ISO/IEC JTC 1/SWG 5
Internet of Things (IoT)
Secretariat: KATS (Korea, Republic of)

Document type:	Other document (Open)
Title:	Report of SWG-P on Ubiquitous Computing enabling Internet of Things (IoT)
Status:	This document was published by JTC 1/SWG-P in 2012 and will be presented in the 1st SWG-IoT meeting.
Date of document:	2013-01-30
Source:	SWG on Planning
Expected action:	INFO
No. of pages:	42
Email of secretary:	khj@etri.re.kr
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1swg5

ISO/IEC JTC 1
Information technology
Secretariat: ANSI (USA)

Document type:	Other document (Defined)
Title:	Report of SWG-P on Ubiquitous Computing
Status:	This document is circulated to JTC 1 National Bodies for review and consideration at the November 2012 JTC 1 Plenary in Jeju.
Date of document:	2012-10-02
Source:	SWG-P
Expected action:	ACT
Action due date:	2012-11-05
Email of secretary:	lrajchel@ansi.org
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1

ISO/IEC JTC 1/SWG 3
Planning
Secretariat: DIN

Replaces:	N 369
Document type:	Other document (Defined)
Title:	Report on "Ubiquitous Computing enabling Internet of Things" -- Final Version
Status:	The document contains the report of ISO/IEC JTC 1/SWG 03 on Planning on "Ubiquitous Computing enabling Internet of Things" to the JTC 1 Plenary 2012 in Jeju, Republic of Korea. The report was submitted to JTC 1 on 2012-09-27. The report was adopted at the 25 September 2012 conference call of SWG on Planning and is circulated in SWG on Planning for information and reference.
Date of document:	2012-09-26
Source:	JTC 1 Special Working Group on Planning
Expected action:	INFO
Email of secretary:	cord.wischhoefer@din.de
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1swg3

Ubiquitous Computing enabling Internet of Things

September 2012 (Final)

ISO/IEC JTC 1 SWG-Planning[1]

[1] Editor: Sangkeun YOO (ETRI, Republic of KOREA), lobbi@etri.re.kr

1. Scope

Currently various, visionary technology domains have been introduced so far such as Internet of Things (IoT) [1], Machine-to-Machine communication (M2M) [2], Smart Device Communications (SDC) [3], Machine-Oriented Communication (MOC) [4], Ubiquitous Sensor Network (USN) [5], and Ubiquitous Computing [6]. The Internet of Things is understood as a concept like an umbrella which may accommodate the others and may be realized by them while Ubiquitous Computing may be considered as the whole capability of gaining and/or transmitting data from the physical world; producing information; exploiting knowledge; and provisioning wisdom to end-users.

This document provides an overall review on the specified topics of Ubiquitous Computing and Internet of Things in terms of exploring standardization opportunities for JTC 1.

This report aims at:

- reviewing current definitions and scopes of Ubiquitous Computing within and Internet of Things within and outside JTC 1;
- reviewing the related technologies for Ubiquitous Computing and Internet of Things;
- reviewing standardization activities in international standardization bodies, consortia and fora where specifications related to Ubiquitous Computing and Internet of Things are being developed;
- identifying standardization gaps for progress of Ubiquitous Computing and Internet of Things; and,
- proposing prospective standardization areas and topics toward ISO/IEC JTC 1.

2. References

This report refers to the following standards, specifications, articles and papers:

[1] Pre-published Recommendation ITU-T Y.2060, “Overview of Internet of Things”

[2] ETSI TS 102 689, “Machine-to-Machine communications (M2M); M2M service requirements”

[3] TIA TR-50, “Smart Device Communications”

[4] Pre-published Recommendation ITU-T Y.2061, “Requirements for support of machine oriented communication applications in the NGN environment”

[5] ITU-T Y.2221, “Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment”

[6] WIKIPEDIA, “Ubiquitous Computing”, November 2008, http://en.wikipedia.org/wiki/Ubiquitous_computing

[7] Mark Weiser, “Hot Topics: Ubiquitous Computing”, IEEE Computer, October 1993

[8] CASAGRAS, “RFID and the Internet of Things: Enablers of Ubiquitous Computing and Network”

[9] ISO/IEC 29182-2, “Sensor Network Reference Architecture (SNRA) – Part 2: Vocabulary and Terminology”

[10] ISO/IEC 29182-1, “Sensor Network Reference Architecture (SNRA) – Part 1: General overview and requirements”

[11] ITU-T Y.2002, "Overview of ubiquitous networking and of its support in NGN"

[12] CERP-IoT, "Vision and Challenges for Realising the Internet of Things", March 2010

[13] ISO/IEC 29172, "Automatic identification and data capture techniques – Mobile item identification and management – Reference architecture for Mobile AIDC services"

[14] David Boswarthick, ETSI Technical Officer for TC M2M, "M2M Activities in ETSI", SCS Conference, Sophia 2nd July 2009

[15] 3GPP TS 22.368, "Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 11)"

[16] 3GPP TR 23.888, "System Improvements for Machine-Type Communications; (Release 11)"

[17] German Industry association for M2M-technology

[18] WIKIPEDIA, "Service-Oriented Architecture," April 2009, http://en.wikipedia.org/wiki/Service-oriented_architecture

3. Terms and definitions

3.1. Terms defined elsewhere

This report uses the following terms defined elsewhere:

