SYNCHRONICITY

GA no:	732240
Action full title:	SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond
Call/Topic:	Large Scale Pilots
Type of Action:	Innovation Action (IA)
Starting date of action:	01.01.2017
Project duration:	33 months
Project end date:	30.09.2019
Deliverable number:	D1.3
Deliverable title:	Guidelines for SynchroniCity architecture
Document version:	1.0
WP number:	WP1
Lead beneficiary:	DigiCat
Main author(s):	Alex Gluhak, Andrea Gaglione, Angelo Capossele (DigiCat), Thomas Gilbert (AI), Martino Maggio (ENG), Hanna Niemi-Hugaerts (FVH), Lucio Scudiero (MI), Arturo Medela (TST), Luis Muñoz (UC), Martin Brynskov (AU)
Internal reviewer(s):	Laurent Horvath (Carouge), Omer Ozdemir (ATOS), Pieter Colpaert (IMEC)
Type of deliverable:	Report
Dissemination level:	Public
Delivery date from Annex 1:	M4
Actual delivery date:	M5

Co-funded by the European Union

This deliverable is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732240.

Executive Summary

Many cities are investing into digital technologies to improve efficiency of activities, processes, decision making as well as to increase the citizens' quality of life. Examples range from improved mobility experience through adaptive traffic management and multi-modal transport over to resource reductions achieved by smart street light control, waste collection and irrigation management.

SynchroniCity's vision is to scale these opportunities by envisioning a vibrant and common digital single market for IoT-enabled urban services with standardized interfaces, common information models and new market place enablers. This vision is also shared with the Open & Agile Smart Cities (OASC) community, which already now encompasses more than 100 cities across the world.

In SynchroniCity, eight European cities are leading the way in establishing reference zones for such a digital single market under the IoT Large Scale Pilot Programme umbrella. The cities include Antwerp, Carouge, Eindhoven, Helsinki, Manchester, Milano, Porto, and Santander.

This report provides a first step in establishing more concrete boundaries of the digital single market vision by examining current key challenges for realizing IoT-enabled urban services and identifying technological and socio-economic barriers and desired properties for such an environment.

The envisioned opportunities are extracted by a joint analysis with the eight cities and shaped as use cases, high level platform requirements and initial architectural considerations. Furthermore, the report examines practices for the governance of IoT infrastructure and open data across the eight cities and makes recommendations for principles to be considered for the governance of the envisioned marketplace.

One should note that this document is a first step towards the design of a system architecture underlying the digital single market for IoT enabled urban services. As the work on the architecture and its components mature and find initial validation, more detailed guidelines and recommendation on their use in cities will emerge.

In the following, we provide a high-level summary of the key points addressed in the report. For more details, please consult the respective sections of the report.

Identified barriers for the smart city market

Our initial analysis in Section 2 reveals seven key technical and four socio-economic barriers that hamper the progress on the smart city market.

Key identified technological barriers are:

1. *Lack of standardized multi-vendor ecosystem*
2. *Lack of common service provisioning environments across cities*
3. *Close coupling of IoT infrastructure and applications (IoT solution silos)*
4. *Lack of tools, license models and platforms to facilitate the incentivized sharing of urban IoT data and other relevant data sets*
5. *Lack of harmonized business practice and legal frameworks across cities*
6. *Lack of understanding of privacy and personal data protection implications*
7. *Lack of confidence in adopting emerging technologies due to increasing technology fluidity*

Likewise, the key identified non-technical barriers included:

1. *Economical costs and budget constraints*
2. *Frequent political changes and lack of continuity*
3. *Lack of involvement of citizens, SMEs or support from them*
4. *Lack of a holistic smart city strategy*

Properties of a digital single market for IoT enabled urban services

The identified barriers revealed a large fragmentation across different cities and a lack of coherent support mechanisms that make a common addressable market to emerge. In order to overcome these barriers, a digital single market should exhibit the following properties:

1. *Interoperability*
2. *Free competition of vendors and solution providers*
3. *Common service environments*
4. *IoT infrastructure re-use*
5. *Trusted participation of IoT data providers and consumers*
6. *Incentivized data sharing*
7. *Common legal foundation*

Technical vision

Overcoming the identified barriers requires a common approach across the different reference zones. This includes the following key elements:

A common reference architecture for smart city platforms. *A standardized reference architecture, which is widely adopted among cities with clearly defined components and interfaces, is fundamental to overcome vendor lock-in. It will boost market confidence and lay down the foundations for the required economies of scale.*

Common northbound interface. *Developers require a common, homogeneous and IoT independent way to access data from the devices infrastructure, but also from any other subsystem in the city that can provide valuable information to develop smart services and applications. More specifically, this includes 1) a common standard API for context information management; 2) a common set of information models enabling actual interoperability of applications; 3) a set of common standards data publication platforms have to comply with, enabling the harvesting of data coming from multiple federated platforms as well as the publication of real-time open data.*

Common southbound interface. *For IoT device vendors and manufacturers it should become easier to offer suitable device stacks for integrating heterogeneous IoT components into a common environment, together with a market place for compliant IoT products and solutions.*

Market place enablers, *that encourage sharing of urban IoT data and other relevant data sets among different stakeholders. By providing a market place as a one-stop-shop, it will become much easier for data consumers to discover and access urban data sources. The availability of a trusted market place with monetization mechanisms will allow third parties to generate easier revenue streams from their urban data sources. This will encourage more businesses to share currently closed data sources or incentivize deployments of new IoT infrastructure as secondary revenue streams can be generated, making more business cases viable. Data consumers may not require lengthy negotiations of license terms as data license terms can be negotiated from pre-configured options of the provider on the fly.*

System use cases

A detailed stakeholder analysis identified primary stakeholders that would take part in the proposed digital single market. By examining interactions among the stakeholders across the marketplace, we could identify the system use cases which can be grouped as follows:

- ***Cities*** *- use cases cover how to unlock insights into problems using data sources available on the market place, discovery of assets prior to procurement or the discovery of existing SynchroniCity compliant solutions that exist in other cities.*
- ***Market place providers*** *- use cases include the on-boarding of providers of data/services to the digital single market, data usage monitoring, ensuring compliance on standards and SLA and quality*

assurance.

- ***IoT device operators*** *- use cases related to IoT device provisioning, their management, definition of access policies and SLAs.*
- ***Service component provider*** *- use cases addressing the definition of usage licences, access policies and SLA and service component registration.*
- ***Data provider*** *- definition of data license, data access polices and SLA, data cleansing, data source registration and compliance verification with respect to data protection rules.*
- ***Data consumer*** *- use cases include the discovery of data availability, understanding of metadata, data/API access and subscription, popularity/reputation of data sources, discovery of other data consumers for same sources and verification of data source compliance with respect to data protection rules.*
- ***Infrastructure provider*** *- primary use case is the discovery of complaint specifications to enter the digital single market for IoT enabled urban services.*
- ***Citizen/End user*** *- use cases relate to the access to information about personal data processing and demands signaling.*

Recommendations for governance of IoT and data infrastructure in cities

An important point for the effective realization of a DSM across the eight cities of the project is to establish a common set of governance principles for the operation of IoT and data infrastructure in the cities. Our approach was to look initially at best practices across different cities and what precautions are taken to stimulate data availability and use as well as compliance to personal data regulations. We examined a variety of corresponding policy documents across all cities and direct input provided by them and performed an analysis of common or possibly conflicting approaches or gaps in their current practice. We also took into consideration the New York City principles, which more than 30 US cities are supporting.

As a result of this study we derived overall ***50 recommendations*** *that provide the initial basis for the governance of the digital single market among the cities. The recommendations cover the following concerns with regard to IoT infrastructure:*

- *Privacy*
- *Data management*
- *Openness of standards and interfaces*
- *Infrastructure*
- *Architecture*
- *Security*
- *Social responsibility*
- *Managing open data availability*
- *Personal data compliance*

Principles for the management of Open Data in cities included the following two dimensions:

- *Managing open data availability*
- *Personal data compliance*

The recommendations considered the personal data protection policies in line with Directive 95/46/EC, the General Data Protection Regulation, the ePrivacy Directive, and the PSI Directive. A more in-depth discussion of the implications of these for cities can be found in SynchroniCity deliverable D1.4.

Abbreviations

ANT	Antwerp
CAR	Carouge
CC BY	Creative Commons Attribution License
D	Deliverable
DPIA	Data Protection Impact Assessment
DSM	Digital Single Market
EC	European Commission
EIN	Eindhoven
GDPR	General Data Protection Regulation
HEL	Helsinki
IoT	Internet of Things
LIV	Lokale Integrale Veiligheidscel
LSP	Large-scale Pilot
MAN	Manchester
NYC	New York City
OASC	Open & Agile Smart Cities
PbD	Privacy by Design
PIA	Privacy Impact Assessment
POR	Porto
PSI	Directive on the re-use of Public Sector Information (Directive 2003/98/EC)
RZ	Reference Zone
SAN	Santander
SCP	Smart City Platform
SEB	Socio-Economic Barrier
SLA	Service Level Agreement
SUC	System Use Case
TB	Technological Barrier
WP	Work Package
WP	Work Package
WT	Work Task

Contents

List of Figures

1 Introduction

Digital technologies offer an opportunity to profoundly change how our existing society works. They can enable a transformation of different industry sectors improving existing business activities, processes, competencies within organizations and across their boundaries.

Data infrastructures and the Internet of Things (IoT) form a critical part of the digitization process by creating adequate awareness of real world processes to drive more efficient (autonomous) decision making.

In terms of data infrastructures, cities have been at the forefront of embracing the open data movement. The release of data sets to the public increased transparency and provided early innovation potential for third party stakeholders. Services such as Citymapper[1] show how open data can add significant benefits to the journey experiences of citizens.

Many cities have invested into the setup of open data portals and pro-actively encourage stakeholders across public departments and the private sector to contribute data sets. At the same time cities are trying to engage entrepreneurs and communities to innovate around these data stores. Early results are promising but static or sporadically changing data sets have their limitations.

IoT infrastructures are increasingly becoming an important element in providing the underpinning digital layer of smart city services. They augment the open data sets with rich real time information about public infrastructure conditions and city processes that can be exploited for a more responsive delivery of public services. Examples range from an improved mobility experience through adaptive traffic management and multi-modal transport over to resource reductions achieved by smart street light control, waste collection and irrigation management.

Various demonstrators of such systems are emerging across the globe showing the benefits of data-driven services based on IoT and data infrastructures. However, many of these systems currently operate in silos both in terms of technology and city operating environments. Interoperability issues and lack of economies of scale make many potential business cases still hard to justify and result in a lack of confidence on the market.

SynchroniCity aims to overcome the existing barriers on the market by fostering the emergence of a digital single market for smart city services. It brings eight European cities together to work on a common blueprint for their IoT and data infrastructures with standardized interfaces and information models, creating an environment that allows vendors and solution providers to more openly compete.

Our vision is to move from disparate data stores and city platforms to vibrant marketplaces for urban data and services, which provide adequate incentives for a variety of stakeholders for participation. For providers of IoT infrastructure and other urban data sources it should provide a trusted environment to generate reliable revenue flows. For application and service developers, it should allow frictionless access to reliable and trusted urban data streams to be used as assets underpinning their innovation – no matter what city. Cities and infrastructure providers can benefit from an aligned environment with standardised interfaces to access a diverse pool of vendor solutions able to fairly compete on price and performance.

This document sets out the groundwork of SynchroniCity by examining existing barriers for realizing IoT enabled smart city services. We identify desired properties of a digital single market for smart city services to tackle these challenges and develop a more detailed concept of it. The document identifies underpinning use cases and derives requirements for the realization of these. It also closely examines current practice for the governance of IoT infrastructure and open data used by the participating cities and synthesis recommendations for common principles to be used across cities. The section ends with outlining possible starting points for an architecture, guiding the development of a more holistic architecture in WP2.

[1] https://citymapper.com/

2 Vision of SynchroniCity

Smart cities hold the potential to be a key driver and catalyst in creating a large scale global IoT market of services and hardware. However, the emerging smart city market faces specific challenges that act as barriers to growth, impeding rapid innovation and inhibiting widespread market adoption.

SynchroniCity represents the first attempt to deliver a digital single market for Europe and beyond for IoT enabled urban services by piloting its foundations at scale in reference zones across eight European cities, involving also other cities globally. It addresses how to incentivize and build trust for companies and citizens to actively participate, in finding common co-created IoT solutions for cities that meet citizen needs and to create an environment of evidence-based solutions that can easily be replicated in other regions. These reference zones are based on cities at the forefront of smart city development covering different geographies, cultures and sizes and include Antwerp (BE), Carouge (CH), Eindhoven (NL), Helsinki (FI), Manchester (UK), Milano (IT), Porto (PT) and Santander (ES). Globally, SynchroniCity adds committed replicating reference zones in Mexico, Korea, USA and Brazil.

In the following section we identify common barriers across these cities and detail desired properties for the desired SynchroniCity digital single market.

2.1 Barriers and difficulties of the current market

Despite the technology hype in recent years, smart cities have remained a difficult market place for both supply side (e.g. vendors and solution providers) as well as demand side stakeholders (e,g. public authorities). The challenges are based on a blend of technological and non-technological barriers that undermine the market confidence of the smart city ecosystem, making wider scale adoption of IoT enabled smart city solutions difficult.

2.1.1 Technological Barriers

In the following we highlight key technical challenges that the SynchroniCity project aims to tackle. We label each technological barrier as TB and include a number for easier referencing.

TB1: Lack of standardized multi-vendor ecosystem
The lack of usable standards and an interoperable vendor ecosystem for IoT-enabled smart city solutions makes it difficult for cities to commit to a specific solution of a vendor, without creating significant dependencies on it for future developments. There is a latent fear of vendor lock-in that can affect further procurement choices for expansions and scaling of the underlying infrastructure, without significant system integration expenses. As a result, cities are often reluctant to make larger investments in smart infrastructure hampering the market uptake of these.

TB2: Lack of common service provisioning environments across cities
Current APIs for accessing streaming data from IoT infrastructures and other sources can vary greatly across cities, and so can the availability of specific data sources and underlying data formats. Further complications arise from the re-negotiations of license terms with alternative data source providers in new city environments. This makes it very challenging for many developers and providers of IoT-based smart city services to deploy and operate a service that has been initially developed for one city environment to another, significantly limiting the opportunities that come from economies of scale. We call the resulting issues “city lock-in” of service developers/providers.

TB3: Close coupling of IoT infrastructure and applications (IoT solution silos)

The lack of interoperability of IoT infrastructure and their tight coupling to specific services and IoT platforms makes it difficult to support IoT infrastructure reuse and achieve necessary economies of scale. The resulting siloed business models, e.g. one deployment for one specific app, make it harder to achieve a viable return of investments. Finding secondary exploitations for IoT deployments would enable new business models and bring down the barrier for investment. This, however, represents a major challenge with the current siloed situation. And sticking to the silos makes cities vulnerable to disruption from the big, global platform operators in the so-called platform economy.

TB4: Lack of tools, license models and platforms to facilitate the incentivized sharing of urban IoT data and other relevant data sets

The first wave of smart city services have been predominantly developed around open data. Such data is in most cases shared if not considered sensitive, and the success of services developed on top is often only modest. Proprietary data sets such as IoT-generated data, closed organizational data or personal data have the potential to offer higher value for richer smart city services, but are not released for exploitation or not readily available. There is a lack of incentives, market confidence and trust for organizations and individuals to share new data sets as licensing models are not yet properly understood and developed, and key ecosystem foundation for such a market place are still missing. The future-proof market mechanisms which would extend the commercial viability of open data beyond traditional licensing models are also not yet in place.

TB5: Lack of harmonized business practice and legal frameworks across cities

Technology alone can quickly lose its effectiveness if the right environment and operational context is not provided. Many factors exist in a city environment that can act as barriers for successful adoption of IoT interventions. Examples are inflexible procurement models or lack of innovation culture and mind-set in city departments. In cases where IoT interventions are expected to drive human behaviour change or disrupts existing business practice, the right legal and policy framework must be in place to incentivize stakeholders' participation and/or buy-in. Current environments are too constrained and rigid to experiment with such new opportunities. Furthermore, there is a lack of common principles across cities and common legislative frameworks making it difficult to easily migrate similar IoT service experiences.

TB6: Lack of understanding of privacy and personal data protection implications

Smart Cities heavily rely on large-scale processing operations which aim to process a considerable amount of data, which can be "personal" in the reading of the European data protection legal framework. In so far personal data are at stake, every stakeholder within the smart city should carefully appraise what are the personal data protection risks run by citizens. This ought to be done by means of a Data Protection Impact Assessment ("DPIA" or "PIA"), whose objective is to map the risks, provide for countermeasures and help designing the smart city according to privacy and data protection principles. It is therefore of the utmost importance to provide cities with a PIA framework readily usable by the various stakeholders involved (e.g. cities' administrators, IT providers, suppliers of public services etc.).

Recent changes to regulatory environment such as the GDPR will also make the cross-linking of personal data more difficult and with it reduce opportunities how exploitable end user insights can be generated. This results in an increased barrier for innovation around end user centric data that must be compensated by new technological solutions that support a more explicit accommodation of end user consent, in order to allow for similar exploitation opportunities.

TB7: Lack of confidence in adopting emerging technologies due to increasing technology fluidity

The pace of technology development is ever increasing across the world. The fierce competition due to globalization on a connected global market has also increased the diversity of competing technical solutions for a particular problem domain. More efficient technology development shortens the development cycle considerably, overhauling a generation of technology before they are properly adopted and tested by the end user communities. As a result, there is a lack of substantial comparative studies and benchmarks of different competing cutting edge technology solution that can demonstrate objectively their trade-offs and provide confidence to adopters needed for further investment decisions. The constant evolution of IoT technologies also raises concerns of securing

smart city infrastructure effectively, as they potentially enlarge the attack vector and make the cities more vulnerable for cyber attacks. It makes it also increasingly harder for cities to understand actual product lifecycles, as deployed solutions may become obsolete before their planned depreciation. All this factors lead to a decrease in end user confidence to make more substantial investments in IoT infrastructures.

2.1.2 Socio-economic barriers

In the following we provide a summary of the key socio-economic barrier for deploying and operating IoT infrastructure in urban environments. We label each socio-economic barrier as SEB followed by a number for easier referencing. While some socio-economic barriers are common across different sectors, here we focus on those specific to cities.

