ICT - 288445

IoT6

Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability

Deliverable D1.1

IoT6 use-case scenario and requirements definition report

Version 1.0 – March 30 2012

Leading Partner: Mandat International (MI)
Report Date: March 30 2012

Contract Start Date: 01/10/11 Duration: 36 months
Project Coordinator: Mandat International (MI)
Table of Contents

[1] Executive Summary ................................................................. 4

[2] Introduction ............................................................................. 5
  2.1 IoT definition ...................................................................... 5
  2.2 IoT6 project in brief .......................................................... 5
  2.3 Work Package 1 on IoT6 architecture design ......................... 6
  2.4 Task T1.1 interactions ......................................................... 7
  2.5 Deliverable D1.1 objectives ............................................... 7


[4] Future IoT generic requirements ............................................. 11
  4.1 Call 1.3 requirements ....................................................... 11
  4.2 IERC vision and recommendations .................................... 11
  4.3 The IoT-A requirements ................................................... 13
  4.4 ETSI requirements .......................................................... 15

Sectorial requirements .................................................................. 20
  4.5 Domain-specific requirements ........................................... 20
    4.5.1 Building automation .................................................... 20
    4.5.2 Smart grid ................................................................... 22
    4.5.3 Telemedicine and e-health .......................................... 24
    4.5.4 Business process management tools .............................. 26

  4.6 Technology-specific requirements ....................................... 28
    4.6.1 RFID tags & Smart Things Information Service ............... 28
    4.6.2 Wireless sensor networks .......................................... 30
    4.6.3 Audio/Video components ............................................ 33
    4.6.4 Cloud computing associated with Software as a Service (SaaS) ... 33
    4.6.5 Safety and security .................................................... 34

[5] Surveys based requirements ..................................................... 35
  5.1 Smart IPv6 building end user requirements .......................... 35
  5.2 IoT6 Industrial Advisory Board (IIAB) requirements .......... 36
  5.3 Delegates survey – a specific end-user perspective on privacy .. 37
    5.3.1 Geographical repartition .............................................. 37
    5.3.2 Concerns regarding data protection ................................ 37
    5.3.3 Recommended actions .............................................. 38
    5.3.4 Expected services ..................................................... 38
    5.3.5 Innovation ............................................................... 38
    5.3.6 Data transmission ..................................................... 38
    5.3.7 Mobile phone use ..................................................... 39
    5.3.8 Data anonymity ....................................................... 39
    5.3.9 Data sharing motivation according to its finality ............. 39
    5.3.10 Privacy perception regarding personal localization .......... 40
    5.3.11 Privacy-related requirements .................................... 40

[6] Use-case scenarios ................................................................. 41
  6.1 Scenario design process ..................................................... 41
  6.2 IIAB inputs for the scenarios .............................................. 42
  6.3 Selected use-case scenarios to be tested and demonstrated .... 43
    6.3.1 Scenario 1 – Building maintenance process .................. 43
    6.3.2 Scenario 2 – Safety alert with QoS through IoT6 .......... 46
[1] Executive Summary

IoT6 is a European research project on the Internet of Things (IoT) and the Internet Protocol version 6 (IPv6). The IoT6 objectives are:

- to research the potential of IPv6 and related standards to support the future Internet of Things and to overcome its current fragmentation and lack of interoperability;
- to develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services;
- to explore innovative forms of interactions with multi-protocol integration, mobile and cellular networks, cloud computing services (SaaS), RFID and Smart Things Information Service, information and intelligence distribution.

The deliverable D1.1, IoT6 Use-Case Scenario and Requirements Definition Report, covers three main objectives:

I. To identify use-case scenarios to be enabled by the IoT6 architecture.
II. To identify the functional and technical requirements to be addressed by the IoT6 architecture.
III. To identify specific privacy concerns of delegates, taken as a group of potential IoT6 end-users.

This report has reviewed and taken into account different sources of requirements, including generic IoT related requirements, sectorial requirements, and specific IoT6 use-case requirements. The consideration of such various sources of requirements should enable us to design architecture suitable for a large range of future Internet of Things based applications and solutions. Based on these different sources of requirements, we have elaborated a list of 56 synthetic requirements to be addressed by the IoT6 project. These requirements provide a conceptual framework that will guide the IoT6 architecture design, including specification of IoT6 functions like network and communications, service layer and applications.

The report presents 5 selected use-case scenarios encompassing different domains: building maintenance process, safety alert with QoS through IoT6, mobility and surveillance, smart office, and a scenario elaborated by the European Commission related to a sick teacher. These 5 use case scenarios intend to illustrate various features to be developed by the IoT6 architecture. They have also enabled the fine tuning of the IoT6 synthetic requirements, as well as listing the key components and protocols to be addressed in the frame of the project.

Several end users groups have been taken into account, including the IoT6 Industry Advisory Board and a panel of delegates representing potential end-users of the IoT6 architecture. The survey with the delegates has confirmed the importance of personal data privacy and data ownership. This will be taken into account in the subsequent work packages.
[2] Introduction

2.1 IoT definition

The term "Internet of Things" (IoT) can be understood in different ways. We will take the definition mentioned in the « Internet of Things, Strategic Research Roadmap » [1]. According to it, the IoT is an integrated part of Future Internet and could be defined as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols. Here physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. In the IoT, “things” are expected to become active participants in business, information and social processes. Things are enabled to interact and communicate both among themselves and with the environment by exchanging data and information ‘sensed’ about the environment, while reacting autonomously to the ‘real/physical world’ events. Things will influence the real world by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these ‘smart things’ over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.” [1]

In other words, the IoT encompass all kinds of communicating devices, which tend to use different communication protocols and standards. It is concerning a larger and larger number of heterogeneous smart and communicating “things”. Their management will require highly scalable solutions able to overcome their heterogeneity and standards fragmentation. In this context, IPv6 constitutes an option to be further researched and explored.

2.2 IoT6 project in brief

IoT6 is a European research project on the Internet of Things (IoT) and the Internet Protocol version 6 (IPv6). The IoT6 objectives are:

- to research the potential of IPv6 and related standards to support the future Internet of Things and to overcome its current fragmentation and lack of interoperability;
- to develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services;
- to explore innovative forms of interactions with multi-protocol integration, mobile and cellular networks, cloud computing services (SaaS), RFID and Smart Things Information Service, information and intelligence distribution.

The main outcomes of the IoT6 project are some recommendations on IP features that can be exploited for the Internet of Things (with a specific emphasis on those unique to IPv6), an open and well-defined IPv6-based Service-Oriented Architecture. [2]
2.3 Work Package 1 on IoT6 architecture design

The objective of work package 1 (WP1) is to provide the architecture design and requirements that will be then used to drive activities in other WPs, including clear specifications for WP2 and WP3, and the formal architecture description to be used for the dissemination (WP8). Retro feeding loops will be provided to adapt and fine tune the design according to the developments made in the subsequent WPs. [2]

The work package is structured around two main tasks:

**Task T1.1 – IoT6 requirements and scenario definition.**
This task aims at specifying, analyzing and evaluating the IoT6 requirements, from both technical and conceptual points of view. The requirements will take into account future Internet of Things generic requirements as well as more specific sources or requirements, including sector specific, use-case based, and end-users defined requirements. The task will involve an end-user perspective and will identify their main concerns regarding their privacy in the frame of an IoT6-based smart-building environment. This task will also define specific use-case scenarios to be implemented in the validation phase. They must demonstrate the added value of the IoT6 architecture in integrating various components such as wireless sensor networks, the mobile phone network, RFID tags, building automation devices, Smart Things Information Services (STIS), Software as a Service (SaaS) and heterogeneous devices using different communication protocols.

**Task T1.2 – IoT6 architecture design.**
Based on T1.1, this task will design and describe the IoT6 IPv6-based service-oriented architecture to be developed in order to enable the integration and interaction among various components of the Internet of Things, and their integration with cloud computing applications (Software as a Service) and business processes management tools. It should tend towards a unifying (or integrating) framework over-coming the current heterogeneity and fragmentation of the Internet of Things. The work will lead to an IoT6 architecture design specification that will identify the main system components and their functionality, interaction patterns, interfaces, the underlying communications links and the ontology to be used in order to assure heterogeneous integration and provide interoperability among them. Security and privacy concerns will be included in this architecture design. In order to integrate the research project developments and results, the architecture will be reviewed and updated through iterative cycles during the whole project duration and be periodically published as a report. It will serve as a common reference document for the other WP developments, as well as for the dissemination work. This task will take into account the work developed by other research projects from the IERC cluster.
2.4 Task T1.1 interactions

The task T1.1 is directly interacting with the task on Architecture design (T1.2), as well as with the other WPs. It will among others influence the selection of devices and protocols to be addressed by the work package on “Multi-protocol interactions” (WP4), as well as the use-case scenarios to be implemented by the work package on “Integration, tests & validation” (WP7). The IoT6 synthetic requirements provided at the end of this Deliverable are high level requirements, which will guide the Architecture design in T1.2.

2.5 Deliverable D1.1 objectives

The deliverable D1.1, IoT6 Use-Case Scenario and Requirements Definition Report, covers three main objectives:

I. To identify use-case scenarios to be enabled by the IoT6 architecture.

II. To identify the functional and technical requirements to be addressed by the IoT6 architecture.

III. To identify specific privacy concerns of delegates, taken as a group of potential IoT6 end-users.

As mentioned in the IoT6 description of work, the IoT6 architecture development will require an iterative process. This deliverable D1.1 being prepared at the very beginning of the project, it is anticipated that certain sections of this deliverable may be updated and completed after Month 6 in order to take into account developments in other WPs.
The IoT6 consortium intends to develop and test an architecture able to interconnect the various segments of the future IoT together, including with virtual resources such as Software as a Service (SaaS), business process management tools, web services and mobile phone networks. This requires to consider three distinct sorts of networks:

- The global Internet (WAN) enabling worldwide interactions and integration with remote resources (SaaS, etc.).

- The local area networks, which are usually controlled by local operators or the end-users.

- The IoT networks, which may be IP-based (e.g. 6LoWPAN) or non-IP-based legacy protocols (e.g. ZigBee).

The IoT6 architecture will encompass and integrate these three sorts of networks. It will consider both IP and non-IP-compliant devices and will research different forms of legacy protocol integration. In such a context, it is important to stress that the requirements presented in this deliverable are targeting more specifically the IP-based part of the architecture. We cannot provide features such as Quality of Service (QoS) on already existing non-IP protocols which are inherently unable to support such services.

Fig. 2 – IoT Architectural scope

The usual approach to identifying requirements is to select several use cases, analyse them and derive requirements. In our case, this was not sufficient as the IoT6 project intends to develop an IPv6-based service-oriented architecture able to integrate heterogeneous resources across a rather fragmented IoT. If we would have limited our approach to extract our requirements from a few specific use cases, it could have generated too narrow and too specific a framework.

The chosen structure and methodology intends to provide IoT6 requirements that would be as relevant as possible for the future Internet of Things in its diversity and complexity. For this reason, we have started by considering various sources of IoT requirements for the future IoT, including requirements identified by other research projects. The use cases have been addressed in the second step, and have contributed to fine tune the generic requirements. Hence, the report voluntarily starts by exploring generic requirements, and progressively focuses on more specific ones. In this Deliverable we do not distinguish the requirements of the three domains of Section 2.5 separately. That will be done following the more detailed architecture and use-case scenarios of later Deliverables.

Several use-case scenarios have been identified to demonstrate the added-value of a cross-domain IoT6 architecture. They have been used also to identify complementary requirements, as well as a provisional list of devices and protocols to be addressed in the implementation and evaluation part of the project.

This deliverable IoT6 use-case scenario and requirements definition report has been structured in five sections:

A – Future IoT requirements analysis
This section reviews some mainstream sources of requirements for the future IoT. It takes into account various inputs, such as the IERC cluster vision and other research projects results (IoT-A, etc.). It intends to align the IoT6 architecture with generic requirements, which are anticipated for the future IoT.

B – Sectorial requirements
The Internet of Things is heterogeneous and spans across a number of application domains and technologies. Therefore, this section identifies specific requirements related to several sectors and will be taken into account in order to provide a multi-domain compliant architecture. Each project partner participated in the elaboration of specific requirements for each domain for which he has got the competences and the knowledge to precisely determine the requirements for a particular domain or technology.

C – Survey-based and end-users requirements
This section addresses the end-user perspective through different inputs: requirements proposed by the IoT6 Industry Advisory Board, the end-user requirements related to a project of “smart IPv6 building” led by Mandat International, and the results of a survey led in the frame of the IoT6 project, in which a panel of delegates has been interviewed, as potential end-users of the smart IPv6 building, in order to identify their key concerns regarding their privacy in the frame of an IoT6 and smart building environment.
D – Use-case scenario selection & requirements
This section presents a selection of use-case scenarios that will be analysed carefully to ensure that they can be accommodated by the architecture. Some of them will be implemented and used to evaluate IoT6 research results. These scenarios have been designed through a participatory process involving all the partners and including the IoT6 Industry Advisory Board (IIAB) members. The use-case scenarios intend to demonstrate the potential and added-value of an IPv6-based cross-domain architecture such as IoT6. The process to obtain these scenarios is explained in this section.