3.1.1. actuator [ISO/IEC 29182-2]

device that provides a physical output in response to an input signal in a predetermined way

3.1.2. Internet of Things (IoT) [ITU-T Y.2060 (pre-published)]

A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.3. Machine-to-Machine communication (M2M) [ETSI TS 102 689]

communication between two or more entities that do not necessarily need any direct human intervention. M2M services intend to automate decision and communication processes

3.1.4. Machine type communication (MTC) [3GPP TS 22.368]

form of data communication which involves one or more entities that do not necessarily need human interaction

3.1.5. Machine-oriented communication (MOC) [ITU-T Y.2061 (pre-published)]

A form of data communication between two or more entities in which at least one entity does not necessarily require human interaction or intervention in the process of communication

3.1.6. Mobile Item Identifier (MII) [ISO/IEC 29172]

realization of Unique Item Identifier for unique identification of entities to be provided as consumer-oriented information services within mobile telecommunication environments

3.1.7. next generation network (NGN) [ITU-T Y.2001]

A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.8. sensor [ISO/IEC 29182-2]

device that observes and measures a physical property of a natural phenomenon or man-made process and converts that measurement into a signal

3.1.9. sensor network gateway [ISO/IEC 29182-2]

sensor network element that connects a sensor network to another network with different architectures or protocols, permitting information exchange between them

3.1.10. sensor node [ISO/IEC 29182-2]

sensor network element that includes at least one sensor and, optionally actuators with communication capabilities and data processing capabilities

3.1.11. ubiquitous sensor networks (USN) [ITU-T Y.2221]

A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness

3.2. Terms defined in this report

This report uses defines the following terms:

N/A

4. Abbreviations, acronyms and conventions

This report uses the following abbreviations and acronyms:

AIDC	Automatic Identification and Data Capture
M2M	Machine-to-Machine
MII	Mobile Item Identifier
MTC	Machine Type Communication
NGN	Next Generation Networks
ODS	Object Directory Service
ONS	Object Naming Service
RFID	Radio Frequency Identification
SOA	Service-Oriented Architecture
UII	Unique Item Identifier
USN	Ubiquitous Sensor Networks
W3C	World Wide Web Consortium

5. Introduction to Ubiquitous Computing

5.1. Definitions of Ubiquitous Computing

It is not easy to define Ubiquitous Computing exactly because the notion of Ubiquitous Computing encompasses a lot of ICT (Information and Communications Technologies), ideas and concepts. None the less, there has been the consensus that Ubiquitous Computing is the new paradigm of information society rather than the new technology.

From the various sources including mainly [6], [7] and [8], we can have the definition of Ubiquitous Computing as follows:

- It is a new wave in computing, in which technology becomes invisible in our lives by integration into common objects and activities. Instead of a person being active on a single personal computer at one moment in time, objects used in ordinary daily activities will be pervasively embedded with interconnected computational devices and intelligent systems. Someone *using* Ubiquitous Computing engages many computational devices and systems simultaneously, in the course of ordinary activities, and may not necessarily even be aware that they are doing so.

As seen in the definition above, the phrase Ubiquitous Computing does not define any specific technologies, but it expresses a paradigm shift away from the *visible* user-centric aspects of computing towards the *invisible* intelligence of computing and networks. That is, the paradigm shift is realized by Ubiquitous Computing capability of gaining and/or transmitting data from the physical world; producing information via appropriate data processing; exploiting knowledge from the information; and provisioning wisdom to end-users. (Figure 1)

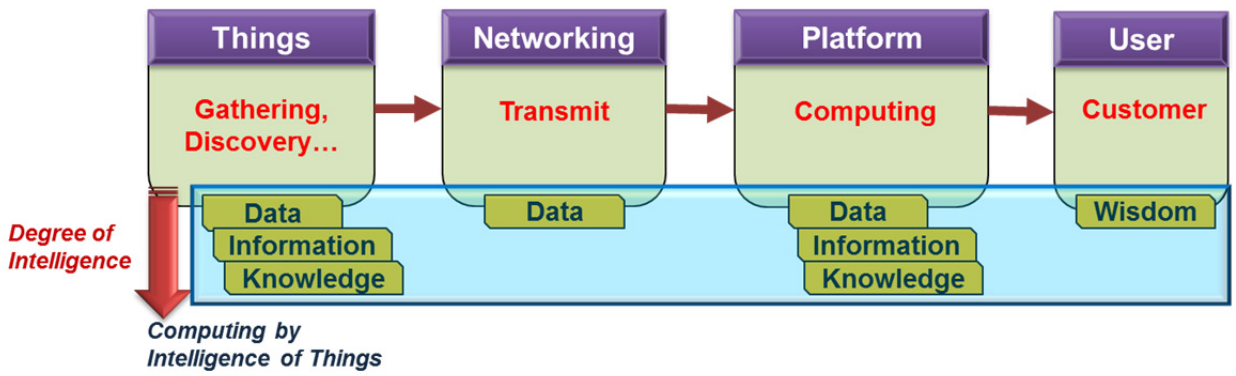

Figure 1 – Ubiquitous Computing enabling Internet of Things

This paradigm is also described as *pervasive computing*, *ambient intelligence*, and more recently, *everyware*, where each term emphasizes slightly different aspects. When primarily concerning the objects involved, it is also described as *physical computing*, the *Internet of Things*, *haptic computing*, and *things that think*. [6]

5.2. Scopes of Ubiquitous Computing

The scopes of Ubiquitous Computing are widely spread over all areas of computer science, including hardware components (e.g. chips), network protocols, interaction substrates (e.g. software for screens and pens), applications, privacy, and computational methods. [1] In order to realize Ubiquitous Computing, a wide range of technologies must be combined, such as sensor networks, ubiquitous networking, RFID, M2M, mobile computing, human-computer interaction, and wearable computers.