SEB1: Economical costs and budget constraints
Budget reduction or shift in priorities. Investment in smart city requires Capex. Benefits may be visible only months or years after the implementation. The lack of immediate return on investment may cut the budget. This leaves cities more susceptible to free "Google-like" offers that trade convenience and cost reduction with possible loss of flexibility and autonomy.

SEB2: Political changes
Election may change the focus of the city. Decisions are not always based on facts but on feelings and ways to disregard the work of the past leader. The smart city process should have a vision for the next decade but unfortunately is subject to change with each election cycle.

SEB3: Lack of involvement of the citizens, SMEs or support from them
If citizens or SMEs do not follow or support the path set by a city, does it worth to continue? Involvement from citizens and SMEs is one of the key success factor to move ahead and to make it grow.

SEB4: Lack of a holistic smart city strategy
The lack of an agreed overarching strategy may limit the effectiveness of proposed technology interventions. What does the city and the citizens need? What are the priorities, what are the goals we want to achieve? What are the next steps, whom data belongs to? Where do we store the data? Are we compliant with the laws? How can a city move forward and where to start? For some cities and politicians, it is too risky to jump into this process.

2.2 Properties of the digital single market for IoT enabled urban services

The above barriers expose a great incoherence across different European cities leading to a perceived fragmentation of the overall Smart city market. This severely limits the opportunity for free competition among multiple vendors and the ability to serve a larger market with single solutions.

By overcoming the barriers mentioned above, SynchroniCity aspires to create a digital single market for IoT enabled smart city services. Borrowing from the general DSM principles and building upon the pillars identified by the EC[2], we aim to create an environment that substantially improves market confidence of IoT enabled smart city services by:

1. providing improved access for business, cities and citizens to services and solutions across the identified pilot reference zones in Europe and beyond;

[2] https://ec.europa.eu/digital-single-market/en/digital-single-market

2. creating the right conditions for a level playing field in the reference zones to foster competition and permissionless innovation;
3. maximize the growth potential of the emerging digital market across these reference zones.

More specifically, the envisioned digital single market should exhibit the following properties (note this is the what and not the how):

Property 1: Interoperability
Provide cities with the freedom to choose interoperable solutions from multiple vendors to provide the necessary enabling technology layer for smart city operations. Use the new European Interoperability Framework (EIF) and its recommendations as a reference.

Property 2: Free competition of vendors and solution providers
Enable free and thriving competitions among vendors and providers of interoperable IoT infrastructure components within the context of a common reference architecture across different city environments

Property 3: Common service environments
Enable frictionless portability of IoT enabled smart city services from one city to another as part of the digital single market. This includes minimizing overhead to adapt APIs and to obtain access to equivalent data sources.

Property 4: IoT infrastructure re-use
Facilitate easy re-use of deployed IoT infrastructures for different IoT services – making multi-tenancy of IoT devices the norm – not the exception.

Property 5: Trusted participation of IoT data providers and consumers
Ensure that data consumers can trust IoT data providers serving in the different reference zones and vice versa. This includes ways to enforce agreed service agreements between both parties and enable corrective actions if violations occur.

Property 6: Incentivize data sharing
Provide a free market in the different reference zones that offers revenue opportunities for providers of IoT data streams and other urban data sources.

Property 7: Common legal foundation
Provide a common legal environment that provides participating stakeholders with a level playing field across all participating reference zones.

Property 8: Increase of competitiveness
Boost local economy by creating or maintaining jobs in Europe and participating cities.

Property 9: Frictionless innovation
Lower barriers for companies to build new and innovative solutions for citizens, organizations and companies within the cities. The DSM should enable and speed-up the creation of innovative solutions.

2.3 Participating stakeholders

Figure 1 presents an overview of the identified stakeholders / entities participating the SynchroniCity DSM and possible interactions and relationships with it.

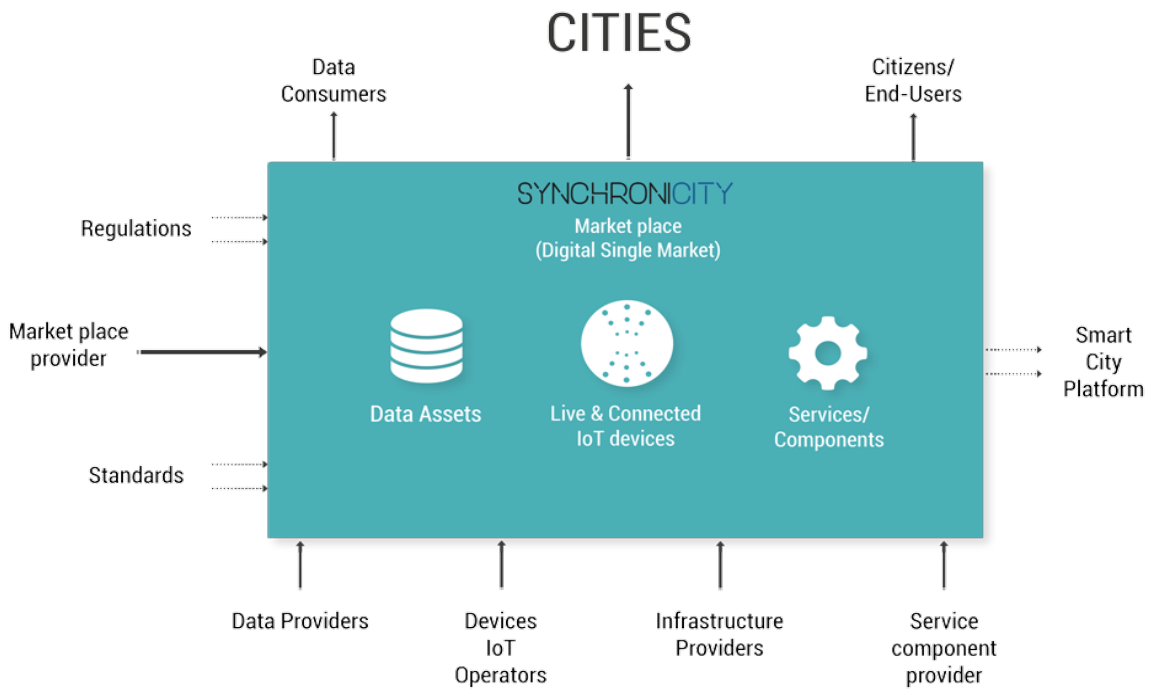

Figure 1. Interaction among the different stakeholders with the SynchroniCity digital single market.

The left-hand side depicts external influences from standards (e.g. for data modelling such as ETSI ISG CIM, ETSI oneM2M, W3C SSN-XG, and also other standards de facto for representing open data) in conjunction with regulations and governance with the data protection, transparency, responsibilities and duties. This market place must be provided and supported by a (neutral) market place provider, which provides the basis for the provisioning of its underlying platform and its governance.

Furthermore, the SynchroniCity digital single market is interfaced and must interoperate with the IoT and data platforms that provide the basis for smart city services. This dependency with Smart City Platforms is illustrated in the figure on the right.

Contributors to the market place are depicted in the bottom part of the figure. They include providers of urban data streams and IoT related services / components that the marketplace will offer. More specifically, the key stakeholders identified are the data providers, which can be end-users such as citizens with proactive approach such as crowd-sensing (participatory sensing), SMEs that share data such as taxis companies etc., and any other public institution such as government (budget, demography…) and other public/private organizations related to tourism, environmental monitoring / weather etc. It is also takes into consideration live / connected IoT devices from testbeds, pilots and functional real-world deployments. These sensors will offer near real-time data streams with current values and the capacity in some occasions even of remote control to carry out specific actions. At the same way, infrastructure providers such as cloud computing storage, networking infrastructure and other general purpose resources / services that are required for the management and use of the data are also included., This view is finally completed with the specific service and components for data processing targeting specific needs and solutions.

Finally, consumers on the market place are shown at the top. This includes end users in the form of service providers, the cities themselves but also their citizens, end-users such as cities. They either utilise directly the data sources and services offered to inform themselves, make decision or build new services for the consumption of others.

2.4 Key concepts of the SynchroniCity Digital Single Market

Overcoming the barriers identified in section 2.2 requires a common approach across the different reference zones. In the following we introduce the key foundations for our vision of the SynchroniCity DSM.

Technical barriers TB1, TB2, TB3 and in part TB7 demand a common reference architecture for smart city platforms. A standardised reference architecture, which is widely adopted among cities with clearly defined components and interfaces is fundamental to overcome vendor lock-in. It will boost market confidence and lay down the foundations for the required economies of scale.

Key elements in this reference architecture are common north and southbound interfaces. TB4 demands new market place enablers that encourage sharing of urban IoT data and other relevant data sets among different stakeholders. Lastly, TB5 and TB6 relate to finding agreement on common principles of governance of a DSM.

In the remainder of this section we discuss north and southbound interfaces of a Synchronicity reference architecture and examine in more detailed our envisioned market place enablers. Common governance principles across cities and suitable guidelines will be covered separately in section 5 and 6 of this report.

2.4.1 Northbound alignment

Seen from a developer's perspective, one city is not a market. A number of countries or a continent is a sizable market. But global de facto standards for portability and interoperability are the only way to create a true global market for smart city services. In such a market, not only large solution providers but entrepreneurs can start investing and specialising with an outlook of sustainable business models in public-private innovation partnerships. Developers require a common, homogeneous and IoT independent way to access data from the devices infrastructure, but also from any other subsystem in the city that can provide valuable information to develop smart services and applications. If cities are not able to select standards collectively, services cannot be developed for multiple customers at once in a feasible manner.

Synchronicity's vision for the northbound alignment is to aim for simple, functional, minimal de facto standard ways of accessing and exchanging data. This would have the potential to take smart city innovation beyond the limits of the current chicken-and-egg situation where no systems can scale and spread because there are no standards, and there are no standards because there is no widespread deployment.

In order materialize this very same vision, the global Open & Agile Smart Cities (OASC) initiative was created to kickstart the use of a shared set of ways to develop systems once for multiple cities and make them interoperable between cities, and within a city.

Cities joining the OASC committed to adopt the following 3 mechanisms:

- **a common standard API for context information management** (gathering, processing, analysis of data at large scale, including data coming from the Internet of Things) bringing information about what is going on in the city: on example of such API is FIWARE NGSI API.
- **a common set of information models** enabling actual interoperability of applications, starting with the ones defined in the CitySDK and FIWARE data models projects.
- **a set of common standards data publication platforms have to comply with**, enabling the harvesting of data coming from multiple federated platforms as well as the publication of real-time open data. CKAN can in many cases serve as the base open source reference implementation of a data publication platform complying with these requirements.

Thanks to the open nature of OASC specifications, cities and application providers will be able to avoid lock-in to a particular Smart Digital Services infrastructure provider. Indeed, application providers will be able to port their applications across different infrastructures, supported by different

infrastructure providers. Decisions to choose a given infrastructure provider will be driven, not only based on costs, but also trust, e.g. who will provide and operate the environment where applications or where data will be hosted. This is particularly relevant when data (e.g. those affecting personal information) have to comply with certain regulations or has to cope with some security and privacy requirements.

2.4.2 Southbound alignment

Increasing demands in the provision of more efficient and sustainable urban services are leading the cities and city managers to adopt information and communication technologies (ICT) as a key enabler in fitting such demands. In particular, Internet of Things (IoT) is becoming one of the most popular technologies which is being adopted to support the operation of services such as waste management, street lighting or efficient water management. There exists a wide plethora of standards for IoT connectivity, from well-known technologies such as WIFI, Bluetooth, ZigBee to advanced and IoT specific approaches as 3GPP and LPWAN (e.g. LoRaWAN, Sigfox) and IoT protocols as MQTT, CoAP or OMA DM and LWM2M. All these technologies have to be integrated opportunistically in cities, and in many cases tailored for specific verticals. Further to this, the still immature status of IoT technologies as well has the heterogeneity in the demands included in most of the public procurements are conveying towards a scenario in which instead of fostering the adoption of common solutions, a plethora of different technologies and solutions are provided, even at the city level.

Several are the consequences of such a scenario but perhaps the most relevant is the impossibility to create an aggregated homogenous demand which fosters the adoption of similar technologies for common services. Thus, making unfeasible the predicted exponential growth of such technologies with the corresponding consequences in the consolidation of the digital market.

SynchroniCity's vision is to provide enablers for integrating heterogeneous IoT components into SynchroniCity, together with a market place for compliant IoT products and solutions, in order to simplify the adoption and integration by smart cities and apps developers. Moreover, it is convenient to provide an easy way to extend the number of supported communication protocols regardless they are based on open or proprietary specifications.

Aiming at pushing for making a reality the paradigm of "IoT as a commodity" one of the key steps is to agree on a common set of technical and functional requirements which can guarantee the seamless integration of the heterogeneous IoT infrastructure with other entities/subsystems which will consume the data generated by such infrastructure. Hence, the design and specification of the proper southbound APIs fulfilling the specified requirements by most of the urban utilities and services bring us to a new scenario in which the massive adoption of IoT becomes feasible both in terms of technology (interoperability guaranteed) and cost (scale economies).

Hence, in summary the following principles have to be considered from the southbound perspective:

- To identify a set of common technical and functional requirements to be fulfilled by the solutions to be integrated from the southbound perspective
- Although it might be desirable to narrow the spectrum of wireless technologies to be deployed (cost reduction), southbound interoperability has to be agnostic in terms of specific underlying communication technologies offered by the vendors.

2.4.3 Marketplace enablers

Open data portals are currently the most common form of cities to share city related information. These portals typically expose curated static data sets from city departments and make them available for download to 3rd parties. Real time information such as transportation information is made available via managed RESTful APIs to 3rd parties, either for free or for a service charge. This

applies also to other IoT data streams that are made available such as environmental monitoring information, parking information, traffic information. Often data sets and APIs are scattered around different websites of different providers and use different APIs and data formats. In summary access to relevant urban data streams is currently fragmented, making it more difficult for developers to access information coherently, negotiate access to data sources. Likewise, potential data owners find it difficult to sign post their city related data sources to interested third parties and open up new revenue streams.

SynchroniCity's vision is to move away from a fragmented data sharing experience in cities towards a more coherent market place, which brings together a variety of different city related IoT data streams and urban data sets. Such a market place would represent a one-stop-shop for the exchange of urban data related to a city. This includes both static data sets or dynamic IoT data. It will allow interested third parties to discover available data sources and chose adequate ones for an envisioned IoT service. Data providers would have a place to advertise their data sets and configure adequate license terms and pricing for the use of the data by third parties. Market place mechanisms would ensure a more structured exchange of the offered urban data and ensure the exchange of adequate value flow according to the configured license terms and perform impartial accounting for both provision and consumption. Additional trust can be established by tracking the reputation of both data providers and data consumers.

The above market place mechanisms will overcome several shortcoming and would support the following features:

1. By providing a market place as a one-stop-shop, it will become much easier for data consumers to discover and access urban data sources
2. The availability of a trusted market place with monetization mechanisms will allow 3rd parties to generate easier revenue streams from their urban data sources. This will encourage more businesses to share currently closed data sources or incentivize deployments of new IoT infrastructure as secondary revenue streams can be generated, making more business cases viable.
3. By providing a set of proven licenses and license templates for urban data, providers to rapidly experiment with adequate models that satisfy demand side requirements.
4. Reputation mechanism and impartial accounting increases the confidence in the market place participants. As such incentives exists for providing high quality data as higher premiums can be requested.
5. Data consumers to not require lengthy negotiations of license terms as data license terms can be negotiated from pre-configured options of the provider on the fly. Providing an easy way for consumers to create a digital contract with a data provider, stating consuming limits, pricing, etc.
6. Through the market place, the city can not only offer access to data but also to functionality by opening up the APIs used in city applications to 3rd parties. E.g., offering citizens to log in into 3rd party applications with their digital city-ID (the same way many applications allow users to log in with their Facebook and Google-accounts).

3 System use cases for the SynchroniCity digital single market

The previous section has highlighted relevant stakeholders participating in the SynchroniCity market place. In the following we examine a set of system use cases, which capture how different participating stakeholders interact with the market place.

3.1 Use case engineering process

Use cases are written for the purpose of extracting high level platform requirements that will feed into task T2.1, and is done in by collaborating with city representatives involved in defining the overall SynchroniCity smart city platform. The process included a workshop led by DigiCat, where several rounds of brainstorms were conducted, ideas were discussed and grouped according to the different relevant topics to get a better understanding of how they related to each other. The process has been very beneficial for the project, and the workshops not only provided insights into use cases and scenarios that should be covered by the project, it also gave partners a much-needed common vocabulary that will be used for the rest of the project.

The initial stakeholder analysis has not included a prioritization phase, where specific stakeholders are given more or less influence over the project. This is also reflected in the derived use cases, where the prioritization will be made democratically by letting the stakeholders vote. The idea is that the perceived importance of each use case will be captured from the viewpoint of each specific stakeholder.

3.2 System use case template

A template has been devised to gather all the relevant information needed. It was imperative that the template was simple enough for non-technical people to use, but also capture enough relevant information on stakeholders and their interactions that meaningful system requirements could be extracted. The template covers the existing practices, how they the use case proposes to improve them, and also a rating system to allow an easy scoring mechanism to sort the use cases based on relevancy.

The fields of the template include:

- Use case title
- Use case objective
- Primary stakeholder
- Primary stakeholder perspectives
- Secondary stakeholder
- Secondary stakeholder perspectives
- Use case narrative
- Barrier to be overcome in current practice
- Relevancy rating

There is also a reading guide built into the template, which is available to partners in JIRA[3]. Here partners and teams can easily collaborate and manage use cases, and link them to requirements without the overhead of maintaining manual references in spreadsheets and documents. It is also easy to generate reports and follow progress through the tool.