The selected use-case scenarios are utilized to identify complementary requirements, in order to fine tune the IoT6 synthetic requirements. The scenarios are also used to elaborate a provisional list of devices and communication protocols to be addressed by the research project.

E – Synthetic IoT6 requirements
The last section translates the findings of the previous sections into a set of synthetic requirements to be addressed by the IoT6 architecture. The requirements are selected according to their relevance for IoT6, taking into account the generic needs of the future IoT and the specific needs of the IoT6 project. The scope of the requirements has been aligned with the scope of the IoT6 project as described in its DoW. Requirements that would be out of scope have not been retained in this list. The synthetic requirements provide a conceptual framework, which will guide the IoT6 architecture design and development.

---

**Fig. 3 – D1.1 Sections interactions**
[4] Future IoT generic requirements

In order for IoT6 to develop an architecture that will be adequate for the future Internet of Things, we have decided to take into account several available sources of requirements, including:

- the FP7 call 1.3 requirements;
- the IERC vision on the future IoT;
- the requirements identified by the FP7 IoT-A project;
- the ETSI requirements.

4.1 Call 1.3 requirements

The European Commission FP7 call 1.3, to which IoT6 is related, includes a certain number of requirements to be addressed, including:

CALL.1) A coherent framework with open interfaces should be developed.

CALL.2) The system should cope with heterogeneity and maximize interoperability across providers and consumers of information and services.

CALL.3) The system should allow for re-use of object entities in the physical world across several application domains.

CALL.4) The system should enable integration with enterprise business processes.

CALL.5) The system should optimally manage a large population of resource-constrained devices.

CALL.6) The system should support self-management, self-configuration, self-healing properties, scalable look-up and discovery of IoT resources and services.

CALL.7) The system should integrate IoT into the service layer moving intelligence and service capabilities for filtering, pattern recognition, machine learning, decision-making towards the very edges of the network, up to users’ terminals and things.

CALL.8) There should be a secure and efficient distribution and aggregation of information.

CALL.9) A context-aware, reliable, energy-efficient, secure communication among networked objects located in diverse geographical locations, seamlessly connected, should be realized.

4.2 IERC vision and recommendations

The European Research Cluster on the Internet of Things (IERC) (www.internet-of-things-research.eu) intends to ease to coordination among European research projects related to the IoT. In March 2010, the IERC published a document of 230 pages under the title “Vision and Challenges for Realizing the Internet of Things” [3]. For the IERC cluster, the Internet of Things “will create a dynamic network of billions or trillions of wireless identifiable “things” communicating with one another. The Internet of Things has vision of ubiquitous computing and ambient intelligence. This will include a full communication and a complete computing capability among things and integrating the elements of continuous communication, identification and interaction. The Internet of Things fuses the digital world and the physical world by
bringing different concepts and technical components together." [3] The Internet of Things is “an integrated part of the Future Internet and could be defined as a dynamic global network infrastructure; with self-configuring capabilities; based on standard communication protocols. Here physical and virtual “things” have identities, physical attributes and virtual personalities; using intelligent interfaces; and are integrated into the information network.” [3]

From the IERC document, we can identify a set of key requirements for the future IoT:

IERC.1) Network of networks: The IoT will require a dynamic global network infrastructure, with the interconnection of the IoT into a common global IT platform of seamless networks and networked “things”.

IERC.2) Self-management and self-configuring capabilities: The IoT architectures should ease the self-configuration and self-management of “things”.

IERC.3) Heterogeneity compatible: The IoT architecture should be able to cope with a high level of heterogeneity, by enabling the combination of smart objects, sensor network technologies, and human beings, using different but inter-operable communication protocols.

IERC.4) Standard protocols: The IoT architectures will require a communication based on standard communication protocols.

IERC.5) Identification: The architecture should be able to provide “things” with identities, physical attributes and virtual personalities, including a Unique identification for each thing.

IERC.6) Scalability: The IoT architecture should be able to handle billions or trillions of wireless identifiable “things” communicating with one another, with an increased communication among terminals and data centers.

IERC.7) Two-way communication: Effective two-way caching and data synchronization techniques

IERC.8) Network-connected endpoints: Network-connected endpoints for virtual representations of the connected things and devices, which can be used for monitoring their location, condition and state, as well as sending requests and instructions to them.

IERC.9) Search and discovery services, enabling things to discover and explore each other and learn to take advantage of each other's data by pooling of resources and dramatically enhancing the scope and reliability of the resulting services.

IERC.10) Ubiquitous interactions: Allows people and things to be connected anytime, anywhere, with anything and anyone, ideally using any path or network and any service.

IERC.11) Virtualization: The IoT architecture should enable the virtualization and mapping of the real/physical world within the digital/virtual space.
4.3 The IoT-A requirements

The IoT-A European research project ([www.iot-a.eu](http://www.iot-a.eu)) is designing an architectural reference model for the interoperability of Internet of Things systems, outlining principles and guidelines for the technical design of its protocols, interfaces, and algorithms. It is designing corresponding mechanisms for the integration of IoT into the service layer of the Future Internet, as well as a novel resolution infrastructure, allowing scalable look-up and discovery of Internet of Things resources, entities of the real world, and their associations. The IoT-A project distinguishes two kinds of requirements: the functional requirements and the design constraints, which can be considered as technical requirements. The IoT-A deliverable D 6.1 [4] presents a complete list of requirements based on their partners’ inputs. Some of them are related to very specific applications. We have ignored those which were too specific, and focused on those which were in the scope of IoT6 research. The requirements of the IoT-A project retained are the following ones:

*Functional requirements:*

IoTA.1) The context of all things or tags should be monitored continuously for a given time slot.

IoTA.2) Every time and from any location the active collection of certain status information should be possible.

IoTA.3) Things should be integrated easily into cloud services.

IoTA.4) The system must allow queries for retrieving things capabilities.

IoTA.5) The system must allow things to collaborate between them for reaching a defined goal.

IoTA.6) The system should provide the semantics of an object.

IoTA.7) The system should allow an actor to create the semantics of an object.

IoTA.8) The system may enable a set of objects to exchange their semantics.

IoTA.9) The system should propose means to design applications based on the semantics carried by the objects.

IoTA.10) Rules based on time, location, consumption or any kind of criteria should be attached to an object and should conduct the behavior of the object.

IoTA.11) The system must allow the composition and/or aggregation of several objects in order to set up a new one.

IoTA.12) The system or parts of it should avoid interfering with the detection and measurements of very low voltage signals.

IoTA.13) All the radio transmitting parts should provide a real-time indication of radio transmission activity.

IoTA.14) All the radio transmitting parts should be instructed real-time to suspend or resume the radio transmission activity.

IoTA.15) The device should have a support for policy, event or schedule based communication.

IoTA.16) The system should have a support for routing of data based on content.

IoTA.17) Current secure messaging suites should provide a sufficient framework to handle trusted communication.
IoTA.18) The system should have support for ordered message delivery based on prioritized service handling.
IoTA.19) The system should have support for priority communication for time-sensitive services.
IoTA.20) The system should support integrity validation based on a trusted execution environment.
IoTA.21) The system should provide alarm signaling to indicate initialization failure.
IoTA.22) The system should provide support for secure storage of sensitive data.
IoTA.23) The system should have support for secure communication via secure protocols.
IoTA.24) The system should have support for secure time synchronization.
IoTA.25) Devices should have autonomous communication with the server via the telecommunication network, either at regular intervals, scheduled times, or based on some event.
IoTA.26) Information should be exchanged bi-directionally between the devices and the servers.
IoTA.27) Different smart IoT systems should be capable of interoperability with one another.
IoTA.28) Persons should be treated anonymously.
IoTA.29) Mobile phones should be usable.
IoTA.30) RFID tags should be placeable on consumer products.
IoTA.31) The mobile phone of the consumer should provide means to access both user profiles and value-added services.
IoTA.32) IoT-A must be able to provide the framework that will set the technological requirements and options to further develop applications based on IoT.
IoTA.33) IoT-A shall innovate in the definition of what an object is and in the relations we have with objects.
IoTA.34) IoT-A shall handle semantic interoperability.
IoTA.35) IoT-A must provide a novel resolution infrastructure regarding the naming, addressing and assignment of objects by using the interoperability.

**Technical requirements:**

IoTA.36) Easy and secure electronic access should be provided on all collected data for anything to the authorized bodies from any location.
IoTA.37) Smart systems should provide the basis for centralized or decentralized automated activities.
IoTA.38) The system should provide an API.
IoTA.39) The system shall support standard communications between objects.
IoTA.40) The system shall support standardization of object semantics.
IoTA.41) The system should have the ability for updating the software and performing other maintenance-type procedures.
IoTA.42) IoT-A shall work on normative aspects of the IoT.
4.4 ETSI requirements

The ETSI (European Telecommunications Standards Institute) is playing a leading role in M2M standardization. It has published a document named *Machine-to-Machine communications (M2M) - M2M service requirements* [5]. It presents which general and functional requirements are needed to facilitate the communication between the different kinds of machines in a global world. The goal of this technical specification is to enable a consistent, cost-effective, communication for a wide-range ubiquitous applications. Different domains are treated in this specification, such as smart metering, home automation, and e-health. The requirements described in the ETSI document can be split into different themes. The following list describes briefly the requirements appearing in the document issued by ETSI.

*General requirements:*

ETSI.1) *M2M Application communication principles:* The M2M System shall be able to allow communication between M2M Applications in the Network and Applications Domain, and the M2M Device or M2M Gateway, by using multiple communication means, e.g. SMS, GPRS and IP Access.

ETSI.2) *Message Delivery for sleeping devices:* The M2M System shall be able to manage communication towards a sleeping device.

ETSI.3) *Delivery modes:* The M2M System shall support anycast, unicast, multicast and broadcast communication modes. Whenever possible a global broadcast should be replaced by a multicast or anycast in order to minimize the load on the communication network.

ETSI.4) *Message transmission scheduling:* The M2M System shall be able to manage the scheduling of network access and of messaging.

ETSI.5) *Message communication path selection:* The M2M System shall be able to optimize communication paths, based on policies such as network cost, delays or transmission failures when other communication paths exist.

ETSI.6) *Communication with devices behind a M2M gateway:* The M2M System should be able to communicate with Devices behind a M2M gateway.

ETSI.7) *Communication failure notification:* M2M Applications, requesting reliable delivery of a message, shall be notified of any failures to deliver the message.

ETSI.8) *Scalability:* The M2M System shall be scalable in terms of number of Connected Objects.

ETSI.9) *Abstraction of technologies heterogeneity:* The M2M Gateway may be capable of interfacing to various M2M Area Network technologies.

ETSI.10) *M2M Service Capabilities discovery and registration:* The M2M System shall support mechanisms to allow M2M Applications to discover M2M Service Capabilities offered to them.

ETSI.11) *M2M Trusted Application:* The M2M Core may handle service request responses for trusted M2M Applications by allowing streamlined authentication procedures for these applications.

ETSI.12) *Mobility:* If the underlying network supports seamless mobility and roaming, the M2M System shall be able to use such mechanisms.

ETSI.13) *Communications integrity:* The M2M System shall be able to support mechanisms to assure communications integrity for M2M services.
ETSI.14) **Device/Gateway integrity check:** The M2M System shall support M2M Device and M2M Gateway integrity check.

ETSI.15) **Continuous connectivity:** The M2M System shall support continuous connectivity, for M2M applications requesting the same M2M service on a regular and continuous basis. This continuous connectivity may be deactivated upon request of the Application or by an internal mechanism in the M2M Core.

ETSI.16) **Confirm:** The M2M System shall support mechanisms to confirm messages. A message may be unconfirmed, confirmed or transaction controlled.

ETSI.17) **Priority:** The M2M System shall support the management of priority levels of the services and communications services. Ongoing communications may be interrupted in order to serve a flow with higher priority (i.e. pre-emption).

ETSI.18) **Logging:** Messaging and transactions requiring non-repudiation shall be capable of being logged. Important events (e.g. received information from the M2M Device or M2M Gateway is faulty, unsuccessful installation attempt from the M2M Device or M2M Gateway, service not operating, etc.) may be logged together with diagnostic information. Logs shall be retrievable upon request.

ETSI.19) **Anonymity:** The M2M System shall be able to support Anonymity. If anonymity is requested by an M2M Application from the M2M Device side and the request is accepted by the network, the network infrastructure will hide the identity and the location of the requestor, subject to regulatory requirements.

ETSI.20) **Time Stamp:** The M2M System shall be able to support accurate and secure and trusted time stamping. M2M Devices and M2M Gateways may support accurate and secure and trusted time stamping.

ETSI.21) **Device/Gateway failure robustness:** After a non-destructive failure, e.g. after a power supply outage, a M2M Device or Gateway should immediately return in a full operating state autonomously, after performing the appropriate initialization e.g. integrity check if supported.

ETSI.22) **Radio transmission activity indication and control:** The radio transmitting parts (e.g. GSM/GPRS) of the M2M Device/Gateway should be able to provide (if required by particular applications e.g. eHealth) a real-time indication of radio transmission activity to the application on the M2M Device/Gateway, and may be instructed real-time by the application on the M2M Device/Gateway to suspend/resume the radio transmission activity.