Though Ubiquitous Computing involves various kinds of technologies, the essence of Ubiquitous Computing is the knowledge of our surroundings (*called context awareness*). By knowing the surroundings, including the situation involving users and environmental condition, computer systems can offer useful customized services to the users which can be humans or machines.

6. Related technologies

As explained in clause 5, Ubiquitous Computing is not concrete and specific technology terms but abstract and conceptual ones. A set of technologies may be involved to realize Ubiquitous Computing and this clause summarizes a set of "key" technologies to be needed for realizing Ubiquitous Computing.

6.1. Sensor networks

ISO/IEC 29182-2 [9] defines the sensor networks as a system of spatially distributed sensor nodes interacting with each other and, depending on applications, possibly with other infrastructure in order to acquire, process, transfer, and provide information extracted from its environment with a primary function of information gathering and possible control capability where:

- sensor node:
  sensor network element that includes at least one sensor and, optionally actuators with communication capabilities and data processing capabilities

- sensor:
  device that observes and measures a physical property of a natural phenomenon or man-made process and converts that measurement into a signal

- actuator:
  device that provides a physical output in response to an input signal in a predetermined way

Typically, the sensor networks gather information about their physical surroundings and deliver this information to the sensor network user(s), and any of the communications links between sensor nodes may be implemented using wired or wireless technologies.

Figure 2 depicts a standalone sensor network that operates on its own and is isolated from other networks.

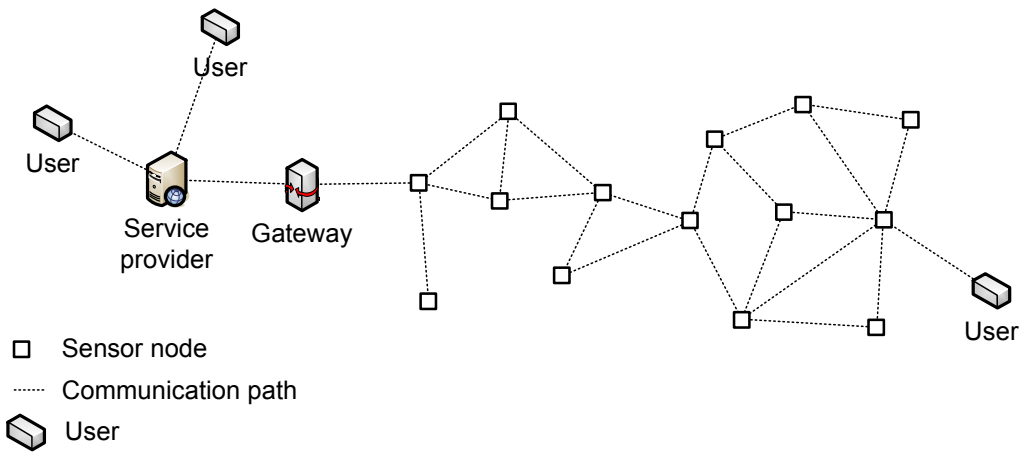

Figure 2 – Standalone sensor network [10]

Figure 3 shows the case where multiple sensor networks, two in the case of this figure, are interconnected via a sensor network gateway. Sensor network gateways can play various roles in a sensor network, as shown in Figure 2 and Figure 3 and shortly in Figure 4.

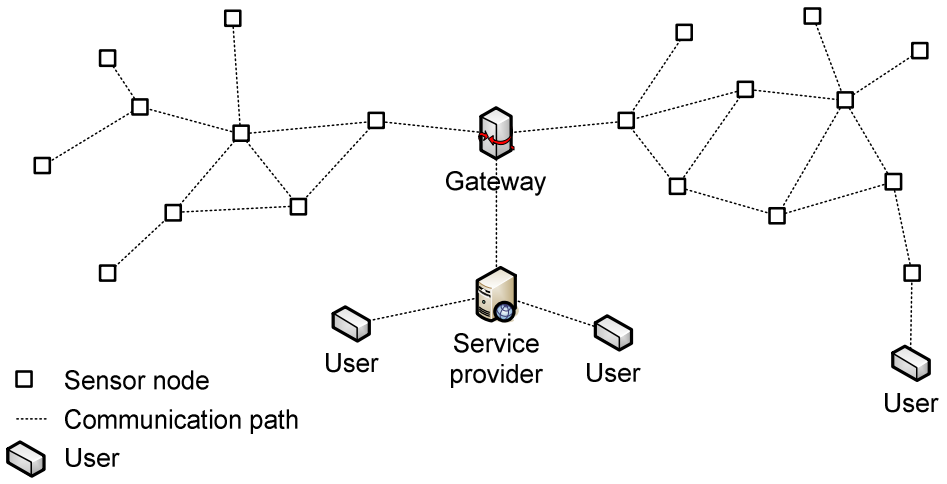

Figure 3 – Interconnected sensor networks [10]

Figure 4 represents sensor networks, two in the case of this figure, which are connected to a backbone network or other entities. In this case, sensor network gateways provide sensor networks with connectivity to other networks possibly through access networks.