3.3 Summary of system use cases

The identified system use cases are organized by the primary stakeholder and encompass the following:

- **Cities -** use cases cover how to unlock insights into problems using data source available on the market place, discovery of assets prior to procurement or the discovery of existing SynchroniCity compliant solutions that exist in other cities.
- **Market place providers -** use cases include the on-boarding of providers of data/services to the digital single market, data usage monitoring, ensuring compliance on standards and SLA and quality assurance.
- **IoT device operators -** use cases related to IoT device provisioning, their management, definition of access policies and SLAs.
- **Service component provider -** use cases addressing the definition of usage licences, access policies and SLA and service component registration.
- **Data provider -** definition of data license, data access polices and SLA, data cleansing, data source registration and compliance verification with respect to data protection rules.
- **Data consumer -** use cases include the discovery of data availability, understanding of metadata, data/API access and subscription, popularity/reputation of data sources, discovery of other data consumers for same sources and verification of data source compliance with respect to data protection rules.
- **Infrastructure provider -** primary use case is the discovery of complaint specifications to enter the DSM.
- **Citizen/End user -** use cases relate to the access to information about personal data processing and demands signalling.

In the following we will summarise each system use case briefly. A detailed description of each system case following the above described template can be found in Appendix A.

3.3.1 Cities

Use case id:	SUC-Asset-Discovery
Use case title:	Asset Discovery Prior Procurement
Use case objective:	Browsing, identifying and obtaining detailed information about already available assets (e.g. datasets, technologies, etc.), to be potentially used as building blocks for a particular required solution.

[3] https://www.atlassian.com/software/jira

Barrier to be overcome in current practice:	Current practice causes cities to incur in non-structured search for information and solution providers, that usually leads to proprietary solutions and information silos. Other barriers include: ● Lack of city marketplaces ● Heterogeneity of marketplaces, overcome by explicitly targeting cities ● Compliance issues, which are minimized because the assets on the market place are SynchroniCity compliant

Use case id:	SUC-Solution-Discovery
Use case title:	Discovery of SynchroniCity Compliant Solutions
Use case objective:	Browsing, identifying and obtaining detailed information about previously developed solutions that were deployed in other cities and thus are considered as SynchroniCity Compliant and can be replicated and/or adapted for use in other cities.
Barrier to be overcome in current practice:	Current practice causes cities to incur in non-structured search for information and solution providers, that usually leads to proprietary solutions and information silos. Other barriers include: ● Lack of city marketplaces ● Heterogeneity of marketplaces, overcome by explicitly targeting cities ● Compliance issues, which are minimized because the solutions on the market place are SynchroniCity compliant

3.3.2 Marketplace providers

Use case id:	SUC-Onboarding
Use case title:	Onboard (3rd party) data / service providers
Use case objective:	To disclose (third party) data (e.g. on mobility) in order to provide it to data consumers. The data/services will be offered in a standardized way.
Barrier to be overcome in current practice:	Current practices vary: some cities have their own marketplace, others use 3rd party marketplaces or don't have a marketplace yet. Some cities only (want to) disclose city owned data on the city marketplace, others (want to) include data from 3rd party data providers. Barriers: ● Pure data provider: business model ● Mobility provider: external control ● Other: absence of standardized data Overcome ● Warranty: only pass through ● Not within this UC

	● Description / best practises

Use case id:	SUC-Data-Source-Usage
Use case title:	Data Usage Monitoring
Use case objective:	To provide marketplace providers with the ability to check which one of the various data they are offering in the market results most successful and/or useful according to experimenters and users. SynchroniCity platform could even suggest some potential useful services derived from that data usage records, which in turn would help stakeholders to outline their action plan.
Barrier to be overcome in current practice:	If the goal is exclusively monitoring, that is crude data not subjected to subjective views like would be the case of rating data. However, it is necessary to develop a robust and reliable monitoring system that provides valuable results (e.g. distinguishing between total data usage and same-IP data usage).

Use case id:	SUC-Compliance-on-Standards
Use case title:	Compliance on Standards
Use case objective:	A way to be sure the delivery of data is compliant to generally accepted standards.
Barrier to be overcome in current practice:	Barriers: ● Too many so-called standards, unclear which ones to apply, let alone enforce towards data providers ● Willingness to change Overcome ● Providing a SynchroniCity quality label for existing standards, define new standards where none exist ● Well documenting

Use case id:	SUC-Compliance-on-SLA
Use case title:	Compliance on SLA
Use case objective:	Offering reliability towards the data consumer for both north- and southbound API's. Making sure that the 'SLA-south bound' (the weakest link) is able to provide enough assurance for our own 'SLA-northbound'.

Barrier to be overcome in current practice:	Barriers: ● No SLA's (data and services are often provided on a best effort basis) ● Non-standard SLA's (not easily comparable) Overcome ● By providing a SynchroniCity quality label where SLA's exist, creating standard SLA's where none exist ● Well documenting ● Provide a SynchroniCity document with the guidelines

3.3.3 IoT device operators

Use case id:	SUC-Device-Provisioning
Use case title:	Device provisioning
Use case objective:	To provide guidelines which help IoT device operator to better know how to perform the deployment of its devices within SynchroniCity context and specify how to include them in the device portfolio that future users will have access to.
Barrier to be overcome in current practice:	Different standards and data models increase complexity and make not easy for potential users try to employ certain IoT devices and their associated data.

Use case id:	SUC-Device-Management
Use case title:	Manage device in uniform way
Use case objective:	To illustrate the benefits of having a common set of management tools for device operation and maintenance.
Barrier to be overcome in current practice:	Currently, devices are managed based on a proprietary basis promoting vendor lock-in. A digital single market approach will clearly overcome such barriers.

Use case id:	SUC-Data-Source-Access-Policy
Use case title:	Define data access policies
Use case objective:	Define rules, procedures, and conditions according to which data resources of a data provider are made available to data consumers.

Barrier to be overcome in current practice:	• Heterogeneity of devices and their purposes • Liability of marketplace provider • Compliance issues • Provide SynchroniCity template document with policies

Use case id:	SUC-Data-Source-SLA
Use case title:	Define data SLAs
Use case objective:	Define an official commitment between data provider and data consumer regarding the quality or availability of data.
Barrier to be overcome in current practice:	• Liability • SLA compliance

3.3.4 Service component provider

Use case id:	SUC-Service-License
Use case title:	License for service component provider
Use case objective:	Define a suitable software license which will grant specific rights to the service consumers
Barrier to be overcome in current practice:	There are many types of open source license alternatives out in the Internet. One needs to choose and adapt this license methodology carefully.

Use case id:	SUC-Service-Registration
Use case title:	Register in service component catalogue
Use case objective:	Registering services which will be used as internal integration components in service catalogue in marketplace.
Barrier to be overcome in current practice:	This case will ease the 3rd party developers to integrate into the platform with their applications which doesn't exist for now.

Use case id:	SUC-Service-Access-Policies

Use case title:	Service access policies
Use case objective:	Defining access policies for the services catalogue in the SynchroniCity catalogue.
Barrier to be overcome in current practice:	n/a

Use case id:	SUC-Service-SLA
Use case title:	Define service SLAs
Use case objective:	Defining SLAs for each service in the catalogue.
Barrier to be overcome in current practice:	SLA terms need to be defined for each type of service

3.3.5 Data provider

Use case id:	SUC-Data-Source-License
Use case title:	Define data license for a new data source in marketplace
Use case objective:	Configuration of appropriate data licenses of a data source provided by a data provider on the SynchroniCity market place
Barrier to be overcome in current practice:	• Define and discover suitable license models for exploitation of data sources • License model flexibility • Provide documents with license options

Use case id:	SUC-Data-Source-Registration
Use case title:	Register a new data source in marketplace
Use case objective:	Make a data source of a **data provider** available in the SynchroniCity market place, so it becomes discoverable by data consumers
Barrier to be overcome in current practice:	• Existence of marketplaces in cities • Heterogeneity of marketplaces • Process in the city / marketplace provider • Liability of marketplace provider • Compliance issues

Use case id:	SUC-Data-Source-Access-Policy
Use case title:	Define data access policies
Use case objective:	Define rules, procedures, and conditions according to which data resources of a data provider are made available to data consumers.
Barrier to be overcome in current practice:	● Heterogeneity of devices and their purposes ● Liability of marketplace provider ● Compliance issues

Use case id:	SUC-Data-Cleansing
Use case title:	Cleansing data
Use case objective:	Ensure that the data provider takes the necessary steps to cleanse his data, making sure that it doesn't contain any information that shouldn't be made available, such as personal data gathered from people who didn't explicitly consented to making it available.
Barrier to be overcome in current practice:	n/a

Use case id:	SUC-Compliance-GDPR-DP
Use case title:	Validate compliance with respect to data protection rules
Use case objective:	Ensure that the **data provider** has complied with personal data protection rules.
Barrier to be overcome in current practice:	Ubiwhere collects and processes personal data from the citizens (data subjects). In doing this it shall ensure that: ● Information on the personal data processing have been provided to the citizens before they could download and use the multi-modal navigation app, including on the purposes of the processing. ● Specific consents have been collected from the citizens with regards to i) the storage of, or access to, information contained in the citizens' mobile (art. 5.3. of Directive 2002/58/EC) and to ii) the processing of the citizen's location data. ● Security safeguards have been applied to personal data (e.g., pseudonymization, encryption etc.). ● Purpose limitation principle is respected (i.e. personal data cannot be processed for purposes which are not compatible with the initial ones).

3.3.6 Data consumer

Use case id:	SUC-Data-Source-Discovery
Use case title:	Discover data availability
Use case objective:	A **data consumer** wishes to build a new and innovative service, and chooses to browse the SynchroniCity DSM. The user should be provided with a search engine, giving search results based on for example tags, semantic information and free text search.
Barrier to be overcome in current practice:	● Achieving critical mass ● Level of documentation ● Quality of data ● Availability of data

Use case id:	SUC-Metadata-Discovery
Use case title:	Understand metadata (accuracy, description, history/length, license/conditions)
Use case objective:	Enable data consumers to check metadata for the available data sources. This metadata consists on any information the data provider may find relevant to feed, such as a general description of the data, its measurements accuracy, the time intervals and periodicity of readings, conditions of use, etc.
Barrier to be overcome in current practice:	n/a

Use case id:	SUC-Data-Source-Subscription
Use case title:	Subscription to the data / API
Use case objective:	A **data consumer** has found one or more interesting data sets on the SynchroniCity DSM. He now wishes to subscribe to the data source, and receive updates when available.
Barrier to be overcome in current practice:	● Level of documentation ● Quality of data ● Availability of data ● Security

Use case id:	SUC-Data-Source-Access
Use case title:	Access data

Use case objective:	A **data consumer** has implemented the API's for several data providers found on the SynchroniCity DSM - now the application has launched and access to the data is crucial.
Barrier to be overcome in current practice:	● Level of documentation ● Quality of data ● Availability of data ● Security

Use case id:	SUC-Data-Source-Popularity
Use case title:	Popularity of data sources
Use case objective:	A **data consumer** can be actively involved in recommending data sources to other potential **data consumers** on the marketplace. It is an important part of the SynchroniCity DSM ecosystem, and helps **data providers** improve their datasets and **data consumers** find relevant data sets.
Barrier to be overcome in current practice:	● Level of documentation ● Quality of data ● Availability of data

Use case id:	SUC-Compliance-GDPR-DC
Use case title:	Validate compliance with respect to data protection rules
Use case objective:	Ensure that the **data consumer** has complied with personal data protection rules.
Barrier to be overcome in current practice:	The cities wish to collect and process an aggregated elaboration of the citizens' personal data (data subjects) in discharging its public task. In doing this it shall: ● Not require citizens' personal data from the data provider, but only aggregation thereof, in so far as this does not impinge on the achievement of the cities' public objectives; ● In case the collection of personal data is necessary, provide to the data subjects concerned some information on the elements of the processing that is not known by them (e.g. from which source the personal data originates and information on the new purposes for which that personal data is processed by the city); this information could be provided also on the city's website or by means of another suitable measure. ● Ensure that the purpose limitation principle is respected (i.e., personal data is not processed for purposes which are not compatible with the initial ones declared to the data subjects by the data provider).

3.3.7 Citizen / End user

Use case id:	SUC-Personal-Data-Processing
Use case title:	Access information about personal data processing
Use case objective:	Enable the citizens of different References Zone to access to the platform providing an overview of all personal data that is being collected and to whom this data is being shared
Barrier to be overcome in current practice:	• Liability of service provider • Data protection issues on sensitive information • Compliance with standards both at national and international level • EU GDPR • Defining 'personal data' • Data transparency (especially in terms of data transferability) • Transparency (trade-off between 'pure' personal data and aggregated data)

Use case id:	SUC-User-Feedback
Use case title:	User feedback
Use case objective:	To enable the citizens and users of SynchroniCity to send out user feedback on the systems deployed and tested in a specific reference zone for different purposes
Barrier to be overcome in current practice:	• To put in place such a "customer service" approach requires huge expenses, the proper supporting mechanism and tools as well as additional research activities that often could not be put in place both by small companies, start-ups or municipalities, especially when the project is still in a development/validation stage • Current mechanisms are often set-up in a one-way direction: from the user to the service. However, a feedback loop towards the user on how the feedback is being handled is required. • The interaction among municipalities, technical staff and users requires relevant efforts in terms of time and translation of needs in effective services and/or applications, as well as to a good data-exchange between the various actors involved • There is the potential risk that there is no follow up on the information and feedback captured from the users

4 High level system requirements

This section presents the high level system requirements for the SynchroniCity "IoT Enabled Framework for Smart Cities" that will support the Digital Single Market to be implemented inside of the project. These requirements have been elicited from the system use cases (see Section 3) and refined through further analysis with the collaboration of the project partners. The requirements have been identified at high level without defining detailed features or technologies to be adopted for implementation: this approach has been followed in order to maintain technological agnostic system view: standards and technologies will be identified and detailed in WP2 during the design of the framework architecture. It is important to underline that the following requirements are related to the SynchroniCity framework core services and not to the pilot applications that will be defined and implemented in WP3.

The requirements, presented in the next paragraphs are described using the following set of attributes:

Title	*The title of the requirement.*
Category	*A high level classification of the requirement.*
ID	*The unique identification code for the requirement.*
Requirement Type	*Typology of the requirement:* *Functional: it is a requirement that expresses a functionality of the platform that will be directly used by a user (human or external system).* *Non-Functional: this type of requirement is related with platform features that are not specific behaviours or functions, such as performance, security and interoperability.*
Requirement Description	*The description of the requirement.*
Rationale	*Motivations that justify the need for the requirement in the context of the project.*
Priority	*The priority level for the implementation of the requirement:* *High: the requirement has high priority and has to be implemented in the first version of the platform.* *Medium: the requirement has medium priority and should be implemented in the final version of the platform.* *Low: the requirement has low priority and its implementation is optional.*
Notes	*Notes about relation with use cases or open issues to be solved.*

The requirements are classified in category based subsections. In particular the following categories have been identified:

- Marketplace
- Privacy
- License and Policies
- API
- SLA
- Models
- Monitor and feedback
- IoT

4.1 Marketplace

This category contains the requirements related to the Marketplace that should be provided by the SynchroniCity System. The Marketplace is a digital platform that should provide, to different types of end users, to search and access to different type of assets that are part of the SynchroniCity Digital Single Market (e.g. data, services, application).

Title	Marketplace Access				
ID	SR-MKTPLACE-01	**Category**	Marketplace	**Priority**	High
Requirement Description	The System has to provide a marketplace in which it is possible to register and sign up with different user roles (e.g. a city or a data/service provider, citizen, etc.)				
Rationale	The System has to allow the participation of all the actors interested in the DSM				
Notes	Related use cases: SUC-Asset-Discovery; SUC-Data-Source-Discovery; SUC-Data-Source-Registration; SUC-Device-Provisioning; SUC-Service-Registration; SUC-Solution-Discovery				
Requirement type	Functional				

Title	Asset publication procedure				
ID	SR-MKTPLACE-02	**Category**	Marketplace	**Priority**	Medium
Requirement Description	The system has to provide a validation procedure that has be follow to publish assets in the Marketplace				
Rationale	The marketplace provider wants to ensure the quality of published resources (e.g. in terms of documentation, availability, completeness etc.)				
Notes	Related use cases: SUC-Data-Source-Registration;				
Requirement type	Functional				

Title	Flexible revenue and pricing models				
ID	SR-MKTPLACE-03	**Category**	Marketplace	**Priority**	High
Requirement Description	The system has to provide different assets (e.g. data/service/application) usage revenue models (e.g. pay per use)				
Rationale	The marketplace should support a dynamic ecosystem in which providers can establish various business models.				
Notes	Related use cases: SUC-Data-Source-License				
Requirement type	Functional				

Title	Asset catalogue				
ID	SR-MKTPLACE-04	**Category**	Marketplace	**Priority**	High
Requirement Description	The System has to provide a marketplace in which it is possible to publish and search for different assets: services, data, providers and applications				

Rationale	Different types of providers (of data, services, applications) have to be visible on a large audience in order to provide their assets in the DSM
Notes	Related use cases: SUC-Asset-Discovery; SUC-Data-Source-Discovery; SUC-Data-Source-Registration; SUC-Device-Provisioning; SUC-Service-Registration; SUC-Solution-Discovery
Requirement type	Functional

Title	SynchroniCity compliance policy validation				
ID	SR-MKTPLACE-05	**Category**	Marketplace	**Priority**	Medium
Requirement Description	The System has to provide a set of SynchroniCity compliance policies for the developed solutions and it has to be able to validate them inside the marketplace.				
Rationale	Cities need to know if a solution, developed for another city/domain, can be adopted/reused quickly and without a lot of customization.				
Notes	Related use cases: SUC-Solution-Discovery				
Requirement type	Functional				

4.2 Privacy

This category covers aspects of privacy and data protection. For instance, the assurance that the data provided to third parties is not used for purposes other than those for which the end user was asked for permission.

