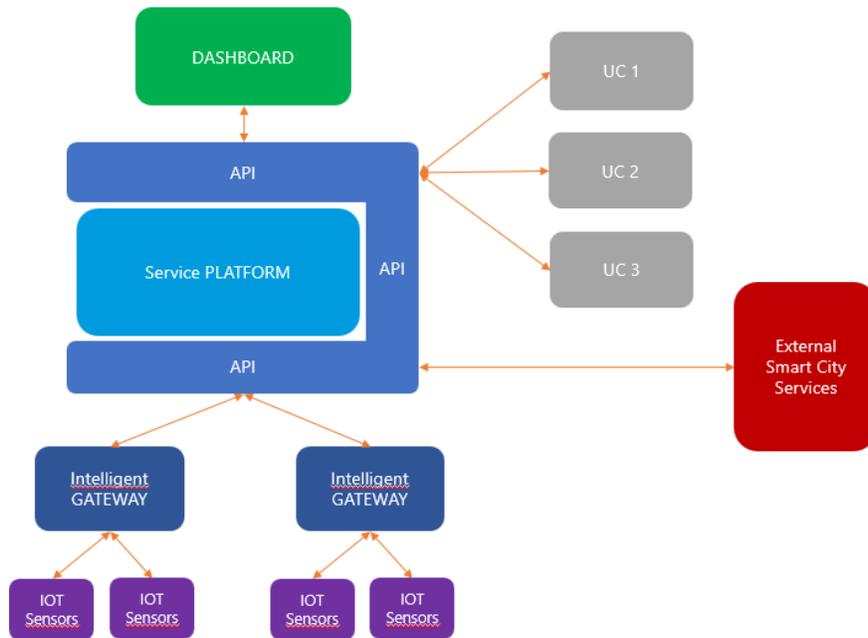
D2.1

| | | |
|----------|--|---|
| | Cache stability | It is meant by cache stability, the stability of contents in the cache. This metric is interesting mainly for SSD memories as it impacts their durability (i.e. lifetime). It can be measured by counting the number of changes in the cache. |
| | Cache load distribution | The caching strategy should consider the load balancing between the different caches. The variance of the load on the different Magic-Boxes' caches will reflect this metric. |
| | Content density in caches vs. popularity | The number of copies of the same contents that should be stored on local caches depends on its popularity. The more popular the content, the greater its density in caches should be. It can be measured by counting the number of popular files in the cache |
| | Cache cooperation | This metric measures the average number of caches that will cooperate to serve a user demand. The cooperation here means that several cache nodes may provide different parts of a piece of content (e.g., a video) to satisfy the user's requests. |
| General | Packets' drops (loss rate) | This metric directly reflects the congestion level of the network. It can be measured at the different nodes (i.e. at the transmission buffer level). |
| Security | False Positive Rate | This metric reflects the number of raised alerts which are not attacks. The objective of the security service will be to have this ratio as small as possible to avoid false alarm inspection and therefore time delay. |
| Security | True Positive Rate | This metric directly reflects the number of attacks detected. The security service must provide a high true positive rate. |
| Security | Time to detect | This metric represents the delay between the start of an attack and its detection. SCENE security service will try to provide a delay as small as possible. |

7 PRELIMINARY SYSTEM ARCHITECTURE

7.1 Preliminary System Architecture

The SCENE Platform is composed by several subsystems that implements specific functionalities. A general architecture schema based on functional high-level modules is presented. The reference is the following diagram



General High Level of SCENE Platform Architecture

Each module is described in the following table

| Entity | Description |
|------------------|--|
| Dashboard | The Dashboard is the GUI module that will allow a user to interact with the SCENE platform. Based on web technologies it will offer functionalities for monitoring the platform, for accessing the data managed by the system, analytics and statistics, as well as functions for managing all the actors involved in the use of SCENE platform. All the functions will be presented based on user authentication and role-based authorization. |
| Service Platform | This is the central core system of the SCENE Platform. It includes all functionalities for: 1) Data persistence for all the data coming from sensors and gateways; 2) Middleware logic for orchestration of internal and external services, Event and Notification Management; 3) System Registry and |

D2.1

| | |
|------------------------------|---|
| | Provisioning, for setting configuration and users, device and sensors provisioning procedures; 4) Identity Access Management, for implementing the central functionalities for users and application security; 5) Device management module to manage all the aspect of interaction with IGW; 6) An analytics module, for gathering all the information related to SCENE service, postprocessing it and inferring different metrics 7) managing caching and prefetching in IWG for content delivery purposes |
| API | An Interface layer to allow SCENE to dialog with all components of the Platform as well with External Smart City Services. It will be realized by using standard technologies |
| IGW | The Intelligent Gateway has to perform following main functions: 1) Data Collector: This module has to communicate with IOT Sensor in order to perform set of operations such as push data to the IOT sensor in order to perform specific operation and/or pulling data from IOT sensor and send it to Service Platform. 2) SOTA (Software Over The Air): Install set of smart cities application into the gateway and run it instead of executing into 3) Management of IOT sensor 4) Content delivery: 4.1) Interface with Internet 4.2) content caching and prefetching 4.3) content distribution using WIFI 5) expose API for Service Platform in order to retrieve data for analytics for example 6) MUST have internet connectivity in order to communicate with the Service Platform |
| IOT Sensors | They are the IOT sensors belonging to a generic Customer, deployed throughout the Smart City. They will interact with IGW for sending data to SCENE Platform |
| External Smart City Services | They are the Customers' systems to whom the SCENE Platform offer its services |
| UCx | They are the instance of “External Smart City Services” dedicated to our four Pilot Use Cases |

This general architectural scheme represents an initial organization of the SCENE Platform. The functional modules here described show the overall structure of the system and constitute the input for determining a detailed SCENE Platform Architecture, that will be described in the deliverable D2.2.

D2.1

8 CONCLUSION

The present document starts to present the first definition of the Use Cases for the project. Three use cases reflect needs of city government and planners or managers, while the fourth focusses on content delivery for transit users.

In the second part requirements for the system – both on a business and general level as well as on a per use case level – are presented. Then verification methods for the requirements are shown as well as relevant KPIs. Finally, a preliminary system architecture is shown.

The document will serve the consortium to develop the prototypes for the different modules as well as defining the pilots of the systems - it will then be revisited as Deliverable 2.3 in month 14.