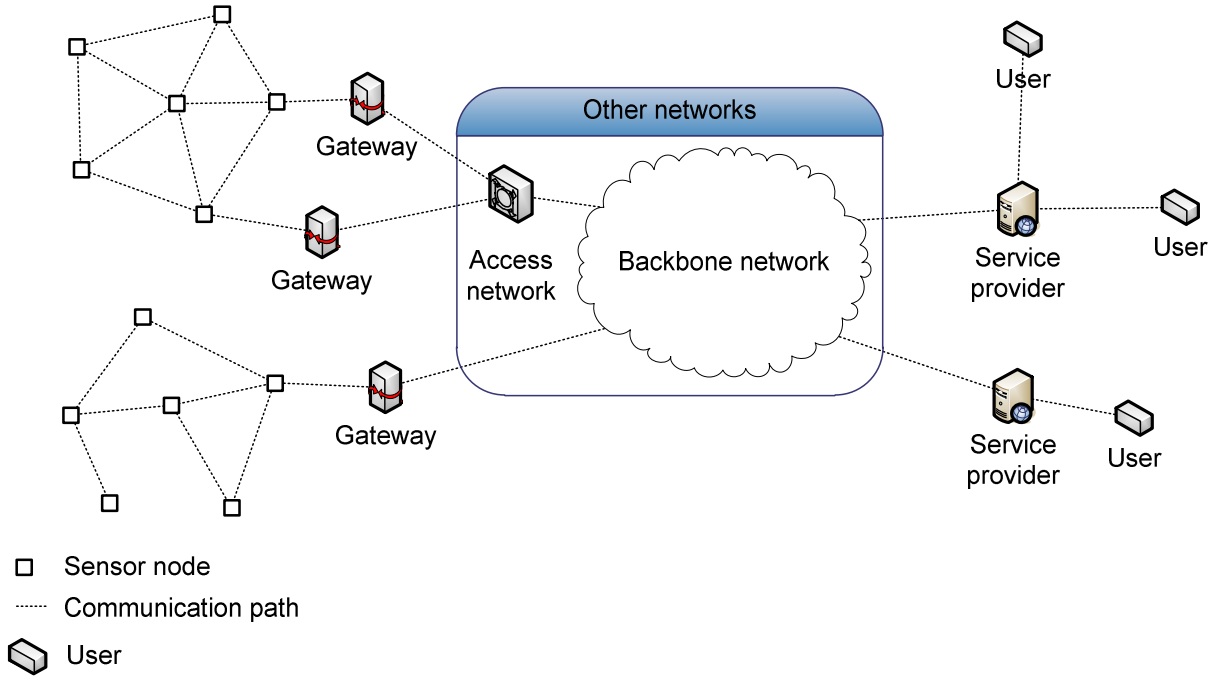

Figure 4 – Sensor networks connected to other networks [10]

Sensor network applications may require application-layer technologies such as data processing (data integration, data filtering), sensor information description and presentation. Data is acquired by sensor nodes and either processed within the sensor network (e.g., sensor nodes in the sensor

network) or by service providers connected to the sensor networks. Alternatively it can be transferred, through a backbone network, to applications and other entities such as service providers.

As for service provisioning, sensor network services may be provided either by a sensor node directly or by a service provider. Users may request services, without an intermediary, from an arbitrary or a designated sensor node or from a service provider. A service provider gathers sensor data either from sensor networks directly or through a backbone network and facilitates the negotiation of the service to be provided. In some cases, a user that requests services from a sensor node may be integrated with that sensor node.

ISO/IEC 29182-1 [10] summarized the unique characteristics of sensor networks as follows:

- Service provisioning for individual requirements:
  Sensor network applications and services allow arbitrary and evolving types and grouping of users. For example, weather information may be provided to consumers such as tourists and fishermen as well as business partners such as airlines, shipping companies and travel agencies. Functions and services provided by sensor networks may be quite diverse supporting many applications, market segments and types of users.

- Data gathering and pre-processing:
  Sensor nodes gather data from the physical world and pre-process the sensed data (e.g., through data integration or filtering) and then supply sensor network services to the user, either directly from the sensor node or via a service provider.

- Collaborative information processing:
  In some sensor network applications, the sensor nodes may collaborate to solve complex sensing problems such as the detection, classification and tracking of objects in the physical world. The data from a sensor may be pre-processed and refined at the sensor node acquiring the sensed data or at another sensor node. Depending on the application, intermediate data, such as features or estimated parameters, may be extracted from the sensed data during the pre-processing. The results from this pre-processing may be shared among the sensor nodes in the sensor network. Once shared, the intermediate data from multiple sensor nodes can be transformed into context data and situation information by data fusion.

- Maintenance-free operation:
  Sensor networks may have to operate for a long period of time without maintenance or technical support to resolve problems. Provision of remote diagnostics and resolution may be required.

- Dynamic network topology:
  The topology of a wireless sensor network is rarely fixed. A sensor network may have to adapt to the availability of communication links between sensor nodes, to the changing positions of sensor nodes due to mobility, to energy levels (e.g., a node may drop out as its battery runs out) and to the changing of the roles of sensor nodes (e.g., when a sensor node becomes to take the roles of a sensor network gateway). Implementations where sensor nodes move within the network require routing and communication protocols that are flexible and quick to response to changes. Sensor network topologies have to be capable of handling sensor nodes leaving or joining the network without unmanaged degradation of sensor network performance. Some sensor network topologies are self-healing and self-organizing.