Title	Privacy policies guidelines

ID	SR-PRIVACY-01	**Category**	Privacy	**Priority**	High
Requirement Description	The system has to provide procedures and guidelines in order to ensure compliance with respect to data protection rules				
Rationale	Both the data provider and the data consumer must comply with the privacy and data protection policy.				
Notes	Related use cases: SUC-Compliance-GDPR-DP; SUC-Compliance-GDPR-DC				
Requirement type	Functional				

Title	Data protection				
ID	SR-PRIVACY-02	**Category**	Privacy	**Priority**	Medium
Requirement Description	The systems should be able to properly react to data violations (e.g. data is accessed by unauthorized entities or other data breach) with defined procedures.				
Rationale	It is necessary to provide systems for monitoring against any attacks and if a breach occurs an appropriate procedure must be in place to handle it.				
Notes	Related use cases: SUC-Compliance-GDPR-DP; SUC-Compliance-GDPR-DC				
Requirement type	Functional				

Title	Anonymization				
ID	SR-PRIVACY-03	**Category**	Privacy	**Priority**	High
Requirement Description	The system has to provide data anonymization/aggregation functions in order to delete personal or restricted information coming from the data sources				

Rationale	It is necessary to have this type of functionalities in order to (re)use and publish data coming from different sources being compliant with privacy and data protection regulations.
Notes	Related use cases: SUC-Data-Cleansing
Requirement type	Functional

Title	Personal Data usage				
ID	SR-PRIVACY-04	**Category**	Privacy	**Priority**	High
Requirement Description	The system has to provide functionalities to allow the end user to control his or her own personal data, defining by whom and how it can be accessed.				
Rationale	End-user should have full control of his personal data				
Notes	Related use cases: SUC-Personal-Data-Processing				
Requirement type	Functional				

4.3 License and policies

This category is about the licenses and policies related to the use and access of data, services or applications within the marketplace. SynchroniCity strives to create an ecosystem where all possible business models are enabled. So, there is a need for maximum flexibility regarding the licensing and policy models that can associated with the assets.

Title	Data licenses definition				
ID	SR-LICENSE-01	**Category**	License	**Priority**	High
Requirement Description	The system should allow data providers to define different usage licenses for data sources/datasets published on the market place.				

Rationale	The marketplace should support a dynamic ecosystem in which providers can establish various business models.
Notes	Related use cases: SUC-Data-Source-License
Requirement type	Functional

Title	Customizable Licenses				
ID	SR-LICENSE-02	**Category**	License	**Priority**	Medium
Requirement Description	In order to ease the definition of data usage licenses, the marketplace should provide templates that can be easily customized to an intended business model.				
Rationale	The system should simplify the process related to licence definition allowing the reuse of existing models				
Notes	Related use cases: SUC-Data-Source-License				
Requirement type	Functional				

Title	Pre-built Licenses				
ID	SR-LICENSE-03	**Category**	License	**Priority**	Medium
Requirement Description	The system should provide data providers with predefined usage licenses.				
Rationale	To facilitate the publication process, providers should be able to use standard licenses (e.g., GPL, Apache, Creative Commons, etc.)				
Notes	Related use cases: SUC-Data-Source-License				

Requirement type	Functional

Title	Access policy				
ID	SR-POLICY-01	**Category**	Licence	**Priority**	High
Requirement Description	The system has to allow to define and manage policies for data/service access/usage				
Rationale	This function allows a data provider to restrict the access of its data source(s) to third parties.				
Notes	Related use cases: SUC-Data-Source-Access-Policy; SUC-Data-Source-License; SUC-Data-Source-Subscription; SUC-Service-Access-Policies; SUC-Service-License				
Requirement type	Functional				

4.4 API

This category concerns the management of SynchroniCity platform APIs. The goal will be to facilitate interoperability and support open standards with the aim of maximizing API adoption and usage.

Title	Standard and Open API				
ID	SR-API-01	**Category**	API	**Priority**	High
Requirement Description	The system has to allow to access/consume data through standard and open API/protocols				
Rationale	The adoption of standard and open API facilitates the reuse of solutions avoiding vendor lock-in				
Notes	Related use cases: SUC-Data-Source-Access;				

	SUC-Device-Management; SUC-Device-Provisioning
Requirement type	Functional

Title	Publish/subscribe data channels				
ID	SR-API-02	**Category**	API	**Priority**	High
Requirement Description	The system has to provide data publish/subscribe functionality				
Rationale	This function is requested in order to simplify and improve the process to send and receive data in the system				
Notes	Related use cases: SUC-Data-Source-Subscription				
Requirement type	Functional				

Title	Asset version management				
ID	SR-API-03	**Category**	API	**Priority**	High
Requirement Description	The system has to be able to track changes and version of API, datasets and assets in general				
Rationale	The function is required in order to avoid problem in the access to the resources.				
Notes	Related use cases: SUC-Data-Source-Access; SUC-Data-Source-Subscription; SUC-Data-Source-Discovery				
Requirement type	Functional				

Title	Resources status notification				
ID	SR-API-04	**Category**	API	**Priority**	High
Requirement Description	The system has to be able to notify the user when resources/assets are updated				
Rationale	The user should be notified about the asset status in order to avoid inconsistencies and problems.				
Notes	Related use cases: SUC-Data-Source-Access; SUC-Data-Source-Subscription				
Requirement type	Functional				

Title	Lookup assets				
ID	SR-API-05	**Category**	API	**Priority**	High
Requirement Description	The system has to provide asset search functionality api. In particular it should be possible to look-up for assets using different methods (e.g. a free text search; search with system filters;Tags;)				
Rationale	This function is necessary to simplify the access to the API in the marketplace				
Notes	Related use cases: SUC-Data-Source-Access; SUC-Data-Source-Discovery				
Requirement type	Functional				

4.5 SLA

In this section, we will establish the requirements for Service Level Agreements (SLAs). A SLA is a contract between a service provider and the end-user that allows to define the service level provided by the service provider. SLA specific purpose is to define the service that the customer will benefit from. SynchroniCity platform will provide the tools needed to manage, define and establish SLA.

Title	SLA management				
ID	SR-SLA-01	**Category**	SLA	**Priority**	High
Requirement Description	The system has to allow to define and manage extensible SLA for data access				
Rationale	Adopting SLA allows to offer different level of services for the different stakeholder that are part of DSM.				
Notes	Related use cases: SUC-Data-Source-SLA; SUC-Service-SLA				
Requirement type	Functional				

Title	SLA common metadata				
ID	SR-SLA-02	**Category**	SLA	**Priority**	High
Requirement Description	The system has to provide a common metadata to define SLA				
Rationale	Adopting common metadata models simplify the management and the comprehension of the SLA descriptions.				
Notes	Related use cases: SUC-Data-Source-SLA; SUC-Service-SLA				
Requirement type	Functional				

4.6 Models

This requirements category is related to the models necessary to define and describe the core assets of the marketplace and SynchroniCity platform. They are not to be confused with the models and metadata useful to represent the data sources that will be made available by the data provider.

Title	Asset description taxonomies				
ID	SR-MODELS-01	**Category**	Models	**Priority**	High
Requirement Description	The system has to provide pre-built taxonomies to describe assets (data, services, application, devices)				
Rationale	This function is necessary to simplify the definition of the assets description and to allow reuse of existing data models				
Notes	Related use cases: SUC-Asset-Discovery; SUC-Data-Source-Discovery; SUC-Data-Source-Registration; SUC-Device-Provisioning; SUC-Service-Registration; SUC-Solution-Discovery				
Requirement type	Functional				

Title	Standard and open data models				
ID	SR-MODELS-02	**Category**	Models	**Priority**	High
Requirement Description	The system has to support open and standard data models and metadata to describe the different assets of the marketplace				
Rationale	The adoption of standard and open data models facilitates the reuse of asset and solutions avoiding vendor-lock in				
Notes	Related use cases:				

	SUC-Data-Source-Registration; SUC-Device-Management; SUC-Metadata-Discovery
Requirement type	Functional

4.7 Monitor and feedback

In this section will be defined the requirements about the monitoring tools that the SynchroniCity platform will have to make available. Along with the feedback mechanisms the users have to be able to evaluate the utility, reliability, and characteristics of the assets they will use.

Title	Usage monitoring				
ID	SR-MONITOR-01	**Category**	Monitor and feedback	**Priority**	High
Requirement Description	The system has to provide advanced data usage monitoring functions				
Rationale	This function is necessary in order to enable other marketplace services (usage statistics, revenue models, technical management).				
Notes	Related use cases: SUC-Data-Source-Usage; SUC-Data-Source-Popularity;				
Requirement type	Functional				

Title	User Feedback collection				
ID	SR-FEEDBACK-01	**Category**	Monitor and feedback	**Priority**	High
Requirement Description	The system has to provide user feedback management for the different assets published on the marketplace				

Rationale	Feedback and rating mechanism are useful in order to facilitate the asset selection to the end users.
Notes	Related use cases: SUC-Data-Source-Popularity; SUC-User-Feedback
Requirement type	Functional

4.8 Device management

This section will define the requirements for the IoT management and the device networks that will collect data and provide data inside the SynchroniCity framework.

Title	Iot Devices management				
ID	SR-IOT-MGMT-01	**Category**	IoT	**Priority**	High
Requirement Description	The system has to allow to access/manage heterogeneous devices through a single common framework				
Rationale	Offer a uniform way to access to the different devices accessible in the marketplace is needed to overcome interoperability problems and facilitate the access reducing the need to deal with heterogeneous technologies				
Notes	Related use cases: SUC-Device-Management				
Requirement type	Functional				

5 Governance principles of the reference zones

In this section, we describe the process adopted to distillate principles for the governance of IoT and data infrastructure across different cities. The process is based on a collection of statements from city policy documents that outline governance ideas for urban IoT infrastructure and IoT data collected from it. Several cities contributed input including Antwerp (ANT), Eindhoven (EIN), Helsinki (HEL), Manchester (MAN), Porto (POR), Santander (SAN), and Carouge (CAR). Furthermore, a comprehensive list compiled by New York City (NYC) was also included in the analysis.

5.1 IoT infrastructure principles

We start by looking at governance principles around IoT infrastructures in cities and what precautions are taken to simulate its availability and use as well as compliance to personal data regulations. It analyses input and statements collected from all European SynchroniCity cities based on policy documents and public information available around their data portals. The statements concern IoT infrastructure principles alongside the following dimensions:

- Privacy
- Data management
- Openness of standards and interfaces
- Infrastructure
- Architecture
- Security
- Social responsibility
- Operation and sustainability

For each of the above dimensions, we examine the statements that the surveyed cities have provided and cluster them according to their underlying intention to identify:

- The intentions of the statements and how they can be categorized into underlying governance concerns
- How these concerns are currently being covered across different cities
- Whether cities have diverging or conflicting statements about these concerns
- Possible gaps currently not addressed by any city
- A candidate set of principles/recommendations that covers the required governance concerns

5.1.1 Privacy

The following high-level concerns can be identified:

- Generic statements relating to the importance of citizen privacy
- Statements that relate to transparency of the underlying processes and policies in how cities handle IoT generated data

- Statements that restrict what IoT data should be collected from an IoT infrastructure in a city
- Statements that refer to the compliance of IoT data handling with respect to laws and regulations
- Statements that refer to anonymization of personal identifiable data and its potential caveats
- Statements that outline conditions on how collected IoT data should be shared

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
Generic on citizen privacy		X		X				X
Transparency on process and policies on IoT data collection		X	X	X			X	X
Restriction to IoT data collection							X	
Compliance on IoT data handling		X	X			X	X	
Anonymization of personally identifiable IoT data		X		X	X	X	X	X
Conditions of sharing collected IoT data		X	X	X		X	X	X

Generic on citizen privacy
EIN covers the importance of privacy of citizens as a fundamental principle for IoT data collection. MAN and CAR state that citizen privacy is a legal obligation.

Transparency on process and policies on IoT data collection
NYC highlights the need to be fully transparent on processes and policies related to IoT infrastructure and data collection and to keep the public aware and up-to-date. MAN and CAR highlight in addition that this is required to nurture the trust of citizens. Both MAN and HEL make references to where their policies are online available. EIN demands that residents are given insight into the data that is collected and control over the way it is and will be used.

Restriction to IoT data collection
Only NYC defines more specifically constraint to when data collection from an IoT infrastructure should take place.

Compliance on IoT data handling
EIN, HEL and SAN, CAR, make clear that handling of IoT data must comply with existing law and regulations. NYC makes more explicit statements on how data should be classified in terms of privacy and its life cycle management in the system.

Anonymization of personally identifiable IoT data
EIN, NYC, SAN and POR argue for user related IoT data to be reliably anonymized before being publically accessible. POR even goes further by allowing for the anonymized participation of

stakeholders within an urban IoT data platform. Both POR and MAN highlight that anonymized data when inter-linked have the potential to be related to individuals.

Conditions of sharing collected IoT data
Cities made different statements regarding sharing of collected IoT data.

SAN and EIN aim to make all collected IoT data which is not personally identifiable accessible for use by 3rd parties. NYC mandates all public data sets to be accessible through its city portal.

HEL does not allow the sharing of any personal identifiable data to third parties and makes clear that any such information is collected for non-commercial use only.

In contrast, NYC and MAN support the sharing of personal identifiable data under certain conditions. MAN requires explicit user consent and data sharing agreements to be in place. NYC allows sharing only if a demand cannot be satisfied by other means (e.g. anonymised data) and necessary safeguards are in place.

5.1.2 Data management

The following high level concerns can be identified:

- Statements that refer to IoT data access through open APIs
- Statements that refer to access to relevant historical data
- Statements that outline how IoT data should be categorized
- Statements that refer to automation of audit checks for accuracy and validity
- Statements that refer to the protection and privacy of data

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
IoT data access through open APIs	X	X		X		X	X	X
Categorization				X			X	
Validation, verification, and versioning of data							X	
Automation of audit checks for accuracy and validity							X	
Data protection and privacy			X	X				X

IoT data access through open APIs
ANT, SAN, and NYC highlight the need for a central portal/repository/coordination to access IoT data. SAN and NYC state that IoT data should be accessible through open APIs. MAN proposes to use the CityVerve Data Platform and domain data stores – CKAN-based BT-provided Data Hub – to

make data available to applications and users of the platform in a standard way. EIN provides an Open data portal with an open API system for all parties who wish to share data. NYC argues that access should be limited when restricted by existing laws or regulations and/or when it compromises privacy or public safety. Only NYC states that, when useful, relevant business and historical data from the City or its partners should be made available and utilized by applications.

Categorization
NYC argues that desired measurements from any IoT system should be collected and categorized as efficiently as possible, using a few steps and/or manipulations if necessary. MAN states that all data sources and devices should be compliant with the Hypercat catalogue.

Validation, verification, and versioning of data
NYC highlight the importance of validation and verification (e.g., through redundancy in data collection and/or historical data) of each IoT device data set (e.g., temperature) and that the resulting master copy should be clearly labelled before it is used, aggregated and/or released. Moreover, versioning of data is required so that any updated data can be distinguished from the original and/or master copy. The retention and disposal policies for the master copy should be explicitly defined.

Automation of audit checks for accuracy and validity
Only NYC states that IoT data should be both audited and continuously monitored for accuracy and validity and that this process should be automated where possible.

Data protection and privacy
The importance of ensuring data protection and privacy is highlighted by HEL and CAR. MAN states that access to data will be primarily through access keys at the application level.

5.1.3 Openness of standards and interfaces

From the point of view of using open standards and interfaces the following aspects can be identified:

- Importance of standards in general
- Provision of data according to open standards
- Harmonization of metadata
- Use of APIs in data provision
- Modular approach enabled by interfaces and standards
- Ability to communicate with devices according to open standards
- Be involved of the development of standards
- Ability to adjust to new standards
- Documentation

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
Importance of standards	X	X	X	X		X	X	X
Provide data in standard formats		X	X	X		X	X	X
Metadata harmonization							X	

Use of APIs		X	X	X			X	X
Modularity	X	X				X		
Communication with devices based on open standards,	X							
Staying on track with new standards			X	X		X	X	X
Ability to adjust to new standards	X					X	X	X
Documentation			X					
SDKs for API users							X	

Importance of standards in general
Most cities recognize the importance of standards and APIs in enabling modular, interoperable multi-vendor platform development and reuse of services. POR: “Many cities are worried with this kind of dependency and are looking for alternatives.”

Provision of data according to open standards
NYC states that “IoT data should be collected and stored according to open standards, contain relevant contextual metadata, be exposed through open, standards-based application program interfaces (APIs).”

EIN: “Wherever available, the IoT infrastructure, connectivity, platforms, devices and services should be built on open or broadly agreed de-facto standards.”

Use of APIs in data provision
Mentioned by many cities.

Modular approach enabled by interfaces and standards
ANT: “By standardizing platform connections and modulation, multi-vendor modules can be implemented in the platform. Swift changes of modules are possible, when defect, or when another vendor improves a module.”

Ability to communicate with devices according to open standards
ANT: “This standardization of connections, hardware and software makes it possible to use multiple vendors, local or worldwide in multiple intercity implementations.”

Be involved in the development of standards
SAN: “Assure the maintenance of openness and standards by keeping track and following national and international standards. Federation of platforms identified as a useful instrument for this purpose.”

Ability to adjust to new standards
NYC recognizes the use of distinct and sometimes conflicting non-proprietary international, national, or industry standards for data and technology interfaces. In cases where standards conflict, the one that most closely aligns to the use case will be selected.

Documentation
Helsinki offers documentation via dev.hel.fi for the APIs.

SDKs for API users

NYC: “IoT data should [..] be exposed through open, standards-based application program interfaces (APIs), and be provided with software development kits (SDKs) where applicable so it can be easily shared or combined with other data sets.

5.1.4 Infrastructure

Making the cities more efficient and sustainable convey the need to deploy the appropriate technology for monitoring processes. Among such technology, IoT plays a capital role both improving legacy urban services and conceiving new ones. In this section some of the main remarks made by the cities in terms of infrastructure are presented and debated. Among them it is worth to highlight the ones below:

- IoT infrastructure has to be reusable for different services
- Avoiding vendor lock-in when choosing the solution
- The need of an inventory of IoT devices deployed in the city
- Adoption of a common protocol for deploying infrastructure in the city

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
Reusing IoT infrastructure	X	X		X	X	X		X
Avoiding vendor lock-in		X	X		X	X		X
Inventory of IoT devices		X				X	X	
Deployment protocol						X	X	
Leveraging on existing wired/wireless infrastructure				X		X	X	X
Basic principles in the use of public assets for the deployment of IoT infrastructure		X		X			X	
Resilience of the IoT infrastructure							X	

Reusing IoT infrastructure
The cities of ANT, EIN, MAN, POR, SAN, and CAR formulate in one or another way the relevance that IoT infrastructure has to multiplex different uses in the city context.

Avoiding vendor lock-in
In an explicit or implicit way EIN, POR, SAN, and CAR highlight the fact that IoT deployments have to avoid vendor lock-in.

Inventory of IoT devices
EIN, SAN and NYC refer to the need of managing an inventory of the deployed devices. Indeed, SAN supports the idea of having a self-management infrastructure framework.