ETSI.23) **Operator telco capabilities exposure:** The M2M interface to the external M2M applications shall enable the exposition of telco operator capabilities (e.g. SMS, USSD, localization, subscription configuration, authentication (e.g. Generic Bootstrapping Architecture), etc.). The service platform shall be able to provide access to non-M2M resources abstracted as M2M resources to provide to the applications a consistent use of the M2M capabilities (e.g. to send an SMS to common cellular phones).

ETSI.24) **Location reporting support:** The M2M System shall be able to report M2M Device/Gateway location to M2M applications when this information is available. The location information of the M2M device/M2M gateway may be determined by the underlying network procedures (taking into account relevant privacy/security settings for transfer of such information), by application-level information reported from the M2M device/gateway application, or a combination of both.
ETSI.25) **Support of multiple M2M Applications:** The M2M System shall support a mechanism to manage a multiple M2M Applications and to provide a mechanism to interact between multiple M2M Applications.

**Management requirements:**

ETSI.26) **Proactive monitoring:** The M2M System shall be capable of proactively monitoring the M2M system in order to attempt to prevent and correct errors.

ETSI.27) **Diagnostics mode:** The M2M System shall provide the means to allow diagnostics for M2M Application functioning.

ETSI.28) **Connectivity test:** The M2M System shall support testing the connectivity towards a selected set of Connected Objects (COs) at regular intervals.

ETSI.29) **Fault discovery and reporting:** The Connected Object (CO) operational status shall be monitorable.

ETSI.30) **Fault Recovery by Remote Management:** M2M devices may support remote management for fault recovery e.g. firmware update, quarantine device. After this operation of firmware update, the device may reboot to a known and consistent state.

ETSI.31) **Service Level Agreement (SLA) monitoring:** M2M devices and M2M gateways that support SLA monitoring may record for example power outages (including the duration, start time and end time), and communication outages (including the duration of lost connectivity, the start time and the end time).

ETSI.32) **Pre-provisioning and auto configuration of the M2M Devices and Gateways:** The M2M Application or Capabilities in the Service Capabilities shall support auto configuration, which is without human intervention, of M2M Device or M2M Gateway when these are turned-on. The M2M Device or M2M Gateway may support auto configuration and registration to M2M Application functions.

ETSI.33) **M2M Area Network resilience:** An M2M Device or M2M Gateway experiencing a fault shall not affect the normal operation of the M2M Area Network.

ETSI.34) **Time synchronization:** The M2M System should support time synchronization. M2M Devices and M2M Gateways may support time synchronization. The level of accuracy and of security for the time synchronization can be system specific.

ETSI.35) **Configuration Management:** The M2M System and M2M Gateways shall support configuration management (i.e. manageability will depend on the end-system).

ETSI.36) **Charging:** The M2M System shall support the generation of charging information about the used M2M resources.

ETSI.37) **Compensation mechanisms:** The M2M System shall support the mechanisms required for secured and traceable compensation and micro-compensation.

**Functional requirements:**

ETSI.38) **Data collection & reporting:** The M2M System shall support the reporting from a specific M2M Device or M2M Gateway or group of M2M Devices or group of M2M Gateways in the way requested by the M2M Application.
Remote control of M2M Devices: The M2M System shall support the capability for an Application to remotely control M2M Devices that support this capability.

Group mechanisms: The M2M System shall support a mechanism to create and remove groups, and to introduce an entity into a group, modify the invariants (i.e. characteristics) of the members in a group, remove an entity from a group, list members of a group, check for an entity's membership in a group, search entities in a group, and identify all groups where the entity is a member.

Quality of Service (QoS): The M2M System should be able to make use of the Quality of Service (QoS) supported by underlying networks. M2M applications or service capabilities may use QoS capabilities of the underlying networks when implemented by the system.

M2M Devices/Gateways type varieties: The M2M System shall be able to support a variety of different M2M Devices/Gateways types, e.g. active M2M Devices and sleeping M2M Devices, upgradable M2M Devices/Gateways and not upgradable M2M Devices/Gateways.

Information reception: The M2M System shall support the different mechanisms for receiving information from M2M Devices and M2M Gateways.

Reachability: The M2M System may be aware of the reachability state of the objects.

Asymmetric flows: M2M Devices and Gateways should support asymmetric flows.

Path diversity: The M2M System should support physical paths diversity if required by the M2M Application.

Heterogeneous M2M Area Networks: The M2M System shall be capable of interfacing heterogeneous M2M Area Networks. This may be achieved at the M2M Gateway.

Information collection & delivery to multiple applications: The M2M System shall support the ability for multiple M2M Applications to interact with the same M2M Devices simultaneously.

Management of multiple M2M Devices/Gateways: The M2M Application shall be able to interact with one or multiple M2M Devices/Gateways, e.g. for information collection, control, either directly or through using M2M Service Capabilities.

M2M Devices/Gateways description: M2M characteristics of the M2M Device/Gateway may be either preconfigured in the M2M System or provided by the M2M Device/Gateways to the M2M System; the characteristics provided by the M2M Device/Gateways take precedence over the preconfigured characteristics.

Security requirements:

Authentication: The M2M system shall support mutual authentication of the M2M Core and the M2M Device or M2M Gateway, and one-way authentication of the M2M Device or M2M Gateway by the M2M Core. For example mutual authentication may be requested between a service provider and the entity requesting the service. The parties may choose the strength of authentication
to ensure appropriate level of security.

ETSI.52) **Authentication of M2M service layer capabilities or M2M applications**: When there is a request for data access or for M2M Device/Gateway access, the M2M Device or M2M Gateway shall be able to mutually authenticate with the M2M Service Capabilities or M2M Applications from which the access request is received.

ETSI.53) **Data transfer confidentiality**: The M2M System shall be able to support appropriate confidentiality of the data exchange. A particular M2M application may or may not require the use of such confidentiality.

ETSI.54) **Data integrity**: The M2M System shall be able to support verification of the integrity of the data exchanged.

ETSI.55) **Prevention of abuse of network connection**: M2M security solution should prevent unauthorized use of the M2M Device/Gateway.

ETSI.56) **Privacy**: The M2M System shall be capable of protecting privacy.

ETSI.57) **Multiple actors**: Multiple actors are involved in the end-to-end M2M service. The M2M System shall allow for such different actors to deliver the service in collaboration, maintaining security of the end-to-end service.

ETSI.58) **Device/Gateway integrity validation**: The M2M System shall be able to support a mechanism for M2M Device/Gateway integrity validation. The M2M Device/Gateway may or may not support integrity validation. If the M2M Device/Gateway supports integrity validation and if the device/gateway validation fails, the device/gateway shall not be allowed to perform device/gateway authentication.

ETSI.59) **Trusted and secure environment**: M2M devices that require device integrity validation shall provide a trusted execution environment. The Trusted Environment (TrE) shall be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE shall be unknowable to unauthorized external entities. The TrE shall perform sensitive functions (such as storing secret keys and providing cryptographic calculations using those secret keys) needed to perform M2M device integrity check and device validation.

ETSI.60) **Security credential and software upgrade at the Application level**: Where permitted by the security policy, M2M System shall be able to remotely provide the following features, at the Application level:
   a. Secure updates of application security software and firmware of the M2M Device/Gateway.
   b. Secure updates of application security context (security keys and algorithms) of the M2M Device/Gateway.

**Naming, numbering and addressing requirements:**

ETSI.61) **Naming**: The M2M System should be able to reach the M2M Devices or M2M Gateways using M2M Device Names or M2M Gateway Names respectively.

ETSI.62) **Identification**: The M2M System should support identification of COs or groups of COs by their names, temporary id, pseudonym (i.e. different names for the same entity), location or combination thereof (e.g. URIs or IMSI).

ETSI.63) **Addressing**: The M2M System shall allow flexible addressing schemes.
**Sectorial requirements**

The Internet of Things being quite heterogeneous, this section identifies specific requirements related to important sectors. Those specific requirements are taken into account in order to enable a multi-domain compliant architecture. We have selected a set of IoT related sectors, combining both technologically defined sectors and application defined sectors. The selection does not intend to be exhaustive, but rather a selection of key sectors to be taken into account, including:

- Building automation
- Smart grid
- Telemedicine and e-Health
- Business process management tools
- RFID tags & smart things information service (such as EPCIS)
- Wireless sensor networks (WSN)
- Audio / video components
- Cloud computing associated with Software as a Service (SaaS)
- Safety and security.

Each sector has been analyzed by partners in order to identify sector-specific requirements, including not only the mandatory ones, but also optional, but highly desirable ones that could help the development of the related sector. Each partner has been invited to research potential requirements such as:

- Required functionalities;
- Security requirements, including user authentication, data encryption and privacy;
- Quality of service (QoS) requirements, including data integrity, routing by priority and transmission confirmation;
- Addressing requirements, in particular the address format and the address length;
- Connection requirements (pull vs. push, synchronous vs. asynchronous, TCP vs. UDP);
- Discovery and lookup requirements.

### 4.5 Domain-specific requirements

#### 4.5.1 Building automation

With the evolution towards more and more pervasive intelligence in building environments, the building automation sector is encompassing a larger and larger set of components with a quest for increasing transversal interactions and scalability. Security and reliability are also key in particular in the area of access control and fire detection.

*Specific functionalities requirements:*

BA.1) Building automation system (BAS) devices using different technologies should be able to communicate with each other; this implies the interoperability between devices. [6]

BA.2) Building automation devices should interact with non-building automation devices. [7]
BA.3) Highly resource-constrained devices must be accommodated (battery-powered, low processing power, little memory).

BA.4) Location of devices should be an available, non-mandatory feature.

BA.5) Remote access to BAS installations should be possible. [8], [9]

*Addressing requirements:*

BA.6) BAS devices should be capable of being globally connected, linking different sites. [10]

BA.7) Support of a logical device address is required.

BA.8) To address multiple devices at once, group communication is desired.

BA.9) The mapping of BAS technologies, using a physical address scheme to an IoT addressing scheme based on IPv6, is required. [10]

*Security, authentication and privacy requirements [11]:*

BA.10) Only authenticated communication partners should be allowed to interact with BAS devices.

BA.11) Unauthorized access needs to be prevented.

BA.12) Only required data should be gathered from BAS devices.

BA.13) Security primitives need to be provided: confidentiality, integrity, non-repudiation.

BA.14) The privacy is relevant for specific use cases (e.g. no occupancy monitoring).

*Quality of service (QoS) requirements, including data integrity, priority routing, transmission confirmation:*

BA.15) Prioritization of messages for life-critical systems is required.

BA.16) Network dependability for security, safety applications should be very high.

BA.17) Low latency for lighting, entertainment areas, should be ensured.

*Data size requirement:*

BA.18) The IPv6 stack needs to be optimized for resource constrained BAS devices.

*Connection requirements [8][9]:*

BA.19) Synchronous and asynchronous communication needs to be supported.

BA.20) Publish/Subscribe communication should be supported.

BA.21) Client/Server communication should be supported.

*Management-related requirements:*

BA.22) Data logging (historic sensor values) should be supported.

BA.23) Management access to devices for parameterization/configuration/initial setup is required.
**Discovery and look-up requirements [12]:**

BA.24) Configuration/parameterization and engineering of communication links between BAS devices needs to be supported.

BA.25) Information models of various BAS technologies need to be integrated or mapped to a cross-domain ontology.

BA.26) Interfaces to mobile devices should be supported.

**Energy efficiency related requirements:**

BA.27) The BAS should be able to interact with the external environment, to take into account information such as peak demand on the electric grid or dynamic pricing.

### 4.5.2 Smart grid

The electric grid is as large as the Internet in terms of nodes. The smart grid constitutes a whole sector of development for the Internet of things with specific requirements.

![Smart grid diagram](Fig. 4 – Smart grid)


**Specific functionalities requirements [13]:**

SG.1) A Smart Grid Information System (SGIS) should be able to handle the prediction of electricity consumption of a given smart grid segment for the next N hours.

SG.2) A Smart Grid Information System (SGIS) should be able to handle the prediction of electricity production of a given smart grid segment for the next N hours.

SG.3) SGIS should take care of peak load shifting of renewable production sources:

   a. The production may quickly reach to zero in few seconds (for instance if a cloud hide the sun).
b. In case of over production, SGIS should be able to avoid energy loss and regulation of network voltage.

SG.4) More generally, SGIS should provide peak shaving and voltage control services, as well as energy arbitrage.

SG.5) Smart Grid should be consumer oriented without new costs => Prosumer.

SG.6) SGIS should be able to support, addressing and managing of Virtual Power Plants.

**Addressing requirements [13]:**

SG.7) Information should be able to cross boundaries and be routed between the different levels of a Smart Grid: from transmission grid to distribution grid to micro grid and reverse.

SG.8) Local handling of information should be available.

**Quality of service (QoS) requirements, including data integrity, transmission confirmation [13]:**

SG.9) Latency of communication should be very short at micro-grid level.

SG.10) The privacy of the consumer must be guaranteed.

SG.11) Only authorized stakeholders should be able to access information generated from micro-grid level.

SG.12) SGIS should offer end-user information and participation by an instantaneous transmission without delay from a source node to a destination node.

SG.13) High availability of energy supply is critical: fall-back solution to ensure the proper functioning of important devices should be ensured (for example health impact due to a freezer disabled during many hours would break the cold chain).