- Energy efficiency and operating lifetime:
  Energy management is important in many sensor networks where the sensor nodes are battery-operated and it is desirable for the network to be operational for as long as possible. Energy harvesting technologies may help with energy management and extending network lifetime.

- Self-adaptation:
  Sensor networks may self-adapt to accommodate changing conditions, to support robustness and reliability and to optimize resource management and sensor node functionality.

From the nature of Ubiquitous Computing, the knowledge of user's surroundings (context awareness) is regarded as one of key features for supporting Ubiquitous Computing services and there is no doubt that sensors network technology supporting context awareness will be one of key enablers for Ubiquitous Computing.

6.2. Ubiquitous networking

ITU-T Y.2002 [11] describes ubiquitous networking as follows:

- The ability for persons and/or devices to access services and communicate while minimizing technical restrictions regarding where, when and how these services are accessed, in the context of the service(s) subscribed to.

Ubiquitous networking is the networking capabilities which are needed to provide the support of various classes of applications/services which require "any services, any time, any where and any objects" type of operation.

Shortly, ubiquitous networking provides seamless communication capabilities of "anything" (e.g., persons and objects). Ubiquitous networking encompasses the following:

- ubiquitous connectivity allowing for whenever, whoever, wherever, whatever types of communications;

- pervasive reality for effective interface to provide connectable real world environments;

- ambient intelligence allowing for innovative communications and providing increased value creation.

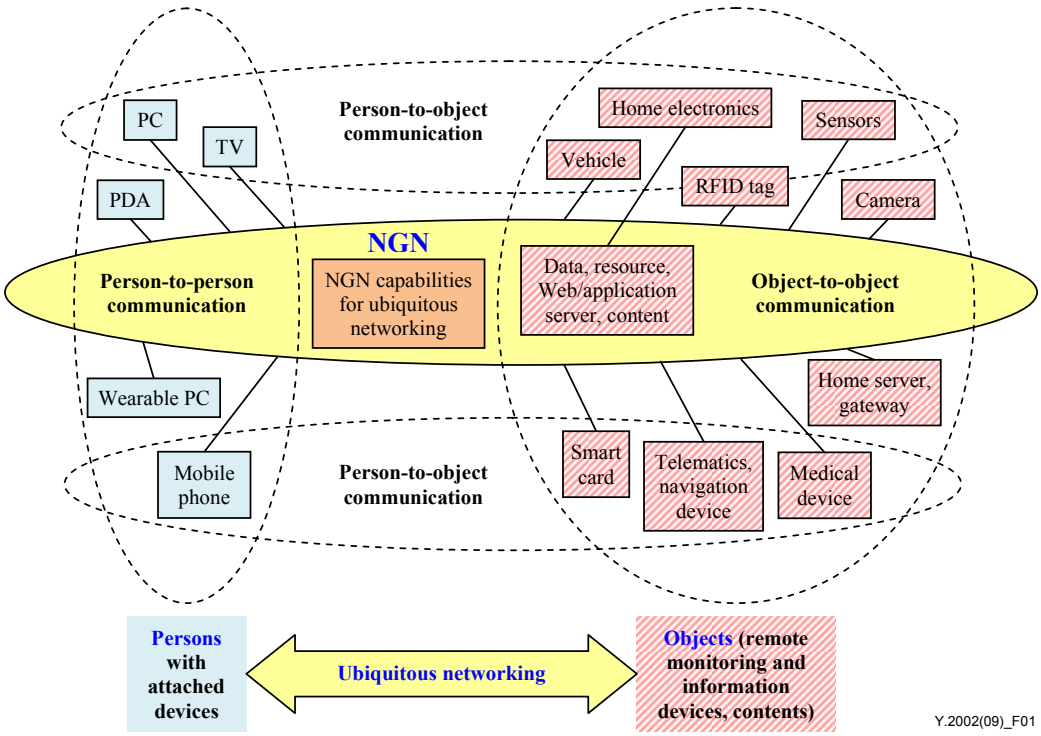

Figure 5 – Ubiquitous networking communication types [11]

As shown in Figure 5, there are three types of communications in ubiquitous networking.

- person-to-person communication:
  persons communicate with each other using attached devices (e.g., mobile phone, PC)

- person-to-object communication:
  persons communicate with a device in order to get specific information (e.g., IPTV content, file transfer)

- object-to-object communication:
  an object delivers information (e.g., sensor related information) to another object with or without the involvement of persons

These three types of communication seem to cover the all types of communication in Ubiquitous Computing. ITU-T Y.2002 [11] explains the fundamental characteristics of ubiquitous networking as follows:

- IP connectivity:
  IP connectivity will allow objects involved in ubiquitous networking to communicate with each other within a network and/or when objects have to be reachable from outside their network.

- Personalization:
  Personalization will allow to meet the user's needs and to improve the user's service experience since delivering appropriate contents and services to the user.

- Intelligence:
  Intelligence which enables network capabilities to provide user-centric and context-aware service is essential and artificial intelligence techniques in networks will help to accelerate

the synergies and ultimately the "fusion" between the involved industries (e.g., the car industry, semi-conductor industry or medical industry).