Deployment protocol

SAN and NYC ask for the definition of a deployment protocol involving the relevant stakeholders.

Leveraging on existing wired/wireless infrastructure
MAN, SAN, NYC highlight the importance to rely on existing city communication network infrastructures when deploying the IoT infrastructure.

Basic principles in the use of public assets for the deployment of the IoT infrastructure
MAN and NYC refer to the use of public infrastructure (street lamps…) for placing IoT devices. NYC is even more concrete invoking to the principles of ownership and governance of such infrastructure. Both topics were heavily analysed by SAN in the past. EIN asks to re-use the public assets already available for placing IoT devices and recommends to make new assets available for sharing.

Resilience of the IoT infrastructure
NYC requests for infrastructure robustness which can fit extreme conditions such as flooding.

5.1.5 Architecture

Many of the cities concerns and their inputs with respect to the architecture dimension are quite related, thus some of the points are also related or are at least worth looking at in a broader context:

- Statements requesting a modular architecture to avoid vendor lock-in and support both legacy and future extensions
- Statements that relate to open standards and interfaces based on common best practices
- Statements requiring that a single specific technology cannot be the basis for the entire platform
- Statements pertaining to performance, stability and scalability

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
Modular architecture	X	X			X	X		
Open / standards based interfaces	X	X				X		X
Technology agnostic					X	X		X
Performance, stability and scalability	X				X	X		X

Modular architecture
EIN describes a modular architecture as its main principle for success, and POR has the same ideas but also has thinks containerized deployments using LXC/container technology should be thought into the design. POR has further described a microservice architecture that will support other interests like independent service deployments and a general technology decoupling.

ANT has called this ‘decoupled and distributed’ components, meaning that the architecture design supports ‘hot-plugging’ and replacement of components without interfering with rest of the system. ANT also sees this as a way to support both legacy and future developments, where multiple versions of services can coexist and new technologies introduced with ease.

SAN’s principles revolve around a modular architecture as it will help to support multiple technologies and avoid vendor lock-in.

Open / standards based interfaces
EIN has recommended that generic open interfaces and protocols are the core if the IoT platform, and ANT speaks both of open protocols/APIs but also standard formats for data exchange such as XML/JSON and SOAP/REST. The most important thing for ANT is that applications and systems integrators can easily consume and use the data that is available.

SAN is interested in the architecture supporting at least the open standards that are supported by large corporations.

Technology agnostic
POR wants the platform to be technology agnostic, enabling support for multiple programming languages while also staying vendor independent. SAN focuses their need on the ability to support early adoption of emerging technologies.

Performance, stability and scalability
POR focuses on performance principals, requiring the architecture to support large quantities of data and support dynamic scaling by adding more resources. ANT has the same concerns about performance but also wants this addressed by an architecture that support horizontal scaling whereby services 'grow' in accordance with the number of users / things attached to the platform. ANT also sees importance is stability and supporting the concept of self-healing deployments where failing services or changes in performance are automatically addressed.

SAN wants the platform to evolve from a 'Performance by design' paradigm, where performance can adapt to the deployment context as well as dynamic needs. SAN also warns not to invest too much time implementing performance optimizations, as new technology might make them obsolete.

5.1.6 Security

The following high level concerns can be identified:

- Generic statements relating to the security and reliability
- Statements that relate to security by design
- Statements about security of data in transit and storage
- Statements that outline access management, audit, responsibility and data control
- Statements about city policy

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
Generic on security		X			X			
Security by design	X				X		X	X
Data encryption and security frameworks							X	
Statements about data access, auditing, and management							X	
City policy							X	X

Generic on security
EIN covers the importance uses generic principles of reliability within the platform, derived solutions and services. POR notes the importance of documenting measures taken and the frameworks that are used to secure the platform. ANT realizes that IoT vulnerabilities are bound to exist in any system, as they do in ordinary IT solutions - therefore best practices from existing IT solutions should be reused.

Security by design
A notable principle presented by NYC is the 'Security by design' principle. Identifying and minimizing risks, limiting potential impact from threats and ensuring fast detection of weaknesses is key. POR extends this principle, and suggests active threat assessment should be done by attacking the platform to identify weaknesses.

ANT calls for using a threat model driven development as their main principle. This allows development to focus on areas where the risk is high, or where the impact in an unlikely event will be severe.

Both ANT and POR have principals about designing the system to comply with existing legal standards and use standard/proven frameworks to achieve this.

Data encryption and security frameworks
NYC is the only city to formulated principles about data security in transit, and security of the physical storage/servers.

Data access, audit and management
Identity and access management is a key principle described by NYC.

City policy
NYC has multiple principles that must be handled at a city level:

- The City has the right to restrict or revoke access to assets, devices, and public networks to protect the public interest and public safety.
- The City and its partners should engage in both audit-based and continuous monitoring to ensure that systems are working and that devices have not been compromised.
- Responsibilities related to security monitoring and the protection of IoT systems should be defined at a city level.

5.1.7 Social responsibility

The following section examines the statements of cities regarding the social responsibility of cities towards their citizens in the context of IoT infrastructure. The statements can be clustered into four themes:

- related to improving quality of life of citizens through smart service innovations enabled by IoT infrastructure deployments
- related to the role of co-creation of smart city services by citizens
- considering improving accessibility of city services
- how to increase the trust of citizens in IoT infrastructures and smart city services

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR

Improving quality of life of citizen	X	X				X		X
Citizen co-creation	X		X			X		X
Accessibility	X	X	X					X
Trust building with citizen			X	X				X

Improving quality of life of citizens
Several cities such as ANT and SAN outline their ambition of their smart city programmes to contribute to improved quality of life of their citizen and to improve economy and city operation. EIN recognizes explicitly that despite the positive ambitions of such technologies, unforeseen effects on society or individuals can occur. This raises the awareness of secondary effects that must be adequately taken into account in particular when providing new technologies and services, and collecting and combining data.

Co-creation
ANT, HEL, SAN, and CAR all recognize the importance of co-creation in order to ensure technical developments around emerging IoT infrastructure are more in line with citizen's needs and those of local businesses. ANT actively encourages citizen participation in co-creation by investing in the digital accessibility of its services and in the closing of the digital divide. Similarly, SAN policy is to reach all layers of society proactively and managing expectations through adequate communication.

Accessibility
Digital accessibility remains a concern as advanced technologies such as enabled IoT services become more commonplace in cities. ANT explicitly highlights the need for digital accessibility for more vulnerable target audiences and the inclusion of divergent sectors and groups of people. HEL argues that efficiency gains from increasing self-services and automation from IoT services can free up resources for helping citizens in need of personal assistance. EIN states that the IoT infrastructure should serve the needs of everyone in the city's public space, regardless of social position and income.

Trust building with citizens
When introducing game-changing technologies such as IoT, trust building with the citizens becomes critical to ensure a meaningful adoption of the technology. MAN have established a Privacy and Trust committee which will go beyond data protection requirements to ensure the delivery a trusted environment for developing services. HEL also emphasises the need for increasing transparency of city operation by publishing availability of services and decision making more prominently on the web, providing feedback channels to citizens.

5.1.8 Operation and sustainability

The following high-level concerns can be identified:

- Statements that refer to the need for a microservice architecture
- Statements that refer to the validation of performance
- Statements related to a sustainability model to ensure that service level agreements are met
- Statements that highlight the need for an analysis of benefits/outcomes prior to any device and solution deployment
- Statements that refer to the definition of data ownership and responsibilities
- Statements related to reusability, modularity, and flexibility requirements
- Statement related to the availability requirement

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	EIN	HEL	MAN	POR	SAN	NYC	CAR
Microservice architecture					X			
Validation of performance	X				X		X	
Sustainability model to ensure that service level agreements are met						X		
Analysis of benefits/outcomes prior to any device and solution deployment							X	X
Data ownership and responsibilities		X					X	X
Reusability, modularity, and flexibility	X	X					X	X
Availability and close to zero maintenance window	X							

Microservice architecture
POR highlights the need for a microservice architecture that uses containers (Dockers) for deployment. Quality assurance should be integrated into a continuous delivery pipeline, making sure that the development environment is as similar as possible to the production environment.

Validation of performance
POR state that the platform should be stress tested and the results documented and fed back to the development teams. This will ensure that the platform performs as expected in terms of resilience, ability to withstand attacks, ability scale horizontally by adding more resources. It will also help to detect and fix bottlenecks. The importance of automated testing is also highlighted by ANT to reduce regression and guarantee quality. NYC states that performance metrics should be maintained for solutions and that agreements should be terminated in the event that a solution does not perform.

Sustainability model to ensure that service level agreements are met
SAN supports the development of a sustainability model to check the level of service expectations and the demand related to business based or depending on provided data.

Analysis of benefits/outcomes prior to any device and solution deployment
NYC argues that demonstrated need, business case, and public benefit (e.g. economic, social, and environmental outcomes) should be required prior to deployment of any new IoT devices or solutions. In addition, proof of concept should be required prior to city wide deployments. The City

shall then prioritize access to its assets and public networks for IoT device deployments that are distributed in an equitable manner and have the greatest public benefit.

Data ownership and responsibilities
For all projects and associated contracts or agreements, NYC highlights the importance of outlining the "who, what, where, when, why and how" of the implementation, operations, risk management, knowledge transfer, and maintenance of IoT systems. This should include clear definitions related to system and data ownership and responsibilities. Concern about social responsibility is also highlighted by CAR and EIN.

Reusability, modularity, and flexibility
NYC states that solutions shall be designed to be flexible and responsive to evolving needs. It also highlights concerns about the reusability of infrastructures and components to develop solutions collaboratively. NYC, EIN, and ANT recognize the importance of modularity that allows continuous integration of new elements, prioritizing open standards where possible, to ensure interoperability and prevent dependency on a single vendor.

Availability and close to zero maintenance window
ANT highlights the importance of having the system 24/7 operational and a close to zero maintenance windows (software upgrades, firmware upgrades).

5.2 Open data principles

In the following, we focus on the governance principles around open data in cities and what precautions are taken to simulate its availability and use as well as compliance to personal data regulations. It analysis input and statements collected from all European SynchroniCity cities based on policy documents and public information available around their data portals.

The analysis is roughly broken down into two parts. Part 1 looks at statements concerning managing open data availability in cities. Part 2 looks at aspects related to personal data compliance.

5.2.1 Managing open data availability

This paragraph examines existing policies and recommendations that the surveyed cities concerning the release of open data and its use by third parties.

The following high-level concerns can be identified from the different statements made by the city:

- Generic statements relating to the public data ownership
- Statements that relate to the management of the release of open data
- Information about data formats, metadata and open data catalogues
- Recommended data licenses used in cities
- Statements that refer to how exploitation of open data by third parties is encouraged
- How users of open data can provide feedback on the data to the city authorities.

The table below shows where cities have correlating statements with the identified concerns. Each of the concerns will be briefly discussed in more detail.

Concern	ANT	END	HEL	MAN	POR	SAN	CAR
Ownership of public data	X	X					X

Managing open data release	X	X	X	X			
Formats of data and catalogues	X	X	X	X	X	X	X
Data licenses	X		X	X	X	X	X
Encouraging 3rd party exploitation	X	X	X				X
Feedback channel			X	X		X	X

Ownership of public data
EIN and CAR state that data in public spaces belongs to everyone. ANT states that open data should be the norm and the use and openness of data is applicable to data collected in the public domain, regardless the party that collects it.

EIN and ANT highlight the need of the city authority to always have visibility on the nature of data collected in the public space.

Managing open data release
EIN makes a more generic statement: data collected and generated in public space, including IoT data, should be opened up in a way everyone can make use of it.

HEL states that agencies and enterprises should promote the open and free distribution of information by making their public information reserves freely available.

ANT goes as far as applying open data principles to all data collected by the city and those commissioned to by the city from third parties. Furthermore, it uses open data principles as a default options for conversations around data with other stakeholders. It demands equal access to for all parties, e.g. by use of an open protocol. No technical or legal obstructions shall be made that hamper the access to the data.

Some cities define also a process by which data sets can be opened up and made public. MAN states that data set publication requires authorization by relevant information asset owner while data sets to be opened up will be based on demand by end users, thus, adequate engagement channels for this are to be provided. ANT states that prior to publication, city data will be screened by the chairman of the Lokale Integrale Veiligheidscel (LIV).

MAN provides important considerations around open data management by recommending: (i) a schedule about the publication of open data sets and (ii) clear versioning of updated data sets.

Formats of data and data catalogues
ANT and EIN state that opened up data should be made available unmodified in raw format.

Open data will be published in different data formats (SAN, HEL, POR), even proprietary formats will have to be expected (MAN), which may limit exploitation by third parties.

Metadata is important to facilitate better exploitation of open data (MAN, SAN, POR) and use of URIs make it more easily linkable to other data sets (MAN).

Clearly structured data catalogues available at appropriate locations support the discovery of published open data sets (SAN, POR, MAN).

Data license

The exploitation of open data should be facilitated by the publication of appropriate data licenses. Most cities (ANT, HEL, MAN, POR, SAN) use a localized version of Creative Commons Attribution License (CC BY).

Encouraging 3rd party exploitation
ANT, EIN and CAR propose that Data should available for both commercial and non-commercial (free of charge) purposes.

EIN and ANT take a proactive approach with third parties who contribute data in the city to encourage the creation of new revenue streams around them.

A proactive approach in encouraging exploitation of open data is also taken by HEL, which organizes regular meetings with the developer and entrepreneur community.

Feedback channel
Whenever open data sets are shared, it is good practice to provide a feedback channel to interested third parties to report issues with the data sets or provide comments around it. MAN, SAN and HEL provide such facility for error reporting and submission of comments and ideas. In addition, HEL monitors the use of APIs to obtain feedback regarding open data access. EIN provides feedback channels through its open data portal.

5.2.2 Personal data compliance

A further important dimension of open data is compliance to existing regulation when containing personal identifiable information. Our analysis of the policy documents and recommendation reveals three different categories:

- Personal data handling – how data containing personal identifiable information is treated before being utilized and shared with third parties
- Personal data storage – how personal data is stored in city platforms
- Exploitation of personal data – under what conditions data containing personal identifiable information can be exploited by third parties.

The table below shows how the examined statements from different cities map to the above identified concerns.

Concern	ANT	EIN	HEL	MAN	POR	SAN	CAR
Personal data handling	X	X				X	X
Personal data storage	X				X	X	X
Exploitation of personal data	X	X					X

Personal data handling
ANT, EIN and CAR agree that data that has personal identifiable information can only be used and processed in accordance with current privacy legislation. SAN states that data with Personal Information is governed under LPI.

Both EIN and CAR state that data that contains personal data can only be opened up and shared after adequate processing by mean of anonymization, thus preventing privacy issues. CAR and SAN

state also that personal data must be secured and stored within the state of Geneva and the City of Santander respectively.

While ANT states that data will be anonymized when there is a privacy or security concern, both EIN and CAR argue for user related open data to be reliably anonymized before being publically accessible.

Personal data storage
Several cities make explicit statements how and where personal data must be stored in accordance to current national and/or European laws.

ANT and EIN data that has privacy or security concerns can only be stored in accordance with current privacy legislation. SAN Data storage respects the current spanish law: it is collected and remains in City of Santander premises. CAR states that any personal data - storage and processing of these data should be performed according to the existing Swiss legislation preferably in the State of Geneva or in Switzerland. Public and cleated personal information may be stored outside of Switzerland. POR handles personal data in accordance with national and European laws, in particular, the Portuguese law number 122/2000 ("Decreto-Lei nº 122/2000", 04 July 2000).

Exploitation of personal data
ANT and EIN highlight that personal data being collected with necessary end user consent can be exploited in accordance to the end user agreement given with the consent. CAR goes more specific tackling the angle of data collected by a private entity. CAR states that data personal processing must be legal, cannot be treated against the will of the person, sensible data cannot be shared with third party, cannot be sent abroad, and must have the consent of the person to collect the data. On request by the person, the private entity has to share the data with the person. EIN states that data from the residents belongs to the residents; they are the owners and decide what happens to the data.

5.3 GDPR and PSI related principles

The project will abide to strict personal data protection policies in line with Directive 95/46/EC, the General Data Protection Regulation and the ePrivacy Directive. In this context, the following general principles shall be followed.

- **Lawfulness, fairness and transparency:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This usually entails that the data subject must give his/her free, unambiguous, informed, prior and demonstrable consent to the processing of his or her personal data for one or more specific purposes. Data subjects will be informed about the processing undergone by their personal data before the processing starts or, when data are not collected from the data subjects themselves, within a reasonable period, in any event no later than the first communication or the first disclosure to the public, when such activities are foreseen.
- **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization**: meaning that the processing of personal data must be the least intrusive possible, and that only personal data that are necessary for the envisaged purposes shall be collected and processed.
- **Accuracy**: Personal data shall be accurate and kept up to date; data subjects' rights of access, rectification, erasure, restriction, data portability and objection shall be ensured at all times.
- **Storage limitation**: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Integrity and confidentiality**: Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, through appropriate technical or organizational measures. The implementation of anonymization and pseudo anonymization techniques at each stage of the project will address confidentiality concerns regarding personally identifiable IoT information.
- **Data protection by design and default**: technical and organizational measures appropriate to the processing activities of the project (including data minimization and pseudo anonymization) will be introduced and implemented from the design phases of the project, and will protect data subjects' information without requiring any further action.
- **Accountability:** Accountability and compliance are part of the project requirements and will guide the architecture design, thus addressing transparency and compliance concerns. A dedicated data protection organization including data protection officers at the project level, reference zones and specific city stakeholder will overview the respect of these principles, carry out Privacy Impact Assessments where necessary and coordinate the implementation of Privacy by Design and by Default in each reference zone.

The Cities and the other bodies governed by public law will grant open access to the information they hold in accordance with Directive 2003/98/EC, known as the "PSI Directive", and its national implementing laws. The following principles apply.

- **Open data:** The project will follow a proactive strategy to make relevant non-personally identifiable data accessible, assessable and intelligible, usable for secondary purposes and interoperable. Personal data will be handled in conformity with the General Data Protection Regulation and will not be shared with third parties, except if a legal ground to do so exists.
- **Re-use:** All content that can be accessed under national access to documents laws is in principle re-usable beyond its initial purpose of collection for commercial and non-commercial purposes.