**Management-related requirements [13]:**

SG.14) Smart-grid components should be able to be managed as virtual entities.

SG.15) SGIS should take care of consumers and end users (how will the energy industry move from energy product-driven to energy service-driven?).

**Discovery and the lookup requirements [13]:**

SG.16) Smart meter and others micro-grid devices should be able to support a kind of Plug &Play in order to be accepted by consumers.

**Cross-domain interactions requirements [13]:**

SG.17) SGIS be able to cooperate with other kinds of information system (weather forecast, production plants, etc.).

SG.18) SGIS should be integrated with a software solution for Business Process Management.
4.5.3 Telemedicine and e-health

E-Health & telemedicine are terms for clinic healthcare supported by electronic processes, telecommunication and information technologies at a distance. These help medical service to eliminate distance barriers and be able to improve accessibility, so medical service can be consistently available in rural area. The typical use cases are remote monitoring, therapy intervention. For supporting these, the system needs to provide ubiquitous computing, medical sensor, network infrastructure, authentication, context-awareness, QoS. So, the following requirements are derived.

![Patients Status Report](image1)
![Patients Tracking](image2)

![Patients Monitoring](image3)

![Remote Healthcare](image4)

![IoT Infrastructure](image5)

Fig. 5 – Telemedicine and e-health services with IoT infrastructure

Specific functionalities requirements [14]:

EH.1) An eHealth system needs to support remote monitoring (e.g. monitoring elderly persons’ status).

EH.2) An eHealth system needs to provide reporting service for doctor and family (e.g. reporting elder persons’ abnormal status).

EH.3) An eHealth system needs to support therapy intervention (e.g. remote diagnosis service).

EH.4) An eHealth system needs to support context-awareness such that predicting the users’ intentions and automatically adapt to a changing environment.

EH.5) All devices and sensors for an eHealth system need to communicate seamlessly with each other without requiring complicated user intervention.

EH.6) Technical aspects of the network mechanisms need to be hidden from the patient and the applications by means of solutions as well as service discovery and management.

EH.7) An eHealth system needs to support heterogeneous devices and networks consisting of a variety of different mobile and stationary devices, wireless technologies and networks.

EH.8) An eHealth system needs to support energy-efficient operations of mobile devices.
**Security, authentication and privacy requirements [14]:**

EH.9) The eHealth system needs to protect personal or monitored information from unauthorized entities.

EH.10) The system needs to support privacy by controlling shared personal resources, services and contents with others using commonly agreed rules.

EH.11) The system needs to protect sensitive personal information such as the vital signals of a patient and the location of the user.

**Quality of service (QoS) requirements, including data integrity, transmission confirmation [15]:**

EH.12) Some eHealth applications require end-to-end quality of service (QoS) while mobile devices (e.g., patient’s sensors or doctor’s smart phone) are moving.

EH.13) An eHealth system needs to be provided with high quality of data (e.g., accuracy of context of physical environment, patient, etc.).

EH.14) An eHealth system needs to provide urgent event notification without delay if patients are in emergency condition.

**Management-related requirements [14]:**

EH.15) An eHealth system needs to provide seamless mobility management of end-user devices.

EH.16) An eHealth system needs to provide self-configuration for ease of use.

EH.17) An eHealth system needs to provide self-healing in order to provide high availability of the system.

**Discovery and the look-up requirements [14]:**

EH.18) An eHealth system needs to be provided with discovery service about an item which has a tag to help persons who need to be monitored.

EH.19) An eHealth system needs to be provided with the current location of persons who need to be monitored.
### 4.5.4 Business process management tools

Business process management (BPM) is defined as a management discipline that treats business processes as assets that directly improve enterprise performance by driving operational excellence and business agility.

For performance, the best BPM tools should have a workflow engine that allows automation of key business processes in the organization. Automation can save time and money for critical processes. Using business process analysis, we can improve the performance of business process model and reduce the cost. In order to facilitate this, a BPM tool should support several interfaces to access the data that can be used for various parts.

![Fig. 6 – The concept of business process model (BPM) tools](image)

**Specific functionalities requirements [16]:**

BPM.1) A BPM tool needs to be provided with an expansion of business process through global connectivity and access of smart things.

BPM.2) For newly designed process, a BPM tool needs to support the interface to access the data.

BPM.3) For automation, a BPM tool needs to support periodic collection of information.
through standard interfaces HTTP based interfaces.

BPM.4) A BPM tool needs to provide the interfaces for data analysis of business process.

BPM.5) A BPM tool should provide uniform access through its own data through standard HTTP-based interfaces.

**Addressing requirements:**

BPM.6) The BPM tool should be 100% accessible through web-based interfaces and API. [16]

**Security, authentication and privacy requirements [16]:**

BPM.7) A BPM tool needs to be provided with the authentication and authorization mechanisms.

BPM.8) A BPM tool needs to be provided with the encrypted communications.

**Qualities of service (QoS) requirements, including data integrity, transmission confirmation:**

BPM.9) A BPM tool needs to be provided with query and response without delay.

**Management-related requirements [16]:**

BPM.10) A BPM tool should allow building a supply chain integration process.

BPM.11) A BPM tool should allow building a CRM integration process.

BPM.12) A BPM tool should allow building an ERP integration process.

BPM.13) For maintenance purposes of process, a BPM tool should provide an extensive mechanism for versioning and deployment of successive versions of the processes.

BPM.14) The management overhead of the BPM tool should be as low as possible; ideally it is a Cloud based BPM.

**Discovery and lookup requirements:**

BPM.15) A BPM tool should have a way to discover the sources that have the data.

BPM.16) A BPM tool needs to manage and control the list of the data sources with timestamp.

BPM.17) The query result between a BPM tool and resource repository needs to be complete and correct.

**Cross-domain interactions requirement [16]:**

BPM.18) The BPM tool should be able to communicate with applications in any domain, that are cloud applications or on premise applications or database.
4.6 Technology-specific requirements

4.6.1 RFID tags & Smart Things Information Service

Radio Frequency Identification (RFID) technology enables tagging of everyday objects with a unique smart thing Identifier (STID). Smart Thing Information Service (STIS), such as EPCIS (http://www.gs1.org/gsmp/kc/epcglobal/epcis), have been developed to ease the management, the sharing and the access to tags related information. The STIS serves as a global infrastructure, providing information about smart thing metadata (e.g., product class or description), traces of location and time, as well as status of smart things. The STIS encompasses information systems, communication protocols, and data types that support capturing, storage, and exchange of smart thing-related data.

Specific functionality requirements [17]:

ST.1) Smart thing information service (STIS) provides instance-level RFID event retrieval given smart thing ID (STID) by exposing web service interface.

ST.2) STIS needs to provide exchange of vocabularies among STISs.

ST.3) STIS needs to provide look-up the metadata of an object with its identifier.

ST.4) STIS needs to provide look-up the trace information of an object with its identifier.

ST.5) STIS needs to provide RFID event processing such as filtering and grouping.

ST.6) STIS needs to provide the configuration of RFID reader and its air protocol.
ST.7) STIS needs to provide a way for clients to register/deregister standing queries to provide instant information on incoming notifications.

**Addressing requirements:**

ST.8) STIS needs to provide methods to refer to objects which are identified by EPC according to Tag Data Standard defined by EPCglobal.

ST.9) STIS needs to provide methods to diversify the referring method to types of items defined in tag data standard, such as SGTIN, GIAl, and so on.

ST.10) STIS needs to provide the diverse form of EPCs such as EPC-pure, EPC-tag, and EPC-binary.

ST.11) STIS needs to provide methods to refer to non-RFID objects such as ZigBee nodes, and 6LoWPAN nodes.

**Security, authentication and privacy requirements [17]:**

ST.12) STIS needs to provide the user authentication.

ST.13) STIS needs to provide the authorization depending on user’s organization and each STID (e.g., EPC ID or IPv6 address) to query.

ST.14) STIS needs to provide encrypted communications.

ST.15) STIS needs to provide public key cryptography for digital signature.

**Qualities of service (QoS) requirements, including data integrity, transmission confirmation [17]:**

ST.16) Responses to the queries on information about objects need to be delivered instantaneously.

ST.17) The confidentiality of both the publisher data and client query needs to be ensured.

ST.18) The query result should be complete, correct and within an acceptable time frame.

ST.19) The query needs to be processed according to the clients’ access rights, defined separately by each information provider.

**Management-related requirements [17]:**

ST.20) STIS needs to provide interfaces for clients to access STIS by STID (e.g., EPC ID).

ST.21) STIS needs to provide self-healing and fault tolerance mechanisms for high availability.

ST.22) STIS needs to keep monitoring smart things to build traces of the smart things.

ST.23) STIS needs to control the monitoring behavior (e.g., monitoring interval, monitored target classes, etc.) to optimize its operations at runtime.

**Discovery and lookup requirements [17]:**

ST.24) Given STID, discovery services needs to provide a bootstrapping strategy for clients to access the correct STIS.
ST.25) Given STID, STIS needs to be accessible from authorized clients.
ST.26) STIS needs to provide information about physical objects at instance level (e.g., serial number) given STID (e.g., EPC ID, or IPv6 address)
ST.27) The discovery service needs to ensure a high availability and reliability.

*Cross-domain interactions requirements [17]:*

*As a server:*

ST.28) STIS needs to provide clients with the instance-level information about objects having IPv6 and EPC addresses.
ST.29) STIS needs to provide clients with publish/subscribe interface to be notified of instance level events on objects in STISs.
ST.30) Clients in IoT6 retrieve the instance-level RFID events from STISs, lookup the metadata and trace information of an object with its identifier.

*As a client:*

ST.31) STIS needs to be provided with information about current location and time of IPv6 devices.
ST.32) STIS should be able to discover and access services hosted on IoT6-enabled devices.
ST.33) STIS needs to be provided with information about physical context from IoT6-enabled sensor devices.

### 4.6.2 Wireless sensor networks

A wireless sensor network (WSN) is a collection of autonomous and distributed sensors which obtain information from the physical world. Different kinds of environmental conditions can be measured by a wireless sensor network, like the temperature, the humidity, the pressure, the sound, etc. Each wireless sensor sends its data to a gateway and then the different sorts of measurements are handled by a centralized intelligent system.

*Specific functionalities requirements:*

WSN.1) Devices should support the remote configuration and controlling (e.g. activating, deactivating and updating). [18]
WSN.2) Devices should support event-based and periodic communication.
WSN.3) Devices should provide request-response communication.
WSN.4) Devices should support unicast and multicast routing. [19]
WSN.5) Devices should support data routing based on content.
WSN.6) Devices should support data processing (filtering, aggregation/fusion, etc.).
WSN.7) Devices should provide location information (pre-established or local-estimation).
WSN.8) Devices should provide sensor information captured of the environment.
**Addressing requirements [20]:**

WSN.9) IPv6 Link Local Address: 128 bits (Used only on a single network link)
WSN.10) IPv6 Global address: 128 bit
WSN.11) IPv6 Multicast address: 128 bit

**Security, authentication, and privacy requirements:**

WSN.12) Devices should provide confidentiality in the wireless communication.
WSN.13) Devices should provide their identifier when they join to the network.
WSN.14) Devices should support encrypt communications.
WSN.15) Devices should support scalable and remote bootstrapping protocols.
WSN.16) Devices should support asymmetric-based cryptographic primitives (e.g. Elliptic Curve Cryptography).

**Quality of Service (QoS) requirements, including data integrity, priority routing, transmission confirmation:**

WSN.17) Devices should differentiate message flows and prioritize according to the type of data.
WSN.18) Nodes of the network should be able to redirect incoming data flows to different IPv6 addressed servers according to the packet content and some pattern recognitions.
WSN.19) Devices should provide the mechanisms necessary to guarantee the data integrity.
WSN.20) Devices should provide status information (battery, memory, radio usage).
WSN.21) Devices should support the live monitoring of the radio activity of gateways.
WSN.22) Devices should provide reliable communication

**Data size requirements (very light data for Wireless Sensor Networks):**

WSN.23) The system should provide the lower overload for communications headers (IPv6, UDP, TCP or 6LoWPAN). [21]
WSN.24) There should be optimization of headings for global communications.
WSN.25) There should be optimization of headings for discovery services, and management protocols.

**Connection requirements (pull vs. push, synchronous vs. asynchronous, TCP vs. UDP):**

WSN.26) The network should provide initial configuration information to new joining nodes.
WSN.27) The network should support the mobility of nodes.
WSN.28) The network should support the automatic mechanisms to add new nodes and remove old nodes.
WSN.29) Devices should provide low-overhead asynchronous communication.
WSN.30) Devices should provide low-overhead UDP protocol. [22]
WSN.31) Capabilities for the identification of a session.
WSN.32) Capabilities for continuous communications management.

*Management-related requirements:*

WSN.33) Devices should provide the self-management processes based on pre-established policies and rules.
WSN.34) Devices should provide the self-configuration tasks for unattended joining to the network.
WSN.35) Devices should provide the self-healing mechanisms for automatic discovery and correction of faults.
WSN.36) Devices should inform about failures of the communication.
WSN.37) There should be systems for security management. This requires management of identity, authorisation, confidentiality, key exchange, audit trails, etc.