- Tagging objects:
  Radio frequency identifier (RFID) is one of tag-based solutions for enabling real-time identification and tracking of objects. Tag-based solutions on ubiquitous environment will allow to get and retrieve information of objects from anywhere through the network.

- Smart devices:
  Smart devices attached to networks can support multiple functions including cameras, video recorders, phones, TVs, music players. Sensor devices which enable detection of environmental status and sensory information can utilize networking functionalities to enable interconnection between very small devices, the so-called 'smart dusts'. Specific environments such as homes, vehicles, and buildings will also require adaptive smart devices.

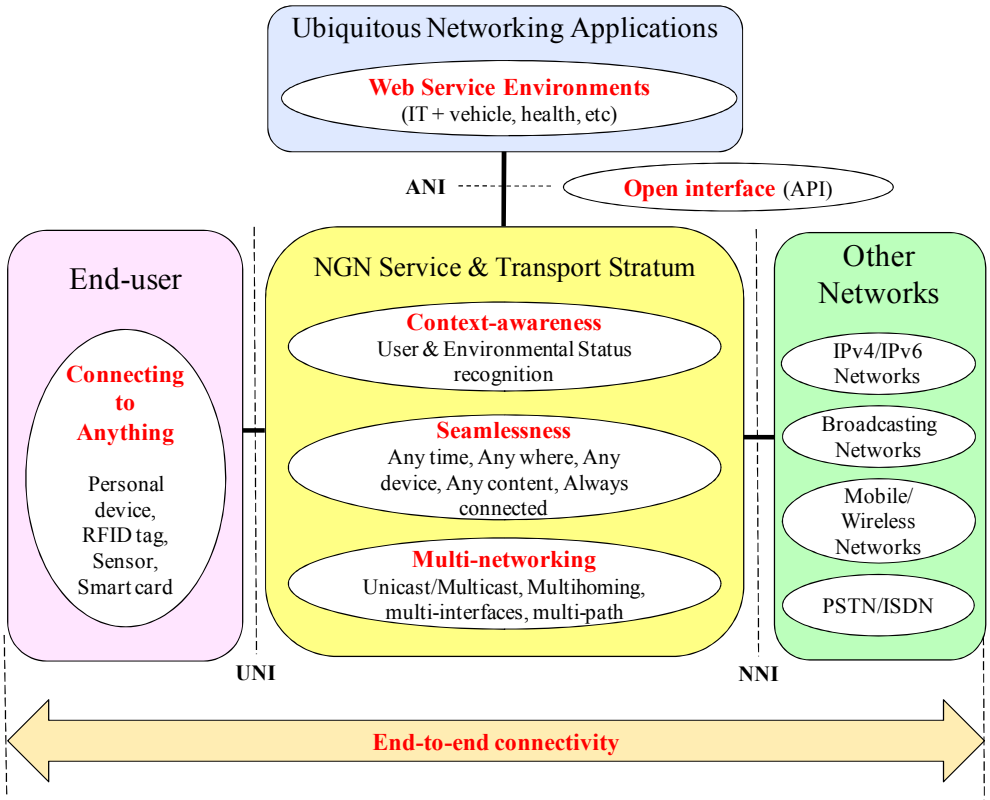

Figure 6 – High-level architectural model for ubiquitous networking in NGN [11]

Figure 6 depicts the high-level architectural model for ubiquitous networking in NGN. In this diagram, a core network (NGN) provides some capabilities such as context-awareness, seamless connectivity and multi-networking which are required in Ubiquitous Computing.

6.3. RFID

RFID is a generic term for technologies that use radio waves to remotely store and retrieve data between interrogator and transponder. In current commercial applications, the interrogator is usually called a reader or reader/writer and the transponder is often called a tag (depending on its size). In other words, RFID is a combined term with RF and ID where RF indicates a wireless communication technology and ID means identification information. [8]

Although some of the underlying technologies for RFID have been around for more than half a century and both technically feasible and practically usable solutions have appeared already more than a decade ago, only recently have supply chain partners started to explore its potential to support core business processes. This shift of attention should be primarily attributed to the decrease of acquisition costs for the technology parts (readers, tags and printers), the availability of related services and functionalities, as well as the emergence of proof-of-concept application prototypes by large retailers and suppliers. Currently, RFID is emerging as an important technology for revolutionizing a wide range of applications, including supply-chain management, retail sales, anti-counterfeiting, and healthcare. [12]

Traditionally RFID technologies have been explored in B2B (Business to Business) domain, however the potential to read RFID tags with mobile devices has always been possible in the industrial and commercial sector. Especially, the advent of smart phones will make acceleration of developing RFID applications in B2C (Business to Consumer) domain and this is called “mobile RFID”. The meaning of “mobile RFID” may confuse the readers. It does not mean that RFID is mobile and flowing, but it is a simply combined term of RFID and mobile telecommunication.