  ☒ By way of exception, content held by museums, libraries and archives is only re-useable if it is made available by the institutions for re-use.

  ☒ Re-use of information will be permitted without prejudice to personal data protection, as regulated by Directive 95/46/EC and Regulation 679/2016.

  ☒ Re-use of information will be permitted without prejudice to third parties' intellectual property rights.

  ☒ Conditions for re-use shall be non-discriminatory for comparable categories of re-use.
- **Charges for re-use** should in principle be limited to the marginal costs of the individual request (reproduction, provision and dissemination costs).

  ☒ Exceptions apply to museums, libraries and archives and to situations in which either the public sector body as such is required to generate revenue to cover a substantial part of the costs relating to the performance of its public tasks or situations in which such requirement applies to a specific piece of content ('document'). In such cases, the charges for re-use have to be limited at a ceiling calculated on the basis of actual costs.

  ☒ Public sector bodies need to calculate charges per re-user in a way so that the total income from charging does not exceed the costs incurred to produce and disseminate the information, together with a reasonable return on investment.

  ☒ Public sector bodies are encouraged to apply lower charges or to apply no charges at all. On request, public sector bodies must indicate the method used to calculate charges.

- ☒ Charges and other conditions for re-use have to be pre-established and published. If a request for re-use is refused, the grounds for refusal and the means of redress need to be explained.

- ☒ Requests for re-use shall be processed within a specific timeframe (20 days for standard cases).

- ☒ Licences should not unnecessarily restrict possibilities for re-use or be used to restrict competition.

- ☒ Where possible, the cities will use standard licences in digital format.

- **Prohibition of cross-subsidies:** If public sector bodies re-use their own documents to offer added-value information services in competition with other re-users, equal charges and other conditions must apply to all of them.

  - ☒ Public sector bodies may not enter into exclusive arrangements with individual re-users, excluding others. Two exceptions apply: Exclusive rights may be authorized in exceptional circumstances: (i) if they are necessary to provide services in the public interest; or (ii) in the context of digitization of cultural resources. In both cases, review clauses ensure that exclusive arrangements are regularly reviewed against the evolution of technology and the market for digitization and provision of electronic services.

6 Design guidelines and recommendations

This section provides a summary of recommendations for how cities should approach the design of IoT and open data infrastructures. The recommendations are derived from an analysis of the statements provided by the different cities in the previous section. They are based on an identification of common patterns found across cities and other useful good practice that individual cities have identified.

The recommendations follow the thematic grouping of statements used in section 5. First IoT infrastructure design recommendations are discussed, followed by those for open data infrastructure. Recommendations are numerically labelled according to the section number. In addition, they are prefixed (RI) if they relate to **I**oT infrastructure and (RO) if they relate to **O**pen data.

6.1 Recommendations regarding IoT infrastructure

6.1.1 Privacy

RI1.1: Citizens' trust should be built upon fair, transparent processes and policies related to IoT data collection by informing citizens through easily accessible channels and enabling citizens to make decisions about how their data is collected and used.

RI1.2: Cities should be explicit on the definition of purpose and restriction regarding IoT data collection.

RI1.3: Cities should implement privacy by design methodologies in order to enforce IoT data protection and be compliant with current national and/or European laws.

RI1.4: IoT data which contains personal identifiable information should be reliably anonymized before being publically accessible while following principles of data minimization and pseudonymization.

RI1.5: When cities share IoT data that does not contain any personal identifiable information with 3rd parties, it is good practice to be explicit on data formats supported and adequate data licenses should be defined.

RI1.6: When cities share IoT data that does contain personal identifiable information with 3rd parties, free, unambiguous, informed, prior and demonstrable user consent as well as its revocation, data sharing agreement and necessary safeguards must be in place.

6.1.2 Data management

RI2.1: IoT data should be accessible through open APIs. The access should be limited when restricted by existing laws or regulations and/or when it compromises privacy or public safety. When useful, relevant business and historical data should be made available.

RI2.2: IoT data should be categorized as efficiently as possible. Compliance with specific standard or catalogue is not enforced at this stage.

RI2.3: Security and privacy concerns should be addressed to protect data and restrict access to unauthorized users.

RI2.4: Each IoT device data set should be validated and verified. Accuracy and validity should be monitored continuously and automatically. Versioning of data can help to distinguish any updated data from the original and/or master copy.

6.1.3 Openness of standards and interfaces

RI3.1: Strive to utilize open interfaces both north and southbound.

RI3.2: Use established standards, aim for interoperability.

RI3.3: Provide a clear documentation of the APIs.

RI3.4: Provide SDKs or other tools to get started.

RI3.5: Design a life cycle and management model for APIs.

RI3.6: Ensure sufficient SLAs.

6.1.4 Infrastructure

RI4.1: Cities have to convey a consensuated demand in requesting for IoT open standards and other measures to prevent vendor lock-in.

RI4.2: It is desirable to agree on a common set of procedures for deploying, operating, managing and maintaining IoT infrastructure deployed in the cities. Additional issues such resilience or use of public infrastructures also have to be considered.

RI4.3: IoT infrastructure deployment has to be planned in a transversal way, that is, supporting as much as services as possible avoiding the silo approach.

RI4.4: Cities have to maximize the use of legacy wired/wireless infrastructures providing support to IoT based services and efficient (re)use of already available assets.

6.1.5 Architecture

RI5.1: A modular architecture design should be used in the development of both platform components and the IoT based applications and services that run on the platform.

RI5.2: Services and components should support deployment through container technology, which will increase the chances of services being adopted by cities. This also reduces the risks associated with deployment, and can greatly improve the development lifecycle.

RI5.3: Each service should be designed using both standards based and open APIs. This will make integration with individual cities easier and enable technology agnostic development.

RI5.4: Designing for performance and scalability has to be thought into the infrastructure services from the beginning. There exists no universal solution, but early usage analysis and designing for horizontal scalability from the beginning is highly recommended.

6.1.6 Security

RI6.1: A system for managing access must be in place, allowing for easy granting and revocation of rights and privileges to the platform. This is a key component, and the responsibility of managing this should be at a city level.

RI6.2: Security by Design means that security has been thought into all processes relating to both deployment and development of the software. It is highly recommended that threats to the system are analysed early and mitigated both through the overall systems architecture

design, but also at service level by using established best practices in code.

RI6.3: Use encryption and technology to secure data in transit and storage. It is highly recommended that all communication be secured through encryption, but also the risk of theft should be mitigated by encryption of physical storage/media.

6.1.7 Social responsibility

RI7.1: IoT infrastructures for smart cities should contribute to improve quality of life of their citizen, economy and city operation while taking into account secondary effects that could arise.

RI7.2: Cities should actively encourage co-creation by engaging citizens' and local business participation through adequate communication channel.

RI7.3: Cities should consider citizens' trust as a key success factor, providing both feedback channels to citizens and transparency of city operation, by publishing availability of services and decision making.

RI7.4: Digital accessibility should target divergent sectors and groups of people.

RI7.5: Cities should exploit the increase of self-services and automation from IoT services that can free up resources for helping citizens in need of personal assistance.

6.1.8 Operation and sustainability

RI8.1: The IoT enabled smart city platform should account for an automated tool to conduct stress tests and check its performance in terms of resilience, ability to withstand attack, ability to scale, and to detect and fix bottlenecks.

RI8.2: The platform should be flexible and responsive to evolving needs. It should be modular and also allowing the reusability of infrastructures and components.

RI8.3: All the projects and associated contracts should include clear definitions related to system and data ownership and responsibilities.

RI8.4: The platform should implement a microservice architecture.

RI8.5: The platform should include a sustainability model to ensure that service level agreements are met.

RI8.6: Cities should carry out an analysis of benefits/outcomes prior to any device and solution deployment and prioritize solutions having the greatest public benefits.

RI8.7: The system should be 24/7 operational and have a close to zero maintenance window.

6.2 Recommendations regarding open data infrastructure

6.2.1 Managing open data availability

RO1.1: A city who makes public data available as open data should provide a clear indication of ownership of the data to facilitate unambiguous exploitation.

RO1.2: Cities should take a proactive stance in opening up responsibly data from public spaces and ensure their access to third parties.

RO1.3: Cities should clearly describe the process by which public data is being released to foster the adoption of a responsible process across different departments.

RO1.4: It is good practice for data sets that evolve to provide a release schedule and adequate versioning to increase third party confidence in the data sets.

RO1.5: It is good practice to make supported data formats explicit to third parties including the format of meta-information about the data and utilized data catalogues.

RO1.6: In order to support efficient exploitation of opened up data by third parties, adequate data licenses should be defined.

RO1.7: Cities should pro-actively engage with entrepreneur and innovation communities to foster faster service innovation around these data sets.

RO1.8: Cities should provide adequate feedback channels to allow end users report on the quality and usefulness of opened up data sets and regularly check their use and popularity.

6.2.2 Personal data compliance

RO2.1: Cities should carefully consider existing national and EU legislation when processing and storing public data with personal identifiable information.

RO2.2: In order to open up personal data available in a compliant way, cities can either rely upon reliable data anonymization or through explicit end user consent.

7 High-level system view and guidelines

Upon the use cases described in Section 3 and the requirements elucidated in Section 4, a high-level view of the SynchroniCity digital single market platform is introduced in this section. Such an architectural overview is to be considered the basis for a more detailed architecture supporting the DSM concept that will be defined in WP2.

7.1 Reference zone main components and requirements

Figure 2 shows the logical overview of the Synchronicity DSM platform that highlights the macro-components providing the functionalities needed to address system requirements specified in Section 4. These components and their relation with system requirement - which are referenced using the notation previously defined (e.g., SR-XX-NN) - are briefly described in the following.

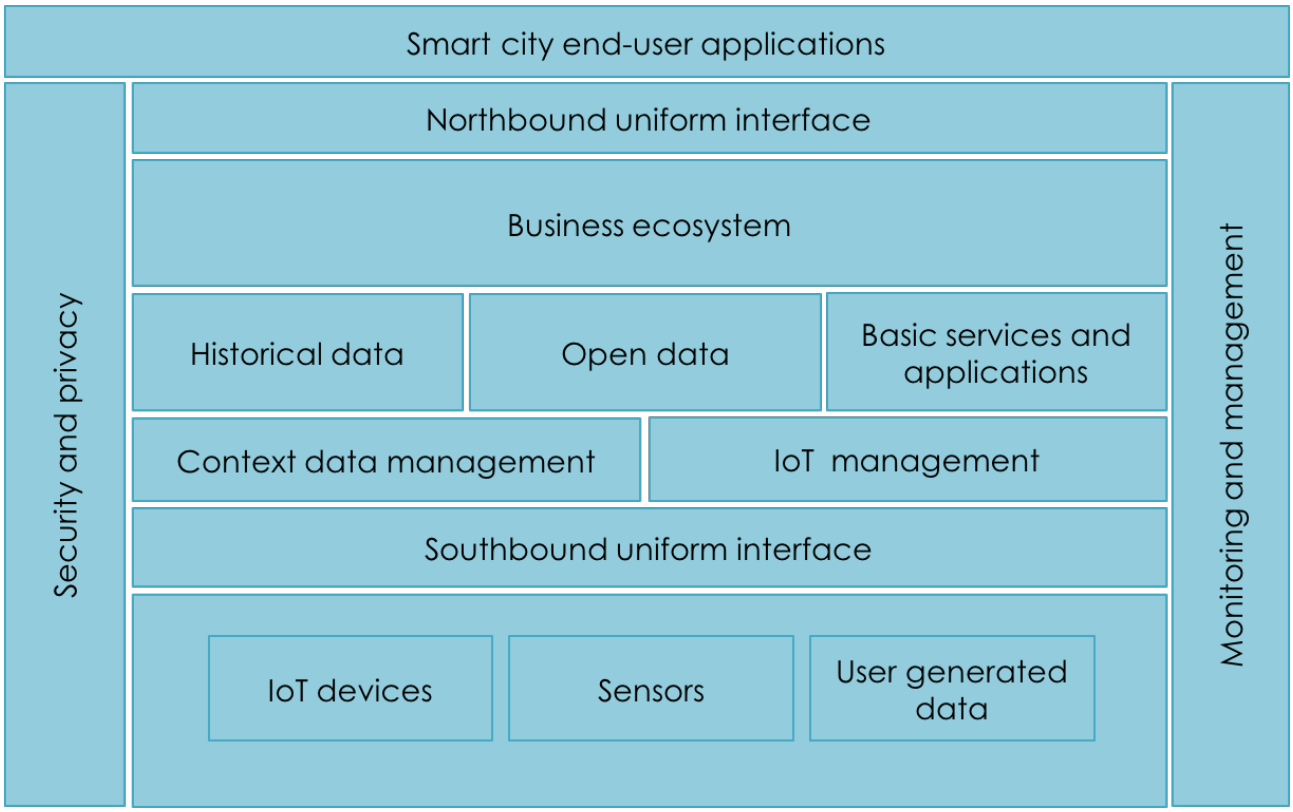

Figure 2. High-level view of the SynchroniCity digital single market platform.

Security and privacy and **monitoring and management** components provide cross-cutting services. Specifically, the first handles all the aspects related to authentication and authorization and provides tools to ensure privacy and protect access to personal and private information (SR-PRIVACY-XX, SR-MKTPLACE-01). The second offers monitoring and logging services to track the usage of data by third parties in accordance with SR-MONITORING-01 and SR-SLA-01.

Data sources (IoT devices, sensors, user generated data) within the RZs are conveyed within the SynchroniCity platform and exposed through the **southbound uniform interface** in order to be

accessed by the **IoT management** (SR-IOT-MGMT-01) and **context data management** (SR-API-01) components. The latter provide functionality to configure and manage the devices as well as to enable access to them in a uniform way using a publish-subscribe communication pattern (SR-API-02).

Data will be the core assets of the platform. They will be made available as contextual data, **historical data** (e.g., collection of IoT sensors data), or in the form of **open data** together with the **basic services and applications** (SR-MKTPLACE-04), which are provided by both the platform and third parties, and can be shared and reused through the business ecosystem.

The **business ecosystem** provides all the functionalities related to the asset catalogue (SR-MKTPLACE-04, SR-MODELS-01, SR-FEEDBACK-01) and the business aspects of revenue models (SR-MKTPLACE-03). It also exposes the observations of the RZ collected data through the **northbound uniform interface** (SR-API-01, SR-MKTPLACE-01). As such, appropriate APIs will be provided to ease the creation and orchestration of services and to enable the usage of the SynchroniCity platform functionalities by **smart city applications**, which will be defined and developed in WP3. The interface shall offer different ways to search assets in order to guarantee the maximum flexibility to the interested parties (SR-API-05). The business ecosystem shall include resource update mechanisms (SR-API-04) and will be also responsible for all the concerns related to the SynchroniCity policies validation (SR-MKTPLACE-05), licences definition and management (SR -DS-LICENSE-XX), and the procedures for asset publication (SR-MKTPLACE-02).

It is worth to highlight that the architecture illustrated above implicitly assumes the use open and standardized data models (SR-MODELS-02, SR-SLA-02) making straightforward the federation of RZs information resources. This is a compulsory step forward in adopting and consolidating the Digital Single Market.

8 Conclusion

To set out the groundwork of the SynchroniCity platform and later define its architecture, we first examined the existing challenges for realizing IoT enabled smart city services. Then we shaped the vision of the SynchroniCity digital single market for IoT-enabled urban services, by defining the desired properties that it should have in order to tackle them and create an ecosystem that improves the market confidence of IoT enabled smart city services.

In collaboration with city representatives, we conducted a stakeholder analysis to identify individual entities involved in the SynchroniCity DSM and their main interaction with it. Underpinning use cases were derived and described for each group of stakeholders by also identifying potentially high-profile tasks that require special attention. High level system requirements were elicited from use cases and further refined as a result of a joint activity among project partners. At this stage, the requirements provide a technological agnostic system specification as standards and technologies will be identified and detailed in WP2 during the design of the framework architecture.

An important part of the activity detailed in this deliverable was the distillation of principles for the governance of IoT infrastructure across different cities. To this aim, we first collected statements from eight cities based on policy documents and public information available around their data portals. Then we classified them according to their underlying intention, identified common concerns across different cities and possible gaps, and finally derived a set of recommendations that the SynchroniCity DSM platform should account for to address those concerns.

Finally, we introduced an initial high-level view of the SynchroniCity digital single market platform whose main components have been defined to address the system requirements. The architectural overview represents the basis for a more detailed architecture supporting the digital single market concept that will be defined in WP2.

Appendix A – Collection of use cases

Following is the collection of all the system use cases in alphabetical order. The forms have been filled in using a template, by city representatives and stakeholders in collaboration with cities.

ID	SUC-Asset-Discovery	
Use case title		
Asset Discovery Prior Procurement		
Use case objective		
Browsing, identifying and obtaining detailed information about already available assets (e.g. datasets, technologies, etc.), to be potentially used as building blocks for a particular required solution.		
Primary stakeholder		
The city		
Stakeholder perspectives		
Market place can be used as a single stop point for discovery of currently available assets. Information is made available in a structured fashion, in particular by using filters and tags, and adapted to its audience. This way, the time and complexity of asset discovery is decreased, as well as the tendency to give preference to local suppliers.		
Secondary stakeholder		
"Asset providers", e.g. IoT device operator, Service component provider, Data provider.		
Stakeholder perspectives		
"Asset providers" increase the visibility of their products and services by being present at the marketplace, and thus discoverable by cities, but may lose business opportunities by inadequate product information and/or specification.		
Use case narrative		
A given city wants to optimize the watering of its public gardens. To do that, the city needs to estimate the moisture of the soils or the rain levels nearby. The city browses the marketplace in search for assets that it can use in the procurement phase. For example, it can use an IoT provider that supplies sensors to be directly installed in the gardens and integrate the city's IoT infrastructure, or a dataset that contains information from pluviometers installed		

throughout the city. Both these assets should have been previously published in the marketplace by the IoT infrastructure provider or the data provider.
Barrier to be overcome in current practice
Current practice causes cities to incur in non-structured search for information and solution providers, that usually leads to proprietary solutions and information silos. Other barriers include: ● Lack of city marketplaces ● Heterogeneity of marketplaces, overcome by explicitly targeting cities ● Compliance issues, which are minimized because the assets on the market place are SynchroniCity compliant
Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Compliance-GDPR-DC

Use case title

Validate compliance with respect to data protection rules

Use case objective

What does the use case try to achieve for the primary stakeholder?