*Discovery and lookup requirements:*

WSN.38) The network should provide the mechanisms necessary for discovering devices that join to the network, along with their capabilities.
WSN.39) Devices should publish information about their computing and sensor capabilities.
WSN.40) A common semantic description.
WSN.41) A discovery protocol to advertise resources in other subnets, in addition to the local resources.
WSN.42) Resource directory for legacy devices and technologies in local and other subnets.
WSN.43) Integration and compatibility of the Discovery and look-up services with the IPv6-based approaches (e.g. DNS).
WSN.44) Support for advertising services.

*Energy-related requirements:*

WSN.45) Devices should provide long-time life with battery-power.
WSN.46) Devices should keep a real-time clock.
WSN.47) Devices should support time synchronization to optimize the radio usage.
WSN.48) Energy awareness through the services layer.

*Cross-domain interactions requirements:*

As a service:

WSN.49) Get the identified information of a specific device.
WSN.50) Get the location information of a specific device.
WSN.51) Get the sensor data of a specific device.
WSN.52) Get the status of a specific device.
As a client:
  WSN.53) Get the configuration of a gateway device.
  WSN.54) Get the time synchronization of a gateway device.
  WSN.55) Notification of communication failures.
  WSN.56) Information of changes in mobility.

4.6.3 Audio/Video components
Audio and video components are widely used by the entertainment industry and are more and more interacting with the IoT through devices such as mobile phones, video cameras and audio sensors. This raises specific requirements related to the streaming of data. There are several specific functionalities that need to be supported as part of the utilisation of audio and video devices:

AV.1) The architecture should be able to handle streaming services and route streaming data.

AV.2) Status of audio/video devices needs to be provided: on, off, standby, etc.

AV.3) Device status needs to be remotely controlled (on/off/standby).

AV.4) Access to specific device functionalities must be given (play, FF, etc.).

AV.5) Quality of Service (QoS) is required, including data integrity and avoidance of any streaming interruption.

AV.6) Low latency: entertainment devices need to react within less than 1 second.

4.6.4 Cloud computing associated with Software as a Service (SaaS)
Cloud computing is a «style of computing where scalable and elastic IT-related capabilities are provided as a service to external customers using Internet technologies» (Gartner Inc.). It can cover all stacks of IT technologies, from software (aka SaaS, Software as a Service), to platform (aka PaaS, platform as a service) and infrastructure (aka IaaS, infrastructure as a service).

The requirements for cloud computing system at the SaaS, PaaS or IaaS level are [23][24]:

CC.1) Delay-free: no installation nor significant delay (e.g. <1 hour) should be necessary to install the system or scale it.

CC.2) Interoperability: the system should be 100% inter-operable using standard Web-based APIs; the set of API should cover the core functionality of the system as well as its management operations. [25]

CC.3) Security: the system should provide at least one standard security mechanism at the user interface level and the API level

CC.4) Availability: the system should use standard web protocols and formats for its user interfaces as well as its API, and they should all be available over the Internet. [25]
CC.5) **Management:** management of the system should be included in its usage policy and handled by the provider.

If personal data are to be stored in a cloud system, compliance of the system with EU regulations at the time of project deployment must be verified (physical location of data, compliance with Safe Harbour, etc.). In any case core data should be stored using state of the art encryption (128 bits asymmetric mechanism), with encryption keys that are different per customer account on the system («tenant»), and possibly controllable by each «tenant»; in some systems the ability to locate part of the account data (e.g. personal data) on a private storage account might be investigated, at the exclusion of any processing. More generally smooth integration with cloud computing systems requires that IoT6 components offer APIs based on HTTP protocol and standard web formats (e.g. XML or JSON): ideally ReST type API. [25]

### 4.6.5 Safety and security

Safety and security are the most important part in each technical project, because the life of each human being can be influenced by a mistake when the security or the safety is underestimated by the engineers developing a system. Security is the protection against the different sorts of criminal actions, the physical damage and the loss of material. Generally, the security contends against the evil intentions of people. Safety is the protection against the accidents, the incidents, the dangers and the failures. The solutions helping to resolve safety problems are most often based on technical advances.

Basically, the main constraints to ensure **security and safety** are given below:

S.1) Confidentiality of the information.
S.2) Secured distribution of the data.
S.3) Integrity of the data during the transmissions.

**Specific functionalities requirements:**

S.4) Fire detection, access control, surveillance, emergency path must be supported.
S.5) Dependable communication channels mandatory.
S.6) Device status needs to be monitored and device functionality must be given.
S.7) Auditing of installation/device functionality must be provided.

**Connection requirement:**

S.8) Periodic heart-beat signals.

**Quality of Service requirements, including data integrity, priority routing and transmission confirmation:**

S.9) Standards and national requirements about reliability for safety critical communication infrastructure need to be adhered to.
S.10) Test for working connections and data transfer.
[5] Surveys based requirements

IoT6 intends to include an end-user perspective in its research and development cycle. In order to do so, three perspectives have been integrated:

- Taking into account the end-users requirements of a smart IPv6 building project led by Mandat International;
- Inviting the IoT6 Industry Advisory Board members to contribute with complementary requirements;
- Identifying privacy requirements through a panel of potential IoT6 end-users composed of delegates from different parts of the World.

5.1 Smart IPv6 building end user requirements

Mandat International (MI) intends to build an 11 floors building to support and accommodate delegates coming from developing countries to attend conferences at the European UN headquarter in Geneva. MI intends to turn this building into a fully smart IPv6 building. It will require the integration of various and heterogeneous components and sub-systems of the Internet of things with various possible cross-domains interactions. If successful, the IoT6 architecture will be transferred and used for this project and similar ones\(^1\).

The technical and functional requirements of this smart IPv6 building project have been already analyzed in the frame of the FP7 Hobnet research project ([www.hobnet-project.eu](http://www.hobnet-project.eu)) and include:

HOB.1) Global integration and interoperability among the various components and subsystems integrated into the architecture;

HOB.2) High scalability of the architecture and solutions, using IPv6 addresses and IPv6 compliant solutions wherever possible;

HOB.3) Reliability of the proposed solutions, including Quality of Service (with different priorities to data flow);

HOB.4) New solutions which are as much as possible agnostic of underlying products, solutions, trademarks and protocols, with the ability to overpass the fragmentation and heterogeneity of sensors and smart devices integrated in the Hobnet architecture;

HOB.5) Modular and evolutionary architecture, easing the integration and the development of existing and future systems;

HOB.6) Green ICT (Information and Communication Technologies) orientation to limit the energy consumed by the ICT infrastructure;

HOB.7) Integration of the Hobnet developments with the UDG control and monitoring system, which will be used to manage the pilot and the future building;

HOB.8) Ease of use, configuration and maintenance, with better design of service, higher usability, and friendly management system interfaces;

\(^1\) More information is available on [www.internationalcooperationhouse.org](http://www.internationalcooperationhouse.org) and [www.smartipv6building.org](http://www.smartipv6building.org)
HOB.9) To avoid any harmful radiation or effect on health or safety;
HOB.10) Possibility to integrate low-cost products and solutions.

5.2 IoT6 Industrial Advisory Board (IIAB) requirements

A questionnaire has been sent to all the IoT6 Industrial Advisory Board (IIAB). The following specific requirements have been identified by the IIAB members:

IIAB.1) Interoperability/Interactivity between the different components: the different kinds of components coming from several manufacturers should communicate between them without any problems. New interactions between different sorts of devices could appear and provide new interesting services to the end users.

IIAB.2) Wireless technology compatible to reduce the cabling: the main benefit from using wireless communication is to reduce the cabling needed by old communication technologies. Today, the cabling is very expensive: the price of the raw materials, like the copper, is higher and the deployment of wired communication systems requires some important qualified manpower.

IIAB.3) Security: the security should be always increased when the communication between the human beings or the machines becomes global. The global communication is an important theme in the conception of the Internet Protocol version 6 (IPv6).

IIAB.4) Confidentiality: the confidentiality of the personal data from each end user should be guaranteed in any circumstances. Only authorized people should access to the personal data.

IIAB.5) Scalability: with the appearance of IPv6, it becomes easier to connect a lot of devices between them. More interactions are possible with a great range of addresses.

IIAB.6) Standardized data format: the system to develop should manage the current standards used in the different domains to ensure a good communication with the devices already installed.

IIAB.7) Limited standardization to leave more possibilities to developers: during the project, the standardization should be as limited as possible. The goal is to obtain more liberties for the developers which will be more creative. New interesting applications could eventually appear if the system is open.

IIAB.8) Autonomous devices if the network is crashed: each device should continue to run when the IP network is down. Some mechanisms should be put in place to avoid any problems with the disconnected devices and to guarantee the independence of the devices with respect to the network.

IIAB.9) IP support as deep as possible in the network: the IP protocol, preferably IPv6, should be the central protocol of the system in development. [22]

IIAB.10) IP-based services: the system should offer different sorts of services for the end users. The access to these services should be easy and based on the IP protocol. Typically, the services are web services or cloud applications. [22]
5.3 Delegates survey – a specific end-user perspective on privacy

With more and more pervasive intelligence, privacy will be a major issue for the future Internet of things. In order to address it in our architecture design, we have launched a survey with visiting delegates attending UN conferences who are potential end–users of the IoT6 architecture through the MI project, and who have an inherent interest to protect their privacy due to their work as delegates. A questionnaire has been elaborated with open and closed questions in order to assess the delegates’ interest and concern regarding the privacy issues that may arise in the frame of the IoT6 research project. 22 delegates have been individually interviewed in order to collect their inputs.

The interviews were structured in three parts. At first, we presented the research project to them. Afterwards, the delegates were invited to answer open questions. In a third part, they were invited to respond to closed questions. This order was respected to prevent a possible influence of the closed questions on the open ones.

5.3.1 Geographical repartition
The 22 interviewed delegates were coming from different parts of the World with the following geographic distribution:

![Geographic repartition](image)

Fig. 8 – Geographic repartition

5.3.2 Concerns regarding data protection
The delegates were invited to indicate three main issues regarding the protection of personal data. The interviews revealed several areas of concerns:

- the use of personal data (45% of the panel)
- the confidentiality of personal data (36% of the panel)
- the computer network security (27% of the panel)
- the security of their personal objects (23% of the panel)
- the telecommunication network (14% of the panel)
- the data storage (9% of the panel)
- the human factor (9% of the panel)

A significant part of the panel (23%) said they had no concern with data protection.
5.3.3 Recommended actions
The delegates were invited to propose three actions to solve issues related to the protection of their personal data. The main proposals are the following ones:

- 32% of the panel proposed juridical measures, such as non-disclosure agreement or legal norms to support the data privacy;
- 27% of the panel proposed to strengthen the access control to the building, and to each room containing personal data or objects;
- 23% of the panel suggested technological measures to ensure the computer network security, such as firewalls, passwords, or encryption of the personal data;
- 14% of the panel suggested increasing the information on data privacy for the delegates.
- 23% of the panel did not propose any solution.

5.3.4 Expected services
The panel was invited to suggest services that could be provided by an intelligent building management system. The main proposals were the following:

- 41% of the panel mentioned energy and water saving;
- 41% of the panel mentioned more security, for instance by using controlled accesses, alarms and video cameras in public areas;
- 27% of the panel suggested entertainment system, with suggestions regarding more multi-functional, user friendly, cheap and cultural diverse systems;
- 18% of the panel mentioned more safety, against the fire for example;
- 14% of the panel proposed services to increase the comfort in the rooms;
- 14% of the panel mentioned heating regulation;
- 9% of the panel suggested cleaning services;
- 5% of the panel mentioned automatic check-in for the delegates.
- 18% of the panel did not submit any proposition.

5.3.5 Innovation
The following questions were closed, with five possible answers: very negative, rather negative, neutral, rather positive, very positive. The first question was on their support for technological innovations. All the interviewed support in principle technological innovations: 60% are totally in favor and 40% are rather in favor.

5.3.6 Data transmission
The next question was on the transmission of data to the building management system, with different kinds of data. The vast majority of the delegates agreed to give information to the building management system to indicate whether a room is occupied (45% of the panel is totally for and 41% are rather for). However, about a half of delegates didn't want to transmit information to the system regarding who was actually in a particular room (23% of the panel is totally against and 27% of the same panel is rather against). Regarding delegates localization in the building, half of the delegates was opposed to it (14% of the panel is totally against and 36% of the panel is rather against). A large majority of delegates agree to provide data to the building management system for the energy saving (55% of the panel is totally for and 27% of the panel is rather for).
The next question was on the acceptance to transmit data to different entities, with a list of entities including the delegate himself, the building managers, other delegates in the building, the universities and the public. A large majority of the delegates are interested to access to the energy consumption of their room and to the global energy consumption of the building (36% of the panel is totally for and 45% of the panel is rather for). There is a large support to make the energy consumption available to the building manager (57% of the panel is totally for and 33% of the panel is rather for). A smaller majority of interviewed delegates agree to share their personal energy consumption with the other delegates (36% of the panel is totally for and 23% of the panel is rather for), with a significant minority who would not like to share their energy consumption with the other delegates (9% of the panel is totally against and 23% of the panel is rather against). This part of delegates considers that the energy consumption for each delegate is personal information and it should remain private. The majority of delegates agrees to transmit the building energy consumption to the universities (38% of the panel is totally for and 29% of the panel is rather for), but some delegates did not understand the reasons to share data on their personal energy consumption with universities (19% of the panel is totally against). A majority of the delegates agree to make the building energy consumption information available to the public at large (32% of the panel is rather for and 27% of the panel is totally for). However, a significant part of the panel does not approve to give the building energy consumption to the public (23% of the panel is totally against and 14% of the panel is rather against).