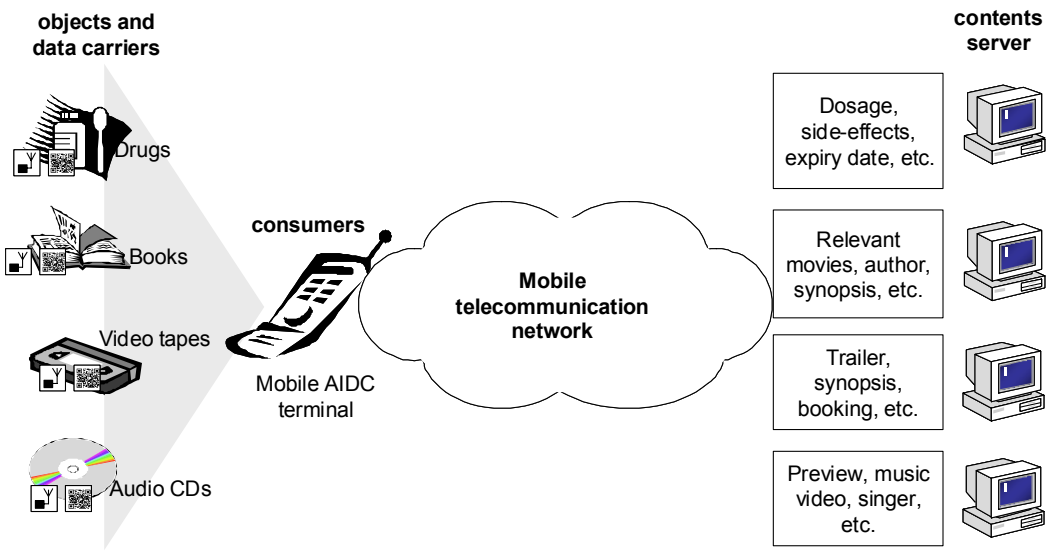

Figure 7 – Use cases of Mobile RFID applications and services [13]

Figure 7 shows four examples of B2C RFID applications/services models.

The procedures that a user with mobile RFID terminal gets information from RFID tags are summarized as follows:

1. Data reading:
   A mobile RFID device reads tag data from a data carrier and;
2. MII (or UII) identifying:
   A mobile RFID learns what type of ID schemes is used for a given MII. Learning what type of ID scheme is used means not only learning its identity but also getting its format and structure information;
3. MII (or UII) resolving:
   Usually ID schemes appear in the form of a series of numbers or alphanumeric characters. An MII assigned by such ID schemes does not have application-specific meaning until it is associated with certain information for a target object to which the MII is allocated. This association is resolved by the MII resolution. MII resolution is carried out between a mobile RFID terminal and an external directory service (e.g., EPCglobal’s ONS or ISO/IEC 29177

ODS). The input data for an MII resolution is an MII and the output data is associated information (e.g., information content like audio, video, text or image, or access information like a URI). However, the output data of MII resolutions is usually URIs because the information are most often provided by web technologies and retrieved through URIs by information browsers;

4. Information retrieving:
   The information retrieving operation is initiated by the information browser . Typical examples of the information browser are mobile web browsers supporting conventional web information access.

There are many types of RFID tags that use different radio frequencies and different protocols. In Ubiquitous Computing, there are right tags for given situations. In a typical Ubiquitous Computing application, there is usually a constraint on the physical characteristics of the objects in which RFID tags is attached or embedded. Application requirements and the physical characteristics favor a different type of radio frequency usage. For example [8],

- If the object has water-rich contents (water-rich food product, liquid medicine bag, etc.), it is needed to use relatively lower radio frequency for communication between the tag and the reader.
- If RFID tags are used for precise positioning purposes such as in location-aware information services, then it is needed to use relatively high 2GHz bands to achieve the high accuracy of 20-30 centimeters.
- If the tags are attached to metal objects, it is required to pay attention to the way the tags are attached to the surface of metal objects, the shape of antennae of the tags and the frequency used.
- Different regions of the world impose different usage restrictions: frequencies, allowed power, etc.

For these reasons, it is a must to use different types of tags for different applications in the Ubiquitous Computing environment.

From the fact that infrared and optical tags (linear barcodes or 2D barcodes) are widely used in the identification application domains, RFID tags are not the only useful containers or carriers for identification information in the Ubiquitous Computing environment.

However, RFID tags have the advantages of being readable concurrently, and are relatively resistant to scratching which makes optical tags unreadable, moreover supports distant reading form the tags. These features make RFID technologies one of key enablers for Ubiquitous Computing.

6.4. M2M (including MTC)

ETSI TS 102 689 **Fehler! Verweisquelle konnte nicht gefunden werden.** defines M2M communication as the communication between two or more entities that do not necessarily need any direct human intervention. M2M services intend to automate decision and communication processes.

M2M technology is very similar to sensor network technology from the perspective that the M2M devices gather information about their physical surroundings and deliver this information to the M2M severs, then the M2M servers provide information extracted from its environmental information and possible control capability. Many articles and standards about M2M describe that

M2M devices installed with sensor(s) gather information about physical surroundings and deliver this information to a remote entity which is called an M2M server.