Ensure that the **data consumer** has complied with personal data protection rules

Primary stakeholder

Who is the primary stakeholder in this use case?

the data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

Participate to a smart city initiative focused on smart traffic management

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

the data provider

Stakeholder perspectives

Their benefits or possible conflicts?

Derive inferences from raw data provided by the data provider in order to develop a policy for efficient traffic management and safe circulation of vehicles within the city. The conflict here may be between the initial purpose of personal data collection declared by the data provider to the data subjects and the purposes pursued by the data consumer.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

UbiWhere, one of the SMEs in the SynchroniCity consortium (the data provider) has developed a multi-modal navigation app for citizens, that allows citizens to minimize end-to-end travel time and alleviates overall traffic hotspots in the city. The app makes use of different real time

information coming from IoT data feeds of traffic loops and parking sensors as well as live information from locations public transport vehicles and time tables.

Porto and the other cities (data consumers) ask UbiWhere to provide them with aggregated information on the traffic flow in certain zones of the city, the average time spent by citizens to cover some routes within the city and statistics about the number, the types and the location of accidents occurred within the city. The cities want to use this information to introduce a new urban policy for traffic management and road safety.

From a data protection standpoint, both UbiWhere and the Cities are autonomous data controllers. The flow of personal data from UbiWhere (the data provider-data controller) to the city (the data consumer-data controller) is a communication of personal data, unless data are anonymized; in the latter case, data protection rules do not apply.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

The cities wish to collect and process an aggregated elaboration of the citizens' personal data (data subjects) in discharging its public task. In doing this it shall:

- not require citizens' personal data from the data provider, but only aggregation thereof, in so far as this does not impinge on the achievement of the cities' public objectives;
- in case the collection of personal data is necessary, provide to the data subjects concerned some information on the elements of the processing that are not known by them (e.g. from which source the personal data originate and information on the new purposes for which that personal data are processed by the city); this information could be provided also on the city's website or by means of another suitable measure.
- ensure that purpose limitation principle is respected (i.e. personal data are not processed for purposes which are not compatible with the initial ones declared to the data subjects by the data provider).

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

High relevance on both the data provider and data consumer sides.

ID	SUC-Compliance-GDPR-DP

Use case title

Validate compliance with respect to data protection rules

Use case objective

What does the use case try to achieve for the primary stakeholder?

Ensure that the **data provider** has complied with personal data protection rules

Primary stakeholder

Who is the primary stakeholder in this use case?

the data provider

Stakeholder perspectives

Their benefits or possible conflicts?

Participate to a smart city initiative focused on smart traffic management

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

the data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

Derive inferences from raw data provided by the data provider in order to develop a policy for efficient traffic management and safe circulation of vehicles within the city. The conflict here may be between the initial purpose of personal data collection declared by the data provider to the data subjects and the purposes pursued by the data consumer.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

UbiWhere, one of the SMEs in the SynchroniCity consortium (the data provider) has developed a multi-modal navigation app for citizens, that allows citizens to minimize end-to-end travel time and alleviates overall traffic hotspots in the city. The app makes use of different real time information coming from IoT data feeds of traffic loops and parking

sensors as well as live information from locations public transport vehicles and time tables. The service has been launched successfully in Porto and now the company is thinking of expanding the service to other metropolitan cities in Europe.

Porto and the other cities (data consumers) ask UbiWhere to provide them with aggregated information on the traffic flow in certain zones of the city, the average time spent by citizens to cover some routes within the city and statistics about the number, the types and the location of accidents occurred within the city. The cities want to use this information to introduce a new urban policy for traffic management and road safety.

From a data protection standpoint, both UbiWhere and the Cities are autonomous data controllers. The flow of personal data from UbiWhere (the data provider-data controller) to the city (the data consumer-data controller) is a communication of personal data, unless data are anonymized; in the latter case, data protection rules do not apply.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Ubiwhere collects and processes personal data from the citizens(data subjects). In doing this it shall ensure that:

- information on the personal data processing have been provided to the citizens before they could download and use the multi-modal navigation app, including on the purposes of the processing;
- Specific consents have been collected from the citizens with regards to i) the storage of, or access to, information contained in the citizens' mobile (art. 5.3. of Directive 2002/58/EC) and to ii) the processing of the citizen's location data.
- Security safeguards have been applied to personal data (e.g. pseudonymization, encryption etc.)
- purpose limitation principle is respected (i.e. personal data cannot be processed for purposes which are not compatible with the initial ones).

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

High relevance on both the data provider and data consumer sides.

ID	SUC-Compliance-on-SLA

Use case title

Compliance on SLA

Use case objective

What does the use case try to achieve for the primary stakeholder?

Offering reliability towards the data consumer for both north- and southbound API's. Making sure that the 'SLA-south bound' (the weakest link) is able to provide enough ensurance for our own 'SLA-north bound'.

Primary stakeholder

Who is the primary stakeholder in this use case?

Marketplace provider

Stakeholder perspectives

Their benefits or possible conflicts?

Benefits:
Our position has to be strong enough to ensure a high standard of data quality to our consumers. There has to be a uniform way to check the different SLA's.

Conflicts:
We must make sure the weakest link is still strong enough to being able to provide our SLA to the consumer. If any SLA exist they possibly will have to be renegotiated.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

(Third party) data providers and consumers

Stakeholder perspectives

Their benefits or possible conflicts?

Benefits:
When a **data provider** is SLA compliant he will be able to connect more easily to the platform of all SynchroniCity members. This could lead to more leverage to the data provider his own contractor parties.

Consumers have the assurance that all data and services remain at a high level.

Conflicts:
Effort needed by all (sub) contractors. The consumers wanting a tighter SLA may have to settle with less.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

The City of Antwerp wants to disclose mobility data on its marketplace in a reliable way, so other stakeholders can make use of these data in order to be able to develop interesting applications exploiting the data. It wants to make sure the collected mobility data SLA's to third parties are standardized, i.e. easily understandable, easily comparable and inter exchangeable. The contract also makes sure the penalties, when not reaching the goals, are uniform.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Barriers:
- no SLA's (data and services are often provided on a best effort basis)
- non standard SLA's (not easily comparable)

Overcome
- by providing a SynchroniCity quality label where SLA's exist, creating standard SLA's where none exist.
- well documenting

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Compliance-on-Standards

Use case title

Compliance on Standards

Use case objective

What does the use case try to achieve for the primary stakeholder?

A way to be sure the delivery of data is compliant to generally accepted standards

Primary stakeholder

Who is the primary stakeholder in this use case?

Marketplace provider

Stakeholder perspectives

Their benefits or possible conflicts?

Benefits:

- When the connection is compliant then we are sure that the further handlings takes the least effort (way less error handling and management needed)
- Portability and interoperability

Conflicts:
When the third party is not willing to manage the reported errors or - even worse - when they can't or don't want to deliver the data in the standard way

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

(Third party) data providers, data consumers

Stakeholder perspectives

Their benefits or possible conflicts?

Benefits:
When using this standard they could possibly use this way to communicate to other providers or consumers (apart from our platform), i.e. portability and interoperability.

Conflicts:
Effort needed to get compliant

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

The City of Antwerp wants to disclose mobility data on its marketplace in a standardized way, so other stakeholders can make use of these data in order to be able to develop interesting applications exploiting the data. The city refers its data providers to the standards defined by SynchroniCity, and will execute the compliance check defined in the SynchroniCity project prior to publication of the data on the marketplace. Data consumers can now use standardized data from the marketplace.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Barriers:
- too many so called standards, unclear which ones to apply, let alone enforce towards data providers
- willingness to change

Overcome
- providing a SynchroniCity quality label for existing standards, define new standards where none exist
- well documenting

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Data-Cleansing
Use case title	
Cleansing data	
Use case objective	
What does the use case try to achieve for the primary stakeholder? Ensure that the data provider takes the necessary steps to cleanse his data, making sure that it doesn't contain any information that shouldn't be made available, such as personal data gathered from people who didn't explicitly consented to making it available.	
Primary stakeholder	
Who is the primary stakeholder in this use case? Data providers	
Stakeholder perspectives	
Their benefits or possible conflicts? Benefits: Data providers won't provide any information they weren't supposed to provide, ensuring they abide by the rules and laws in place. Possible conflicts: Some data may not be as useful if it's anonymized, aggregated or cleansed in any other way.	
Secondary stakeholder	
What other secondary stakeholders are part or affected by the use case? Data consumers who are use the data sources made available by the data providers.	
Stakeholder perspectives	
Their benefits or possible conflicts? Data consumers will be sure that the applications or services they build on top of these data sources won't provide any personal information that isn't necessary.	

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Porto's water management company would like to make some data available regarding people's home water consumption. The water company has hourly readings on water consumption for its users, but it cannot make that data available as is, since users did not give their consent to this, and making this data available might be problematic, since it would allow a data consumer to know if a given user was home for a given time period, for instance. However, the water company decides to aggregate this data, providing the water consumption totals and averages per day for the different areas in the city. This data is still useful for data consumers who want to build applications to find out how much water is being used by person in the city, and it does not compromise specific details about any given user.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Prioritization

How important is this use case perceived from different stakeholders perspective

TBC

ID	SUC-Data-Source-Access

Use case title

Access data

Use case objective

What does the use case try to achieve for the primary stakeholder?

A **data consumer** has implemented the API's for several data providers found on the SynchroniCity DSM - now the application has launched and access to the data is crucial.

Primary stakeholder

Who is the primary stakeholder in this use case?

Data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

The **data consumer** needs to be able to consume the data from the **data provider**, made available on the **marketplace provider**. The datasets could be downloadable files, data available through a REST API or data available on a message queue like Kafka or MQTT.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Marketplace provider, eg. city

Data provider

Stakeholder perspectives

Their benefits or possible conflicts?

The **data provider** and and **marketplace provider** both wish to provide easy access to their data sources. The **marketplace provider** must maintain the link/relation between the **data consumer** and the **data provider** so that the applications build will run with a high degree of stability. The **data provider** must be aware of services using the data, so that

updates and notifications can be sent to the **data consumer**. **Data consumers** must also be able to subscribe to news and updates related to data that is not actively being used.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Thomas has made an application that uses multiple data sources, that were found on the SynchroniCity DSM. The application uses both data sources providing real-time data via. MQTT and data from files that are updated less frequent.

One of the data providers has flagged an API as 'deprecated' and has published a new API and endpoint. Thomas is automatically notified of this change, and has time to implement the new API in his application.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- Level of documentation
- Quality of data
- Availability of data
- Security

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Data-Source-Access-Policy

Use case title

Provide a one liner

Define data access policies

Use case objective

What does the use case try to achieve for the primary stakeholder?

Define rules, procedures, and conditions according to which data resources of a data provider are made available to data consumers.

Primary stakeholder

Who is the primary stakeholder in this use case?

Data provider.

Stakeholder perspectives

Their benefits or possible conflicts?

Allow a data provider to restrict the access of its data source(s) to third parties, in order to guarantee the privacy or security of its data.

Disclosure of sensitive information to unauthorized users may lead to several issues for a data provider (e.g., identity theft, economic loss)

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Marketplace provider.

Stakeholder perspectives

Their benefits or possible conflicts?

The marketplace provider has to allow data providers to specify policies regulating the access to their data, which might contain sensitive information and must be protected by unauthorized access.

Disclosure of sensitive information may lead to reputational and economic issues for the marketplace.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Data provider *P* wants to expose bicycle tracking data for the local city council which can then use this information to build or reshape bicycle paths in the city in order to reduce traffic. After registering a set of data sources in the market place, *P* defines access policies which indicate who is authorized to access and use the data and with which modalities (e.g., access data only at specific times of the day)
Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it? ● Heterogeneity of devices and their purposes ● Liability of marketplace provider ● Compliance issues
Relevancy rating
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Data-Source-Discovery

Use case title

Discover data availability

Use case objective

What does the use case try to achieve for the primary stakeholder?

A **data consumer** wishes to build a new and innovative service, and chooses to browse the SynchroniCity DSM. The user should be provided with a search engine, giving search results based on for example tags, semantic information and free text search.

Primary stakeholder

Who is the primary stakeholder in this use case?

Data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

The **data consumer** needs to be able to find all available data sources on the SynchroniCity DSM. The challenge is that the **data providers** and **market providers** must allow easy discovery and consumption of data. Without this, the **data consumer** will go elsewhere for the data.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Marketplace provider, eg. city

Data provider

Stakeholder perspectives

Their benefits or possible conflicts?

The **data provider** and and **marketplace provider** both wish to provide easy access to their data sources. Either for altruistic purposes, or for monetary gain.

The more **data consumers** that use the specific data sources, the more publicity the **data provider** gets. This means that the **data provider** and **marketplace provider** must work together, to provide quality data/services to the **data consumer**.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Thomas is an independent app developer, and has an idea about showing environmental data to users, based on their current location, or a specific location on a map. The aim is to help prospective homeowners choose a good location to buy / build a home in an area with favourable environmental parameters. This could be air quality, water quality, noise pollution etc.

He searches the internet and finds the SynchroniCity DSM. He then searches for data providers/data sets containing environmental data in Denmark. He uses both keywords and natural language text to search through available datasets, and is able to navigate to the relevant data. As Thomas is an amateur app developer, the datasets he chooses are ones with good documentation and ones that are either frequently updated, or based on data streams.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- Achieving critical mass
- Level of documentation
- Quality of data
- Availability of data

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Data-Source-License

Use case title

Define data license for a new data source in marketplace

Use case objective

Configuration of appropriate data licenses of a data source provided by a **data provider** on the SynchroniCity market place

Primary stakeholder

Data provider

Stakeholder perspectives

Allows a **data provider** to define the terms of and conditions associated to the usage of a data source on the SynchroniCity market place. It defines possible license models and conditions for successfully obtaining them.

Secondary stakeholder

1. Marketplace provider, eg. City
2. Data consumer

Stakeholder perspectives

The **marketplace provider** may be interested in favoring data sources of specific license models based on the "philosophy" of the marketplace. A marketplace provider may also seek revenue share through certain license agreements with the data source providers.

A **data consumer** would like to clearly understand the terms and conditions around the use of data sources and chose from those that suit best his requirement and needs.

Use case narrative

Thomas has just successfully registered his AQ data sources on the SynchroniCity market place. He offers high quality data and would like to establish revenues streams for it.

In order to attract users, he offers a Fremium model and different premium models for the access of the data. The Freemium model grants end users access to all AQ data sources but on a down sampled stream of data of one reading per hour free of charge. This allows data consumers to "testdrive" the data offering and gain confidence in the use of the data for the intended purpose.

Data consumers who want unlock more accurate data beyond the one-month period can subscribe to a monthly flat rate license that provides access to the data at 5-minute reporting intervals. End users that want to exploit the data for commercial purpose must pay an additional fee, whereas use of the data for non-commercial purposes comes at lower costs. He also offers a pay-per-use license to that data allows 12 readings to be obtained within a 24-hour window whenever the user desires.

Thomas uses available templates for appropriate license models on the synchronicity market place and tailors them to suit the above characteristics. Interested data consumers are now able to learn about the T&C attached to it and what respective usage licenses are available and make the most appropriate selection.
Barrier to be overcome in current practice
● Define and discover suitable license models for exploitation of data sources ● License model flexibilities
Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Data-Source-Popularity

Use case title

Popularity of data sources

Use case objective

What does the use case try to achieve for the primary stakeholder?

A **data consumer** has can be actively involved in recommending data sources to other potential **data consumers** on the marketplace. It is an important part of the SynchroniCity DSM ecosystem, and helps **data providers** improve theirs datasets and **data consumers** find relevant data sets.

Primary stakeholder

Who is the primary stakeholder in this use case?

Data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

The **data consumer** has the ability to choose between multiple data providers that provide comparable data. **Data providers** and data sets are rated by **data consumers** and there is a feedback mechanism where **data consumers** can provide suggestions to **data providers**.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Marketplace provider, eg. city

Data provider

Stakeholder perspectives

Their benefits or possible conflicts?

The **marketplace provider** hosts a rating and feedback mechanism, where **data providers** receive feedback based on the quality of their data, API's, stability etc.
Use case narrative
Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place Thomas has been using a particular data set for a while now, and is very happy with the quality of the data and the support that he has received by the data provider. He therefore decides to give the data provider a 5 star rating on the SynchroniCity DSM, so that other users might be attracted to the data provider.
Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it? ● Level of documentation ● Quality of data ● Availability of data
Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Data-Source-Registration

Use case title

Register a new data source in marketplace

Use case objective

What does the use case try to achieve for the primary stakeholder?

Make a data source of a **data provider** available in the SynchroniCity market place, so it becomes discoverable by data consumers

Primary stakeholder

Who is the primary stakeholder in this use case?

Data provider

Stakeholder perspectives

Their benefits or possible conflicts?

Allows a data provider to expose its data source(s) to third parties, in order to generate revenue or derive other value from the use of it

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Marketplace provider, eg. city

Stakeholder perspectives

Their benefits or possible conflicts?

The marketplace provider may be interested in onboarding only trusted data sources

Onboarding “good” data source may lead to an increase in value of the market place

Onboarding “bad” data sources may lead to reputational issues

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Thomas wants to make air quality information from his IoT deployments in Østbirk available on the marketplace of its city, so third parties can develop interesting applications exploiting the data, e.g. AQ aware travel planner.

He visits the website of his municipality that exposes the marketplace, logs into his accounts and registers a set of data sources. During the registration his is requested to provide meta-information about them.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- Existence of marketplaces in cities
- Heterogeneity of marketplaces
- Process in the city / marketplace provider
- Liability of marketplace provider
- Compliance issues

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Data-Source-SLA

Use case title

Provide a one liner

Define data SLAs

Use case objective

What does the use case try to achieve for the primary stakeholder?

Define an official commitment between data provider and data consumer regarding the quality or availability of data.

Primary stakeholder

Who is the primary stakeholder in this use case?

Data provider.

Stakeholder perspectives

Their benefits or possible conflicts?

Allow a data provider to define data service level agreements (SLAs) which can be customized to specific consumers depending on their requested quality of service (QoS).

Different SLAs can generate different revenues for a data provider.

The definition of SLAs between a data provider and a data consumer should ensure the provisioning of data sources at pre-negotiated QoS. If the data provider is not able to meet its commitment, then it should refund the losses incurred by the data consumer.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Data consumer.