5.3.7 Mobile phone use
The two following questions were related to mobile phone interactions. A majority of the panel is interested to connect their mobile phones to the intelligent building management system (40% of the panel is rather for and 30% of the panel is totally for). A majority of them is also interested to receive information from the building management system on their mobile phones (23% of the panel is rather for and 32% of the panel is totally for). However, a significant number of interviewed was not interested to receive information on their phone (41%).

5.3.8 Data anonymity
The next question concerned the anonymity of the collected personal data. The survey shows that a large majority of the interviewed delegates encourage the anonymity of personal data (57% of the panel is totally for and 19% of the panel is rather for).

5.3.9 Data sharing motivation according to its finality
The interviewed were invited to respond whether they were ready to share personal information according to different goals: energy saving, access control and security, comfort, and networking with other delegates. The answers were globally positive and most interviewed delegates were ready to share personal information in order to:
- Save energy (55% of the panel is rather for and 36% totally for).
- Improve security (23% of the panel is rather for and 55% totally for).
- Improve comfort (27% of the panel is rather for and 64% totally for)
- Increase the networking between the delegates (27% of the panel is rather for and 59% totally for).
5.3.10 Privacy perception regarding personal localization
The last question was a closed question on the privacy of the current location of a person in the building. Four responses were proposed: public, fairly public, fairly private and very private. 43% of the panel considers that their current location in the building is fairly private, 29% as fairly public, and 24% as totally public.

![Privacy of individual location](image)

5.3.11 Privacy-related requirements
The survey was designed to integrate the perspective of a panel of potential end-users. Because of its size, it does not pretend to provide any universal conclusion. However, it enables us to extract a certain number of relevant requirements to address the privacy concerns:

**DEL.1**) There are heterogeneous perceptions and positions from one person to another and this diversity should be taken into account. The system should enable an opting in or opting out mechanism regarding personal data exploitation. The opting in/out mechanism should be granular, enabling a person to accept certain options and refuse others.

**DEL.2**) Users are more willing to share personal data if they perceive a clear individual or collective interest. It would be important to explain to potential users the relationship between data exploitation and its use and impact.

**DEL.3**) Users must be well informed on the data collection and the research project objectives.

**DEL.4**) No personal data should be transmitted outside the building without the person’s consent or without being anonymized.

**DEL.5**) Personal data encryption and confidentiality should be ensured.

**DEL.6**) A clear legal/agreement framework should be provided.
[6] Use-case scenarios

One of the objectives of task T1.1 is to define specific scenarios that will be demonstrated in the validation phase. These scenarios must demonstrate the added value of IoT6 architecture to integrate heterogeneous components and to enable cross-domain interactions. It should also define specific application scenarios to be tested with potential market perspectives in mind, such as energy efficiency, safety and business process management.

These scenarios are expected to be re-used for the conception of the WP7 demonstration. As the project is just starting, it is expected that the selected use case scenarios will evolve in line with the project developments. Nevertheless, these scenarios already enable us to:

- Identify complementary functional and technical requirements;
- Elaborate a provisional list of devices to be considered by WP7 for the demonstrations;
- Fine tune a list of key communication protocols to be addressed by WP4.

6.1 Scenario design process

In order to align the scenarios with the industry areas of interest, the scenarios have been selected through a participatory process involving the IoT6 Industry Advisory Board (IIAB) members. A participatory scenario design workshop with all IoT6 Industrial Advisory Board members was originally planned. However, it proved to be more efficient to replace it by another process.

A questionnaire has been sent to the IIAB partners with a list of question to identify attractive applications and components to include in the scenarios. This approach enabled the IIAB members to circulate it internally and to mobilize the inputs of people who would not have been able to attend the workshop. Additional scenarios inputs have been taken into account, such as the European Commission’s videos presenting future IoT-related application scenarios.

The IoT6 research partners have met and discussed the IIAB inputs in the frame of a project workshop. It has enabled the consortium to elaborate a first set of cross-domain use-case scenarios, with three main concerns:

- To cover different domains of applications;
- To include scenarios with potential market perspectives;
- To include scenarios able to demonstrate IPv6-based features that will be addressed by the IoT6 architecture.

After the workshop, these scenarios were further discussed remotely and fine-tuned by the consortium, eventually ending up with a list of 5 IoT6 use-case scenarios, spanning across various application domains.
6.2 IIAB inputs for the scenarios

The IIAB members have been invited to submit ideas to be used for the scenarios. The following are the ideas received from the IIAB members:

1) Optimization of energy usage and comfort by IoT: This scenario could demonstrate that the productivity of occupants in the building will increase. If an IoT system increases the comfort for the people in an office, these people will work with more efficiency and increase the productivity of the enterprise.

2) Scenarios for urban centers: The scenario could create a welcoming ambiance for people to come and stay. It could also enable safe and easy traffic flow for cars, public transport and pedestrians.

3) Scenarios for shops: The scenario would use window dressing, music & lighting to invite people to come in, to buy and to make them come back.

4) Scenarios for office building: The scenario could enable a more flexible use of spaces with adaptation of local environment, energy saving and security features.

5) HVAC control system connected to blinds and lightings: This scenario should demonstrate an increase of comfort and energy saving. The blinds and the lightings installed into a building are remotely controlled by a building management system. In function of the presence of somebody in a room, the lightings and the blinds are adjusted by the HVAC control system to save energy.

6) Virtualization of the resources: All physical resources should be represented in a virtual manner in the IoT philosophy.

7) Content-based routing: The type data should be routeable to different endpoints. The content of data in an IPv6 frame could determine the destination of this frame, independently from the classical destination address.

Suggested devices:

1) A BMS (Building Management System).
2) Chiller.
3) Air handling unit.
4) Opening windows.
5) Blind controls.
6) Different kinds of electric light controls.
7) Occupancy detectors.
8) Online feedback of installed control systems and sensors.
6.3 **Selected use-case scenarios to be tested and demonstrated**

We will analyse the following Use Cases to ensure that the architecture that we develop will support their requirements. Portions of the scenarios will be implemented to validate the architecture.

6.3.1 **Scenario 1 – Building maintenance process**

The first scenario addresses the maintenance process of building automation components through the cross-domain IoT6 architecture. It intends to demonstrate the benefits of the IoT6 architecture to ease the integration of the IoT (with a focus on building automation components) with mobile phones, as well as with virtual resources, such as STIS, SaaS and business management application:

1) A local maintenance employee identifies a problem with a building automation device. He reads the tag of the device through an interface of his mobile phone, such as NFC, and sends the identifier with a comment to an online maintenance tool (a SaaS). The IPv6 address of the online maintenance tool is provided by a resource directory, which contains all updated links to the IoT6 resources.

2) The SaaS generates a maintenance ticket.

3) The SaaS searches for and retrieves information on the device through, among others, the Smart Things Information Service (STIS). It sends the information to a maintenance officer on his mobile phone. First of all, the maintenance tool does a query to the resource directory to obtain the IPv6 address of the Smart Things Information Service (STIS).

4) The maintenance officer launches some tests through his terminal and collects data from local sensors, including non-IP based sensors, to make a diagnostic of the problem. The identification of the sensors to use are provided by a resource directory.

5) The maintenance officer uses the SaaS maintenance tool from his mobile phone to order the spare parts.

6) The device arrives on site. A local maintenance employee scans the device ID through an interface of his mobile phone, such as NFC. The information is sent to the SaaS maintenance tool. Before to send the information to the online maintenance tool, the IPv6 address of the maintenance tool is needed and a request to the resource directory is realised by the mobile phone network to obtain this address.

7) The local employee receives instruction on how to replace the device and validates the replacement once it is done.

8) The remote maintenance officer tests remotely and validates the installation of the new device. Then he closes the maintenance ticket of the maintenance process in the SaaS.
Previsional sequence diagrams (UML):

**Step 1:**

**Step 2:**

**Step 3:**

**Step 4:**
Previsional list of devices:
- A building automation device, which can be for example a blind controller, a motorized radiator valve or a temperature sensor.
- Miscellaneous sensors to collect data.
- A mobile phone used as a terminal for the maintenance worker.
- A web service for the cloud computing application together with SaaS to manage the maintenance process.
- A Smart Thing Information Service to retrieve device information.

Specific requirements:
- Reliability and Quality of Service: the transmission from the defaulting device to the rest of the system should be reliable.
- Ubiquitous access: the devices should be accessible from any place in the world.
- Access control: the access to the devices should be protected and restricted to authorized users only in a best effort manner.
- Heterogeneous integration: the system should enable the integration of heterogeneous devices using different communication protocols.
- Routing: smart routing would contribute to the implementation of this use case.

6.3.2 Scenario 2 – Safety alert with QoS through IoT6
This use-case scenario is focused on security and safety. It intends to demonstrate IPv6 and IoT6-related features, such as anycast, “smart routing”, priority routing and QoS to ensure fast and reliable exchanges of data between different components and applications:

1) A device/sensor sends abnormal temperature values to a local data server. We consider that the device or sensor is connected by a non-IP based protocol to the IoT6 architecture. The non-IP based protocols proxy searches for the IPv6 address of the local data server and this address is already stored into the resource directory.

2) This IoT6 data server is able to recognize the abnormal temperature in the received packet and tags the data with a “priority/safety alert” tag.

3) The IoT6 data server looks up the IP addresses of the closest security server and possible back-ups. The resource directory contains all IPv6 addresses needed by the local data server.

4) It forwards the data received to the energy management server and sends a duplicate of the data by anycast with QoS and priority routing to a first group of security servers. If it does not receive a reply in a given time, it sends again the duplicate data to another group of security server.

5) The security server confirms the reception of the data received and multicasts the alert to a group of alarms located in the area of the sensor, as well as to the mobile phones of the staff members located in the vicinity of the sensor. The alarms become active and an alert message is displayed on each mobile phone.

6) An alert ticket is generated on a SaaS safety management tool interface.

7) A staff member checks the room.

8) Once the safety is checked and confirmed, the employee updates the alert
ticket on the Safety Management Tool through his mobile phone. The Safety Management Tool transmits the information to the Security Server. The security server then sends by multicast a command to turn off all activated alarms in the secured area.

Previsional sequence diagrams (UML):

Step 1:

Step 2:

Step 3:

Step 4:
Step 5:

Previsional list of devices:
- A temperature sensor.
- An energy management server.
- A safety and security server.
- A SaaS based alarm management system.
- Several alarms.
- A mobile phone.

Specific requirements:
- **Reliability and Quality of Service:** the transmission from the defaulting device to the rest of the system should be reliable.
- **Routing:** routing based on content and priority.
- **Addressing:** multicast and anycast.
- **Self-healing architecture:** if a node is broken, the system should recover by itself.
6.3.3 Scenario 3 – Mobility and Surveillance

This use-case scenario is focused on mobility features with moving smart things and persons across different locations. It intends to demonstrate the mobility features provided by an IPv6 environment and integrated into the IoT6 architecture, as well as its ability to handle audio and video streams:

1) The grounds of an estate are equipped with both video cameras on the boundary and infra-red ones scattered over the grounds. All are linked to a central control. There are several guards equipped with Wi-Fi, communications with the main building, and cameras. The IR sensors are capable of wireless relay.

2) An intruder is observed entering the grounds. He subsequently sets off IR alarms from deployed devices. The resource repository automatically tracks the location of the alarms and updates the route. The communication is secured.

3) Guards are dispatched to find the intruder. Their devices include a video camera, AV communications and an IR camera networked into a personal area network. This communicates in an ad hoc way through the relays of the deployed sensor network in the grounds.

4) The central control monitors the video stream from the guards’ cameras without any interruption. The location of each guard is saved into the resource repository.

5) While moving, the guards sometimes go out of range of the sensor network. Communications is maintained through alternatively Wi-Fi access points and mobile phone network. The location of each guard is stored, too.

6) Powerful target recognition software, in central control, analyses the camera images – helped by information from the sensor array as to the intruder locations. The resource repository automatically tracks the location of the guards and guides them towards the intruder. The central control sends requests to the resource directory to know the current position of each person. Then the guards are informed about the location of the intruder and eventually of their colleagues.
Previsional sequence diagrams (UML):

Step 2:

Step 4:

Step 5:
Step 6:

Previsional list of devices:
- A mobile communicating device.
- Access points to ensure the mobile connectivity.
- A resource repository.
- Sensor arrays organized as an ad hoc network.
- IR sensors.

Specific requirements:
- **Mobility**: the system should support the mobility of the nodes.
- **End-to-end communication**: between the guards’ Personal Area Network and the resource repositories should be guaranteed.
- **Ubiquitous interactions**: the devices should be accessible from any place.
- **Privacy**: the confidentiality of the data should be ensured.
- **Mobility**: Mobile Ad hoc Network (MANEMO) should be supported.
- **Connectivity**: uninterrupted video communications are required.
- **Integrations with SaaS**: target acquisition via cloud computing is also required.
- **Additional software**: target recognition software is required.

6.3.4 Scenario 4 – The smart office

This scenario is directly inspired by the IIAB proposals. It intends to demonstrate the ability of the IoT6 architecture to interact with heterogeneous devices, including non-IP based protocols, with a focus on energy efficiency and user comfort:

1) An employee arrives at his office building. He identifies himself with his mobile phone through an interface, such as NFC. A terminal reads the tag included in the mobile phone.

2) The lights, the windows and the HVAC system are adapted to create a comfortable and welcoming ambiance for him at his work station.

3) The employee updates his custom preferences through his mobile phone. The service which manages the communications on the mobile phone network does a request to the resource directory to know the IPv6 address of the non-IP based protocols proxy.

4) A visitor arrives and is guided to the waiting lounge. Video and music are launched, together with lightings adaptation to create a welcoming ambiance. A presence sensor installed in the waiting lounge detects the arrival of the visitor and advises the non-IP based protocols proxy which starts the video and the music.
5) When the employee exits his office, the lights, windows and HVAC systems around his work station are automatically adapted in order to save energy. A presence sensor placed in the office detects that nobody is in this room and the different actions to save energy can be initiated.

6) When exiting the building, he receives a farewell message. A request to the resource directory is realized to retrieve the address of the mobile phone.

Previsional sequence diagrams (UML):

Step 1:

Step 2:

Step 3:

Step 4:
Step 5:

- Presence sensor.
- Temperature sensor.
- Lightings.
- Blinds.
- HVAC control system.
- A mobile phone with a NFC interface, for instance.
- A NFC, or other technology terminal into the building, which will act as a gateway between the mobile phone and the local network.
- Speakers.
- TV screen.

Previsional list of devices:

- Presence sensor.
- Temperature sensor.
- Lightings.
- Blinds.
- HVAC control system.
- A mobile phone with a NFC interface, for instance.
- A NFC, or other technology terminal into the building, which will act as a gateway between the mobile phone and the local network.
- Speakers.
- TV screen.

Specific requirements:

- **Multi-protocol interoperability**: different protocols should be supported for this scenario.
- **Privacy**: the confidentiality of the data should be ensured.
- **Mobility**: the system should support the mobility of the nodes.

### 6.3.5 Scenario 5 – The sick teacher

The last scenario is described in the European Commission's video which can be found on Youtube (http://www.youtube.com/watch?v=kq8wqY9Y9W0). The name of the video is *Internet of Things Europe – Teaser N°1: Student*. This scenario intends to demonstrate the versatility of the IoT6 architecture and its ability to exploit IPv6 features, such as multicast, address scability, end-to-end connectivity, as well as thing-to-thing (T2T) and thing-to-service (T2S) interactions:

1. A teacher is sick and stays at home.
2. He calls the university to advertise his absence.
3) Automatically, all students which have got a course with him during the day are notified on their mobile phone. The addresses of all concerned students are retrieved from the resource directory and are used to send the teacher’s absence notification by multicasting.

4) The agenda of each student is updated to take into account the teacher absence. A request to the resource repository is needed to obtain the IPv6 address of each agenda.

5) The precise time to take the bus to the university is recalculated according to the new schedule. The agenda does a query to the resource directory to get the IPv6 address of the online timetable for the public transportation.

6) The alarm clock is automatically set with a new time. A request to the resource repository is realized to obtain the IPv6 address of the clock alarm before sending the new schedule for the alarm.

7) The building automation system adapts the heating strategy for the lecture room, because the students will use the room later. A request to the resource repository permits to get the IPv6 address of the building automation system. Then the building automation system sets the HVAC system to obtain a good temperature according the student’s preferences.

8) The coffee machine of the student is reset to make a cup of coffee at a later time. In this part, the resource directory is used to get the IPv6 address of the coffee machine.

Previsional sequence diagrams (UML):

Step 2:

Step 3:
Step 4: 

```
phone1:MobilePhone mobilePhoneNetwork:MobilePhoneNetwork rd:ResourceDirectory agenda:Agenda
```

- reactToAbsenceNotification
- getReceiverIPv6Address
- getAgendaIPv6Address
- sendAgendaUpdate

Step 5: 

```
agenda:Agenda rd:ResourceDirectory timeTable:TimeTable
```

- getTimeTableIPv6Address
- getTime
- updateBusTime

Step 6: 

```
agenda:Agenda rd:ResourceDirectory clock:AlarmClock
```

- getClockIPv6Address
- setAlarm

Step 7: 

```
```

- getBASIPv6Address
- sendSchedule
- setTemperature

Step 8: 

```
```

- getCoffeeMachineIPv6Address
- sendSchedule
- setNewTime
Previsional list of devices:
- Mobile phones.
- Alarm clock.
- Electronic agendas.
- On-line bus time table.
- Building control and monitoring system.
- Heating system components.
- Coffee machine.

Specific requirements:
- *Ubiquitous interactions:* the devices should be accessible from any place.
- *Addressing:* multicast and anycast addressing should be supported.
- *Communication privacy:* the confidentiality of the data should be ensured.

### 6.4 Complementary functional and technical scenario requirements

The proposed use-case scenarios imply the following specific requirements:

SC.1) *Smart routing:* Content-based routing is required to implement the different scenarios.

SC.2) *QoS with priority routing:* the transmission of data should be reliable, especially for critical data.

SC.3) *Reliability and self-healing architecture:* the system should automatically return from errors to a normal state.

SC.4) *Re-routing of packets:* the packets should be re-routed across the different kinds of IoT6 servers.

SC.5) *Ubiquitous end-to-end communication between components:* the devices should be accessible from any place in the world.

SC.6) *Privacy and security:* the privacy and the security should be guaranteed in all cases.

SC.7) *Addressing:* multicast and anycast addressing should be supported in the scenarios implementation.
6.5 Provisional list of devices

By taking into account:
- the initial IoT6 targeted components;
- the devices proposed by the IIAB;
- the devices required by the use-case scenarios;
we can draw a provisional list of devices to be integrated into the IoT6 architecture:

1) Wireless and wired IPv6 equipment.
2) Mobile phones.
3) Sensors, including:
   a. Occupancy sensor.
   b. Temperature sensor.
   c. Medical sensor for e-health.
4) Building control and monitoring system
5) Building automation devices such as:
   a. Control and visualization device.
   b. Chiller and air handling unit.
   c. Blind controls.
   d. Window actuators.
   e. Lightings and electric light controls
   f. Radiator electro-valve.
6) STIS (Smart Things Information System).
7) SaaS (Software-as-a-Service):
   a. Maintenance process management tool
   b. Alarm management tool
   c. Electronic agendas.
8) Other devices, such as:
   a. Alarm clock.
   b. Coffee machine
   c. TV screen
   d. Speakers

This list of devices is likely to evolve according to the project's development.

6.6 Provisional communication protocols list

Based on the selected use-case scenarios, we have updated the list of communication protocols to be addressed by WP4:
- IPv4 and IPv6 (with UDP and TCP)
- KNX
- BACnet
- ZigBee
- 6LoWPAN
- DLNA/UPnP
- DALI
- NFC (with RFID tags)
- M-Bus

This list of protocols may still change according to the project’s development.
[7] IoT6 synthetic requirements

This section aggregates and synthetizes the different requirements identified in the previous sections of this document, including generic requirements, sector specific requirements, end-users survey based requirements, and use-case scenario-specific requirements.

In order to elaborate this list, the following methodology has been applied:

1) An Excel matrix has been used to organize and classify the various requirements by source (column) and topic (row).

2) A first list of synthetic requirements has been elaborated by merging the various sources together.

3) All requirements have been filtered in order to set aside those which are out of scope of the IoT6 research project. (e.g. radiation issues will not be addressed in the frame of this project).

4) The resulting list has been discussed and reviewed by the consortium partners in order to end up with a final list of synthetic IoT6 requirements.

In the table below we use the word “Compatible with X”. By this we mean that the architecture is fully compatible with any requirements or constraints imposed by X. Thus, for example, “Compatible with IPv6” means that all protocols, facilities and procedures defined for IPv6 should be available in the architecture. Of course this does not guarantee that the implementations include all such facilities.

In order to emphasize features that we consider important, the features are often included specifically as a separate requirement. Thus, for example, by saying “IPv6 compliant”, we clearly include the availability of infrastructures both for mobility and authentication. Nevertheless, both are repeated explicitly to indicate the need for that feature of IPv6.
### 7.1 IoT6 general architecture requirements

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
<th>Related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEN.1</td>
<td><strong>Internet compatibility</strong></td>
<td>WP1, WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable IoT components located in different parts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the world to interact over the Internet with each others through the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IoT6 stack. The IoT6 architecture should enable ubiquitous access to its</td>
<td></td>
</tr>
<tr>
<td></td>
<td>connected IoT6 devices and services.</td>
<td></td>
</tr>
<tr>
<td>GEN.2</td>
<td><strong>IPv6 compliance</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be IPv6 compliant where relevant.</td>
<td></td>
</tr>
<tr>
<td>GEN.3</td>
<td>High scalability</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be highly scalable in terms of number of IoT6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>connected objects, anticipating the growing number of Internet of Things</td>
<td></td>
</tr>
<tr>
<td></td>
<td>components.</td>
<td></td>
</tr>
<tr>
<td>GEN.4</td>
<td><strong>Mobility compatibility</strong></td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should support mobility of nodes and sets of nodes.</td>
<td></td>
</tr>
<tr>
<td>GEN.5</td>
<td><strong>Decentralized and distributed architecture</strong></td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td>IoT6 should enable a decentralized and distributed architecture.</td>
<td></td>
</tr>
<tr>
<td>GEN.6</td>
<td><strong>Information distribution</strong></td>
<td>1.2, 3.1, 3.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable an efficient distribution of information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>from IoT6 components.</td>
<td></td>
</tr>
<tr>
<td>GEN.7</td>
<td><strong>Intermittent and continuous connectivity compatibility</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable intermittent and continuous connectivity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>among IoT6 connected components.</td>
<td></td>
</tr>
<tr>
<td>GEN.8</td>
<td><strong>Energy consideration</strong></td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be in line with the green ICT approaches.</td>
<td></td>
</tr>
<tr>
<td>GEN.9</td>
<td><strong>Cross-domain integration</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable cross-domain interactions, including</td>
<td></td>
</tr>
<tr>
<td></td>
<td>but not limited to:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- mobile phones;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- tags and smart things informations services, such as EPCIS;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- wireless sensor networks;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- building automation components;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Software as a Service (SaaS).</td>
<td></td>
</tr>
<tr>
<td>GEN.10</td>
<td><strong>Heterogeneous (legacy) protocol integration</strong></td>
<td>WP4</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable the interaction with non-IP devices.</td>
<td></td>
</tr>
<tr>
<td>GEN.11</td>
<td><strong>Standards orientation</strong></td>
<td>4.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should take advantage and exploit relevant open</td>
<td></td>
</tr>
<tr>
<td></td>
<td>standards.</td>
<td></td>
</tr>
<tr>
<td>GEN.12</td>
<td><strong>Constrained device compatibility</strong></td>
<td>WP1, WP2, WP3</td>
</tr>
<tr>
<td></td>
<td>IoT6 architecture should be designed in such a way to support constrained</td>
<td></td>
</tr>
<tr>
<td></td>
<td>devices.</td>
<td></td>
</tr>
<tr>
<td>GEN.13</td>
<td><strong>Deployability</strong></td>
<td>2.4, 3.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be deployable on different platforms.</td>
<td></td>
</tr>
</tbody>
</table>
## 7.2 Network and communication

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
<th>Related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Addressing</strong></td>
<td></td>
</tr>
<tr>
<td>ADDR.1</td>
<td><strong>IPv6 addressing compatibility</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be able to use IPv6 addresses to identify and interconnect its various components.</td>
<td></td>
</tr>
<tr>
<td>ADDR.2</td>
<td><strong>6LoWPAN compatibility</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be compatible with shorter addresses schemes and lighter headers, such as 6LoWPAN addresses.</td>
<td></td>
</tr>
<tr>
<td>ADDR.3</td>
<td><strong>IPv4 environment compatibility</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should take into account the fact that in the actual environment, IPv6 is not always available.</td>
<td></td>
</tr>
<tr>
<td>ADDR.4</td>
<td><strong>Legacy integration</strong></td>
<td>WP4</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be able to integrate legacy objects using different addressing schemes and lengths.</td>
<td></td>
</tr>
<tr>
<td>ADDR.5</td>
<td><strong>Anycast and multicast compatibility</strong></td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be able to employ anycast and multicast.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Connectivity and transmission</strong></td>
<td></td>
</tr>
<tr>
<td>CONN.1</td>
<td><strong>End-to-end connectivity</strong></td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should support end-to-end connections among IoT6 connected objects located in diverse geographical locations.</td>
<td></td>
</tr>
<tr>
<td>CONN.2</td>
<td><strong>Smart routing (content based routing)</strong></td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture and stack should enable content-based routing of data. It should enable for instance to differentiate alert messaging and enable ad hoc routing.</td>
<td></td>
</tr>
<tr>
<td>CONN.3</td>
<td><strong>Data and header optimization</strong></td>
<td>2.4</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should optimize the size of the header and data sent over the network.</td>
<td></td>
</tr>
<tr>
<td>CONN.4</td>
<td><strong>Sleeping devices support</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture shall be able to manage communication that includes sleeping IoT6 devices.</td>
<td></td>
</tr>
<tr>
<td>CONN.5</td>
<td><strong>Continuous communication</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should support streams of data transmission, both reliable and</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Quality of Service</strong></td>
<td></td>
</tr>
<tr>
<td>QOS.1</td>
<td><strong>Reliability and communication integrity</strong></td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable reliable communications between its components. When desired, the architecture should provide a mechanism to guarantee that a message sent by a node has been fully and well received by its addressee.</td>
<td></td>
</tr>
<tr>
<td>QOS.2</td>
<td><strong>Priority routing</strong></td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable priority routing of time sensitive packets, such as alarm.</td>
<td></td>
</tr>
<tr>
<td>QOS.3</td>
<td><strong>Resilience</strong></td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be resilient to faults of its components.</td>
<td></td>
</tr>
<tr>
<td>QOS.4</td>
<td><strong>QoS integration</strong></td>
<td>4.2</td>
</tr>
<tr>
<td></td>
<td>When appropriate, the IoT6 architecture should use the Quality of Service (QoS) features supported by underlying networks.</td>
<td></td>
</tr>
</tbody>
</table>
### Security