Stakeholder perspectives

Their benefits or possible conflicts?

A data consumer has the ability to request SLAs on the interested data sources with respect to its application requirements.

There is the need for a trusted system aimed to check data SLA compliance, which allows the data consumer to ask for refund in case the pre-negotiated commitment is not met by the data provider.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Data provider *P* wants to expose bicycle tracking data for the local city council which can then use this information to build or reshape bicycle paths in the city in order to reduce traffic.

After registering a set of data sources, *P* defines SLAs that a data consumer will be able to choose when subscribing to a specific data source owned by *P*. SLAs indicate QoS levels for different parameters (e.g., availability of end-to-end connectivity, response time, expected data arrival rate, MTBF, MTTR).

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- Liability
- SLA compliance

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Data-Source-Subscription

Use case title

Subscription to the data / API

Use case objective

What does the use case try to achieve for the primary stakeholder?

A **data consumer** has found one or more interesting data sets on the SynchroniCity DSM. He now wishes to subscribe to the data source, and receive updates when available.

Primary stakeholder

Who is the primary stakeholder in this use case?

Data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

The **data consumer** needs to be able to subscribe the data from the **data provider**, made available on the **marketplace provider**. The datasets could be downloadable files, data available through a REST API or data available on a message queue like Kafka or MQTT.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Marketplace provider, eg. city

Data provider

Stakeholder perspectives

Their benefits or possible conflicts?

The **data provider** and and **marketplace provider** both wish to provide easy access to their data sources. They must have an understanding about where data should be stored, who is responsible for data quality, retention, support and documentation.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity single market place

Thomas has found the datasources he needs on the SynchroniCity DSM, and now development of his app has started. He uses the API examples available on the SynchroniCity DSM to quickly develop an application prototype to show investors.

Some of the data sources require security information to access the API, but the SynchroniCity DSM provides infrastructure that handles access policies, form the data provider.

The investors see that the app uses the SynchroniCity DSM and know that the platform provides high availability, reliability and support.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- Level of documentation
- Quality of data
- Availability of data
- Security

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Data-Source-Usage

Use case title

Data Usage Monitoring

Use case objective

What does the use case try to achieve for the primary stakeholder?

To provide marketplace providers with the ability to check which one of the various data they are offering in the market results most successful and/or useful according to experimenters and users.

SynchroniCity platform could event suggest some potential useful services derived from that data usage records, which in turn would help stakeholders to outline their action plan.

Primary stakeholder

Who is the primary stakeholder in this use case?

Marketplace provider

Stakeholder perspectives

Their benefits or possible conflicts?

Allows market provider (e.g. city) to know the more demanded sources from its portfolio and adjust accordingly the offer, while at the same time can prepare tenders asking for services employing that data.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

SMEs, Developers

Stakeholder perspectives

Their benefits or possible conflicts?

Pick and develop potential business models related to that data which is so demanded.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

The municipality of Santander counts on a data usage monitoring system which helps it to know periodically which open data sets are the most demanded.

According to the results, citizens demand a new service around the buses schedule and routes, and creates an opportunity for SME's and freelance developers to give shape to a novel mobile application which serves to that interest.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

If the goal is exclusively monitoring, that is crude data not subjected to subjective views like would be the case of rating data. Anyway, it is necessary to develop a robust and reliable monitoring system that provides valuable results (e.g. distinguishing between total data usage and same-IP data usage)

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Device-Management

Use case title

Manage device in uniform way

Use case objective

What does the use case try to achieve for the primary stakeholder?

To illustrate the benefits of having a common set of management tools for device operation and maintenance.

Primary stakeholder

Who is the primary stakeholder in this use case?

IoT provider and system integrator

Stakeholder perspectives

Their benefits or possible conflicts?

The benefit is the existence of a “standard” way to access and manage IoT infrastructure.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Urban utility as IoT consumer, municipalities.

Stakeholder perspectives

Their benefits or possible conflicts?

The main benefit comes from the fact of having a simple framework which allows to manage the plethora of heterogeneous devices.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

Municipality A deploys IoT infrastructure (supporting different urban verticals) fitting the DSM framework in terms of IoT device uniform management. After some years, the Municipality A decides to outsource to a system integrator the operation and management of such infrastructure. The fact that such common framework exists will make “simple” the handover process.

Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it? At time being devices are managed based on a proprietary basis promoting vendor lock-in. Having such DSM clearly will overcome such barriers.
Relevancy rating
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Device-Provisioning

Use case title

Device provisioning

Use case objective

What does the use case try to achieve for the primary stakeholder?

To provide guidelines which help IoT device operator to better know how to perform the deployment of its devices within SynchroniCity context and specify how to include them in the device portfolio that future users will have access to.

Primary stakeholder

Who is the primary stakeholder in this use case?

IoT device operator (e.g. SME)

Stakeholder perspectives

Their benefits or possible conflicts?

Align with the platform standards and thus contribute to fulfil its goals.

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Cities, Data consumer

Stakeholder perspectives

Their benefits or possible conflicts?

To count on an additional data source from which obtain valuable data (e.g. environmental) which can serve to the purposes fixed in their experiments. Furthermore, and depending on the scope of the initiative, could even get physical access to a real piece of hardware.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

A little-known company located in Spain gets in touch with SynchroniCity representatives and decides to integrate some of their powerful IoT devices into their platform, feeding it with novel data.

SynchroniCity data consumers take a look into the device catalog, locate the new ones and choose to employ the data they are providing in their internal tests. After a trial process, and satisfied with the results, use this data in the services they are preparing for the municipality.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Different standards and data models increase complexity and make not easy for potential users try to employ certain IoT devices and their associated data.

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-Metadata-Discovery
Use case title	
Understand metadata (accuracy, description, history/length, license/conditions)	
Use case objective	
What does the use case try to achieve for the primary stakeholder? Enable data consumers to check metadata for the available data sources. This metadata consists on any information the data provider may find relevant to feed, such as a general description of the data, its measurements accuracy, the time intervals and periodicity of readings, conditions of use, etc.	
Primary stakeholder	
Who is the primary stakeholder in this use case? Data consumers	
Stakeholder perspectives	
Their benefits or possible conflicts? Benefits: Have a better understanding of the available data and its context, in order to ensure its correct consumption.	
Secondary stakeholder	
What other secondary stakeholders are part or affected by the use case? Data providers who are responsible for inserting this metadata	
Stakeholder perspectives	
Their benefits or possible conflicts? N/A	
Use case narrative	

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place Gervasio is looking for a data source to feed his smart traffic application in the city of Porto. In the city's portal, he can see all the data sources that may be of use for his application. After selecting a data source, he sees that the data provider has set some metadata about it, so Gervasio knows that this data is collected from some of the cities' traffic light sensors and that it represents the number of vehicles that crossed those lights every five minutes. He also knows that this dataset covers the central part of the city, and that it's updated hourly. This way, Gervasio can determine the best way to represent the information in his smart traffic application.
Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it?
Prioritization
How important is this use case perceived from different stakeholders perspective TBC

ID	SUC-Onboarding

Use case title

Onboard (3rd party) data / service providers

Use case objective

What does the use case try to achieve for the primary stakeholder?

To disclose (third party) data (e.g. on mobility) in order to provide it to data consumers. The data/services will be offered in a standardized way.

Primary stakeholder

Who is the primary stakeholder in this use case?

Marketplace provider

Stakeholder perspectives

Their benefits or possible conflicts?

Benefits:
Provide the data to other third parties in a standardized way, in order to generate revenue or derive other value from the use of it

Conflicts:
Reliability of the data(source); existence of (almost the same) data from different sources resulting in different content, ….

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Data providers, data consumers, e.g. city

Stakeholder perspectives

Their benefits or possible conflicts?

Benefits:
Many to Many instead of many bilateral contacts; data and development are being used effectively; trustworthiness of smaller third parties ;...

Conflicts:
Fear for competition between data providers; inappropriate use of the data; loss of position of power by sharing their data;

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

The City of Antwerp wants to disclose mobility data on its marketplace in a standardized way, so other stakeholders can make use of these data in order to be able to develop interesting applications exploiting the data. The city will agree with its departments (who are the data providers), on the terms and conditions, and license attached to the use of the data by the data consumers. It will disclose the data on its marketplace through standard API's.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Current practices vary: some cities have their own marketplace, others use 3rd party marketplaces or don't have a marketplace yet. Some cities only (want to) disclose city owned data on the city marketplace, others (want to) include data from 3rd party data providers.

Barriers:
- Pure data provider: business model
- mobility provider: external control
- other: absence of standardized data

Overcome
- Warranty: only pass through
- Not within this UC
- Description / best practises

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Personal-Data-Processing
Use case title	
Access information about personal data processing	
Use case objective	
What does the use case try to achieve for the primary stakeholder? Enable the citizens of different References Zone to access to the platform providing an overview of all personal data that is being collected and to whom this data is being shared	
Primary stakeholder	
Who is the primary stakeholder in this use case? Citizens/Users	
Stakeholder perspectives	
Their benefits or possible conflicts? Benefits: have a real and effective control over their data during the whole lifecycle of the project and have a repository for different types of data that otherwise would be lost. Possible conflicts: if personal data are not correctly stored and processed there can be a lack in terms of confidentiality and these can be used for different purposes not accepted by the stakeholders. Moreover, they should be in line with EU legislation with regard to personal data protection.	
Secondary stakeholder	
What other secondary stakeholders are part or affected by the use case? Every data collector taking track of personal data.	
Stakeholder perspectives	
Their benefits or possible conflicts?	

Being aligned with the legal framework to ensure personal data are processed in the correct way.

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

Giulia is participating in a pilot project that measures air quality in the city. She has signed in with her city account. On the Air-website she can login with those credentials to see the current status of the air quality in the city and her personal surroundings. In the 'my profile' page see has a live overview of all personal data that the systems have from Giulia.

Besides of personal data (name, address etc…) she sees also that the system collects GPS-data. In that settings page she has different options to manage her data to give her full control. She can not only edit or delete certain data streams, but she can also control who can also have access to each of the data. Her Giulia sees that the Smart Parking app of the City has request to get access to the GPS data to provide a better parking experience in the City. As Giulia is often confronted with parking issues, she would like to contribute and give access to the Smart Parking app to use the same GPS data

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- Liability of service provider
- Data protection issues on sensitive information
- Compliance with standards both at national and international level
- EU GDPR
- Defining 'personal data'
- Data transparency (especially in terms of data transferability)
- Transparency (trade off between 'pure' personal data and aggregated data)

Prioritization

How important is this use case perceived from different stakeholders perspective

TBC

ID	SUC-Service-Access-Policies

Use case title

Service access policies

Use case objective

What does the use case try to achieve for the primary stakeholder?

Defining access policies for the services catalogue in the SynchroniCity catalogue.

Primary stakeholder

Who is the primary stakeholder in this use case?

Service component provider or system admins

Stakeholder perspectives

Their benefits or possible conflicts?

As stakeholders, they will have the responsibility to define the rules and rights for the 3rd party developers to access the services

Secondary stakeholder

What other secondary stakeholders are part or affected by the use case?

Users who will access and integrate the services need to take into account of the access policies for services.

Stakeholder perspectives

Their benefits or possible conflicts?

Community will have the exact set of rules and policies for services that are exposed in the catalogue

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

As a service owner or a system admin I need to define the access policies for services that are exposed in the service catalogue in the marketplace

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Service-License

Use case title
License for service component provider
Use case objective
What does the use case try to achieve for the primary stakeholder? *Define a suitable software license which will grant specific rights to the service consumers*
Primary stakeholder
Who is the primary stakeholder in this use case? Service component provider
Stakeholder perspectives
Their benefits or possible conflicts? Chooses a suitable license for the service component
Secondary stakeholder
What other secondary stakeholders are part or affected by the use case? 3rd party developers or internal SynchroniCity services
Stakeholder perspectives
Their benefits or possible conflicts? Service users must rely on the license agreements and make sure that it is being adapted and used correctly.
Use case narrative
Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place Responsible/provider of service component defines a software license that needs to be mutually agreed and accepted by both parties(provider and users) so that these services can be used.

Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it? There are many types of open source license alternatives out in the Internet. One needs to choose and adapt this license methodology carefully
Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Service-Registration

Use case title
Register in service component catalogue
Use case objective
What does the use case try to achieve for the primary stakeholder? *Registering services which will be used as internal integration components in service catalogue in marketplace*
Primary stakeholder
Who is the primary stakeholder in this use case? Service developers(not 3rd party developers but by the SynchroniCity partners)
Stakeholder perspectives
Their benefits or possible conflicts? Community will have a service repository that can be used to integrate with the SynchroniCity platform
Secondary stakeholder
What other secondary stakeholders are part or affected by the use case? 3rd party developers will browse through the catalogue to access the services
Stakeholder perspectives
Their benefits or possible conflicts? From the secondary stakeholder perspective, the user will see a lot of services which might be hard to choose and use, so services should be well documented and listed

Use case narrative
Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place 3rd party user wants to integrate his application with the SynchroniCity platform, in order to do this, he needs to provision the application in the whole SynchroniCity platform, to achieve this he goes to service component catalogue in the marketplace and choose the appropriate service to integrate with his application
Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it? This case will ease the 3rd party developers to integrate into the platform with their applications which doesn't exist for now
Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Service-SLA

Use case title
Defining SLAs
Use case objective
What does the use case try to achieve for the primary stakeholder? Defining SLAs for each service in the catalogue
Primary stakeholder
Who is the primary stakeholder in this use case? Service owners or system admins who is responsible of these services
Stakeholder perspectives
Their benefits or possible conflicts? Service providers need to assure the minimum requirements for a service provided by themselves which are defined in SLAs

Secondary stakeholder
What other secondary stakeholders are part or affected by the use case? Consumers or 3rd part developers
Stakeholder perspectives
Their benefits or possible conflicts? Consumers or 3rd part developers who are interacting with the services, they expect to see all SLAs for a service has been fulfilled so that they can use these services as a baseline
Use case narrative
Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place As a service provider or system admin, I need to expose an identity service which acts as the entry point for all the applications, I need to make sure that the SLAs defined for this identity service must fulfill its obligations like uptime or response times etc.. If something goes wrong I need to adapt or replace the current service to make sure systems(built on this service) are working well
Barrier to be overcome in current practice
What is the current practice, existing barriers and how does the proposed use case aims to overcome it? SLA terms need to be defined for each type of service
Prioritization
How important is this use case perceived from different stakeholders perspective [different stakeholders can vote] TBC

ID	SUC-Solution-Discovery
Use case title	
Discovery of SynchroniCity Compliant Solutions	
Use case objective	
Browsing, identifying and obtaining detailed information about previously developed solutions that were deployed in other cities and thus are considered as SynchroniCity Compliant and can be replicated and/or adapted for use in other cities.	
Primary stakeholder	
The city	
Stakeholder perspectives	
Cities can find solutions for common problems in a faster and less expensive way by choosing from a catalogue of trusted SynchroniCity Compliant solutions (and not reinventing the wheel). Besides, cities can easily find solutions whose proof of concept has been previously demonstrated in other cities.	
Secondary stakeholder	
Service component provider	
Stakeholder perspectives	
Service component providers can have their previously developed (and proven) solutions advertised, thus having access to a digital single city market and benefiting from economies of scale by potentially replicating or adapting their solutions for use in other cities.	
Use case narrative	
A given city wants to deploy a city-scale noise monitoring system and browses the marketplace catalogue in order to obtain information about similar solutions which are operating in the other cities, and that were registered by the respective service provider.	
Barrier to be overcome in current practice	

Current practice causes cities to incur in non-structured search for information and solution providers, that usually leads to proprietary solutions and information silos. Other barriers include:

- Lack of city marketplaces
- Heterogeneity of marketplaces, overcome by explicitly targeting cities
- Compliance issues, which are minimized because the solutions on the market place are SynchroniCity compliant

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC

ID	SUC-User-Feedback
Use case title	
User feedback	
Use case objective	
What does the use case try to achieve for the primary stakeholder? To enable the citizens and users of SynchroniCity to send out user feedback on the systems deployed and tested in a specific reference zone for different purposes	
Primary stakeholder	
Who is the primary stakeholder in this use case? Citizens/Users	
Stakeholder perspectives	
Their benefits or possible conflicts? Benefits: enable users/citizens to provide feedback on the systems in place will generate effective services taking into account their needs and have a better solution in the end Possible conflicts: mismatch with expectations (potentially some feedback cannot be implemented and this can generate conflicts among citizens, users, municipalities and the technical staff)	
Secondary stakeholder	
What other secondary stakeholders are part or affected by the use case? Service providers	
Stakeholder perspectives	
Their benefits or possible conflicts?	

Benefits: to access to demand signals sent by the users in order to potentially gather feedback on how to improve services and systems already in place, or the need to develop new applications

Possible conflicts: requests from municipalities to technical staff can be different from the one of the users and would be difficult to define which changes have to be taken into account

Use case narrative

Please provide a brief concise description of the interaction of primary and secondary with the synchronicity digital single market place

William is living in Manchester and is using an application developed by company X in collaboration with the City for controlling in real time the parking slots available close to his home. He is going at home and the systems shows two parking slots available. However, when he arrives no parking slots are available anymore. He sends out a request to the application to implement predictive services that can provide a more reliable forecast. Maureen is also a frequent user of the Manchester parking application. However, lately she notices that the application is not responding when performing certain actions in the application. Via the in-app feedback mechanism she reports the issue. The helpdesk center has spotted the issue and notifies Maureen they are working on it.

Barrier to be overcome in current practice

What is the current practice, existing barriers and how does the proposed use case aims to overcome it?

- To put in place such a "customer service" approach requires huge expenses, the proper supporting mechanism and tools as well as additional research activities that often could not be put in place both by small companies, start-ups or municipalities, especially when the project is still in a development/validation stage
- Current mechanisms are often set-up in a one-way direction: from the user to the service. However, a feedback loop towards the user on how the feedback is being handled is required.
- The interaction among municipalities, technical staff and users requires relevant efforts in terms of time and translation of needs in effective services and/or applications, as well as to a good data-exchange between the various actors involved
- There is the potential risk that there is no follow up on the information and feedback captured from the users

Prioritization

How important is this use case perceived from different stakeholders perspective [different stakeholders can vote]

TBC