<table>
<thead>
<tr>
<th>Section</th>
<th>Topic</th>
<th>WP1, WP3</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.1</td>
<td>Secured communication</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should provide mechanisms for secured and trusted communications.</td>
<td></td>
</tr>
<tr>
<td>SEC.2</td>
<td>Authentication and authorization</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture shall support authentication and authorisation mechanisms.</td>
<td></td>
</tr>
<tr>
<td>SEC.3</td>
<td>Data exchange confidentiality</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable encrypted communications.</td>
<td></td>
</tr>
<tr>
<td>SEC.4</td>
<td>Access control</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should provide mechanisms for access control only to authorized entities.</td>
<td></td>
</tr>
<tr>
<td>SEC.5</td>
<td>Security management</td>
<td>WP1, WP3</td>
</tr>
<tr>
<td></td>
<td>There should be systems for security management, including identity, authorisation, confidentiality, key exchange, audit trails, etc.</td>
<td></td>
</tr>
</tbody>
</table>
### 7.3 Service layer

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
<th>Related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interoperability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INT.1</td>
<td><strong>Heterogeneous integration</strong></td>
<td>WP3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should cope with heterogeneity and maximize interoperability across providers and consumers of information and services.</td>
<td></td>
</tr>
<tr>
<td>INT.2</td>
<td><strong>IoT6 components cooperation</strong></td>
<td>1.2, 3.3, 4.3, 7.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable its different connected components to interact and collaborate efficiently.</td>
<td></td>
</tr>
<tr>
<td>INT.3</td>
<td><strong>Shared IoT6 SOA and information model</strong></td>
<td>WP3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 service layer should provide a set of common services and information model to interact with the Service-Oriented Architecture and the connected components.</td>
<td></td>
</tr>
<tr>
<td><strong>Architecture of service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRV.1</td>
<td><strong>Client-server bi-directionality</strong></td>
<td>WP2, WP3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable 2-ways client-server communications. Where relevant, nodes should be able to work both as client and server.</td>
<td></td>
</tr>
<tr>
<td>SRV.2</td>
<td><strong>Push and pull compatibility</strong></td>
<td>WP2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should support push and pull communication modes. &quot;Push&quot; is understood as the capacity of an IoT6 node to pass information to another IoT6 node without prior request from the latter.</td>
<td></td>
</tr>
<tr>
<td><strong>Discovery and Look-up</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSC.1</td>
<td><strong>Resource directory</strong></td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should provide a resource directory listing and adveertising the IoT6 connected devices and services. It should enable the integration of newly connected devices.</td>
<td></td>
</tr>
<tr>
<td>DSC.2</td>
<td><strong>Scalable look-up and discovery</strong></td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable scalable look-up and discovery of IoT resources and</td>
<td></td>
</tr>
<tr>
<td>DSC.3</td>
<td><strong>Plug and play integration</strong></td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td>A new IoT6 device connected to the IoT6 architecture should be automatically identified and listed by the resource repository with a bootstrapping strategy.</td>
<td></td>
</tr>
<tr>
<td>DSC.4</td>
<td><strong>Semantics</strong></td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should be able to handle the semantics of its connected devices and services. It should enable users to create and change semantics and IoT6 connected components to exchange semantics.</td>
<td></td>
</tr>
<tr>
<td>DSC.5</td>
<td><strong>Subscription</strong></td>
<td>1.2, 3.1, 3.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable subscription to services and information updates.</td>
<td></td>
</tr>
</tbody>
</table>
### Self-management

<table>
<thead>
<tr>
<th>MAN.1</th>
<th>Self-management</th>
<th>2.1, 3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Self-configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable self-configuration of newly IoT6 connected components, enabling among other the new component to get an IP address and to register to the local resource directory.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAN.2</th>
<th>Self-management</th>
<th>2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IoT6 architecture should enable self-management of its IoT6 connected components, including with mobile ones.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAN.3</th>
<th>Self-healing</th>
<th>2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IoT6 architecture should provide self-healing properties, such as:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Identifying any connectivity problem on its network;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Providing alternative routing if an IoT6 node has a problem.</td>
<td></td>
</tr>
</tbody>
</table>

### Intelligence distribution

<table>
<thead>
<tr>
<th>DIS.1</th>
<th>Intelligence and service distribution</th>
<th>3.2, 1.2, 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IoT6 architecture should enable intelligence distribution, by enabling the integration of different services and by moving intelligence and service capabilities for filtering, pattern recognition, machine learning, decision-making towards the edges of the network. This requirement is also related to &quot;smart routing&quot; and ubiquitous access.</td>
<td></td>
</tr>
</tbody>
</table>

### Fault management

<table>
<thead>
<tr>
<th>FLT.1</th>
<th>Fault management and signaling</th>
<th>3.3, 2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IoT6 architecture should provide fault management and signaling.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FLT.2</th>
<th>Resilience</th>
<th>3.3, 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>After a non-destructive failure, e.g. after a power supply outage, an IoT6 device or gateway should immediately return in a full operating state autonomously, after performing the appropriate initialization (e.g. integrity check if supported).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FLT.3</th>
<th>Logging compatibility</th>
<th>3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IoT6 architecture should enable the logging of important messages and transactions. Important events (e.g. received information from the IoT6 device or the gateway is faulty, unsuccessful installation attempt from the device or the gateway, service not operating, etc.) may be logged together with diagnostic information. Logs shall be retrievable upon request.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration

<table>
<thead>
<tr>
<th>CONF.1</th>
<th>Configuration management</th>
<th>3.3, 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IoT6 architecture should provide configuration interfaces.</td>
<td></td>
</tr>
</tbody>
</table>
## 7.4 Application

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
<th>Related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Interoperability across applications</strong></td>
<td></td>
</tr>
<tr>
<td>APP.1</td>
<td><strong>Reuse of virtual representation of entities</strong></td>
<td>4.1, 4.2, 4.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should allow for re-use of virtual object entities in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the physical world across several application domains.</td>
<td></td>
</tr>
<tr>
<td>APP.2</td>
<td><strong>Multiple applications integration</strong></td>
<td>WP6</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable multiple applications integration and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interactions.</td>
<td></td>
</tr>
<tr>
<td>APP.3</td>
<td><strong>Common ontology</strong></td>
<td>WP3, WP4</td>
</tr>
<tr>
<td></td>
<td>Where relevant, the IoT6 architecture should provide a common ontology.</td>
<td></td>
</tr>
<tr>
<td>APP.4</td>
<td><strong>Reliable alert channels</strong></td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable the transmission without delay of alerts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with Quality of Service, with a high level of reliability and a priority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmission.</td>
<td></td>
</tr>
<tr>
<td>APP.5</td>
<td><strong>Mobile components tracking</strong></td>
<td>6.1, 6.2, 6.3,</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable the localization of mobile devices.</td>
<td>2.3, 3.1</td>
</tr>
<tr>
<td>APP.6</td>
<td><strong>Services integration</strong></td>
<td>6.2, 6.3</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture should enable the integration of services such as the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smart Things Information Service. It should include the possibility for a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device to connect to a remote service, and for a service to connect to a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>remote device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Privacy and confidentiality</strong></td>
<td></td>
</tr>
<tr>
<td>PRI.1</td>
<td><strong>Privacy compliance</strong></td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The IoT6 architecture shall enable appropriate privacy management of data,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>including the possibility to provide end-user with control on their personal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>data dissemination, the possibility to anonymize the personal data, and the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>possibility to provide a secured private</td>
<td></td>
</tr>
<tr>
<td>PRI.2</td>
<td><strong>Data ownership</strong></td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>The architecture should enable an effective data ownership management,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>including among others the possibility for a person to mark his ownership</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on a data (including through an anonymized ID of pseudo), and the possibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>for a user to decide with whom he/she wishes to share specific information.</td>
<td></td>
</tr>
</tbody>
</table>
[8] Conclusion

This report has reviewed and taken into account different sources of requirements in order to elaborate a list of 56 synthetic requirements to be addressed by the IoT6 research project. It constitutes a conceptual framework to guide the IoT6 architecture design, in order to make it as adequate as possible for the future Internet of Things.

Five use-case scenarios have been designed in order to illustrate various dimensions of the IoT architecture. The use cases are expected to evolve and to be enriched with the results of the IoT6 research works. The use-case scenarios have already enabled the fine tuning of the synthetic requirements, as well as the identification of key components and protocols to be considered in the frame of the research project.

Finally, the survey with the delegates and the IoT6 Industry Advisory Board inputs have both confirmed the importance of personal data privacy. This will be taken into account in the subsequent work packages.
[9] References


Annexes

10.1 Privacy interview questionnaire

Mandat International is involved in two scientific research projects with several European universities. These projects aim to communicate between objects installed in our facilities to reduce the building energy consumption, increase the security and provide new services to delegates. An important part of the project is to respect the privacy of delegates. We want to hear your opinion and advices:

1) On which continent do you live?

2) In the context of this project, what are for you the three main concerns in terms of data protection?
   1.
   2.
   3.

3) In the context of this project, what are for you the three main actions that should be taken to protect the privacy and personal data?
   1.
   2.
   3.

4) What kinds of services would you expect from an intelligent building management system?
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Totally against</th>
<th>Rather against</th>
<th>No opinion</th>
<th>Rather for</th>
<th>Totally for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you support technological innovations?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Would you agree that the following information is transmitted to the building management system that will control and optimize energy consumption; these data are not accessible to third parties?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicate whether the room is occupied?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicate who is in the room?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicate where is a person in the building?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicate the energy consumption of a room?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Would you agree that information on energy consumption of the building are available:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to yourself?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to building managers?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to delegates actually in the center?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to universities?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to the public?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Would you agree to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use your mobile phone to connect to the building?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive information from the central system to your mobile phone?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think the data should be anonymised as much as possible?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you ready to share personal information to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save energy?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide access control and security to the delegates?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve comfort?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitate networking with other delegates?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) What is the confidentiality level of your location?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Fairly public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Fairly private</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Very private</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10.2 IoT6 Industrial Advisory Board questionnaire

The replies will not be published and will be kept confidential, but will help us to align the IoT6 developments with our industrial partners’ specific interest, needs and requirements. It will also serve to identify relevant use cases to be addressed and implemented by IoT6.

Partner name:
Contact person:
E-mail address:
Phone number:
Date:

1) Could you mention 3 to 5 devices (or services) from your company which are (or could be) connected to an IP network?

1. **Device/service name:**
   - Is it or could it become IPv6 enabled (precise)?
   - Does it require maintenance work?
   - If so, what information could be useful to identify when a maintenance work is required?

2. **Device/service name:**
   - Is it or could it become IPv6 enabled (precise)?
   - Does it require maintenance work?
   - If so, what information could be useful to identify when a maintenance work is required?

3. **Device/service name:**
   - Is it or could it become IPv6 enabled (precise)?
   - Does it require maintenance work?
   - If so, what information could be useful to identify when a maintenance work is required?

4. **Device/service name:**
   - Is it or could it become IPv6 enabled (precise)?
   - Does it require maintenance work?
   - If so, what information could be useful to identify when a maintenance work is required?

5. **Device/service name:**
   - Is it or could it become IPv6 enabled (precise)?
   - Does it require maintenance work?
   - If so, what information could be useful to identify when a maintenance work is required?
2) What key functional and technical requirements would you expect from an architecture that would interconnect your devices/services by your customers to other devices/services, to your company and/or to third parties?

3) Let’s consider that IoT6 architecture would enable the full interconnection and integration of your devices/services with other devices/services. What kind of innovative interactions would you like to implement? Feel free to propose several examples.

4) Do you foresee any cost (for yourself or your customer) that could be reduced through such interactions? Feel free to propose several examples.

5) What are your main expectations regarding IoT6?

6) Would you have any suggestion for the project or for the Industry Advisory Board?