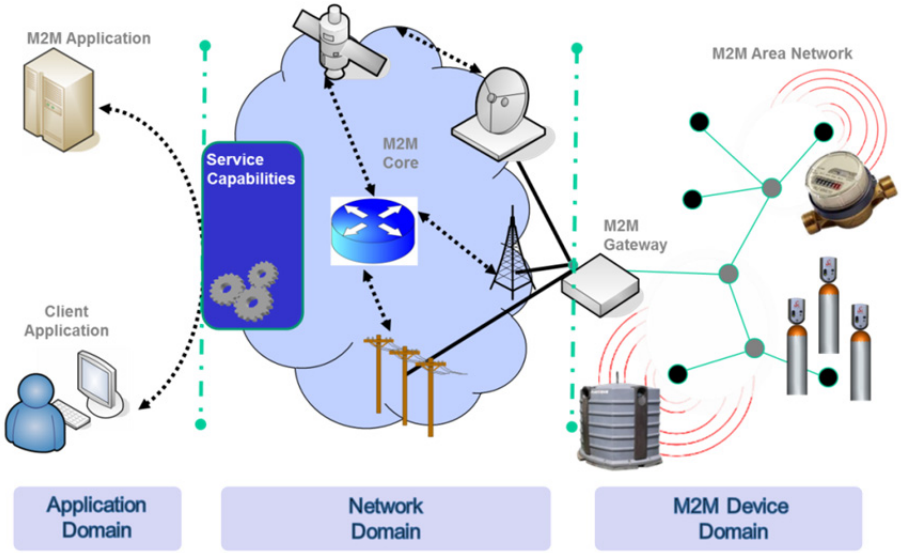

Figure 8 – Simple M2M architecture [14]

Figure 8 shows a simple M2M architecture composed of three domains; application domain, network domain and M2M device domain. An application domain holds M2M users, client applications, M2M applications in M2M servers. Access network, core network and M2M servers supporting service capabilities reside in a network domain. An M2M device domain covers M2M area networks providing connectivity between M2M devices and M2M gateways. At a glance, Figure 8 resembles Figure 4 of sensor networks.

3GPP [15] also defines MTC as a form of data communication which involves one or more entities that do not necessarily need human interaction. The definition of MTC seems to be identical with the definition of M2M. The objective of 3GPP MTC is to develop standards concerned with M2M core of Figure 8 under mobile telecommunication network environment, so called 3GPP systems.

Figure 9 depicts 3GPP architecture for MTC.

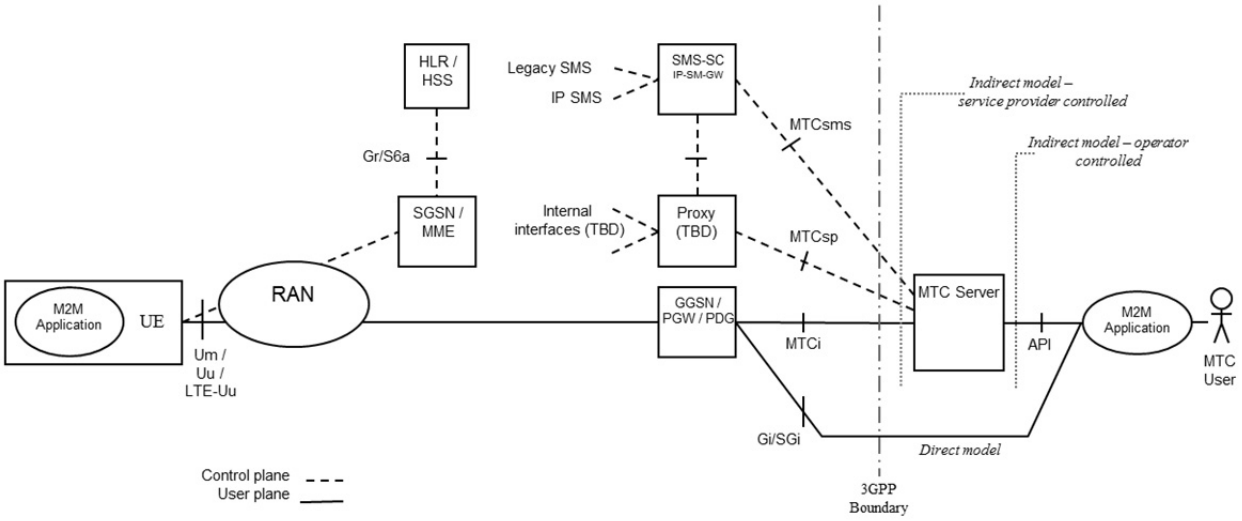

Figure 9 – 3GPP architecture for Machine-Type Communication [16]

The important issues of M2M lie in the business models for broad market penetration, wireless carrier services, and the regulatory surroundings. Although technology for M2M already exists, many separate technologies are needed to be integrated in order to make M2M become reality. Myriads of sensor nodes, RFID tags, their middleware and applications using Web Services must be mixed in an appropriate manner. [8]

From the functionalities and possibilities arising through M2M, an Internet of Things is formed, or an Internet of intelligent objects. [8][17]

Again, the knowledge of user's surroundings (context awareness) is essential to Ubiquitous Computing services. M2M will definitely support this feature and be one of key enablers for Ubiquitous Computing.

6.5. Internet of Things

During the development of ITU-T Y.2060 **Fehler! Verweisquelle konnte nicht gefunden werden.**, there was a severe debate on the definition of Internet of Things. Some people said that Internet of Things is a kind of concept, however some people understood Internet of Things as a technology, moreover there were opinions that Internet of Things should be regarded as an infrastructure for many ICT services.

As a conclusion of the definition of IoT, IoT can be described as follows **Fehler! Verweisquelle konnte nicht gefunden werden.**:

- A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies

  NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
  NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

As shown in Figure 10, the IoT is adding the dimension of "Any THING connection" to the world of information and communication technologies (ICTs) which already provides anytime and anyplace connection. **Fehler! Verweisquelle konnte nicht gefunden werden.**

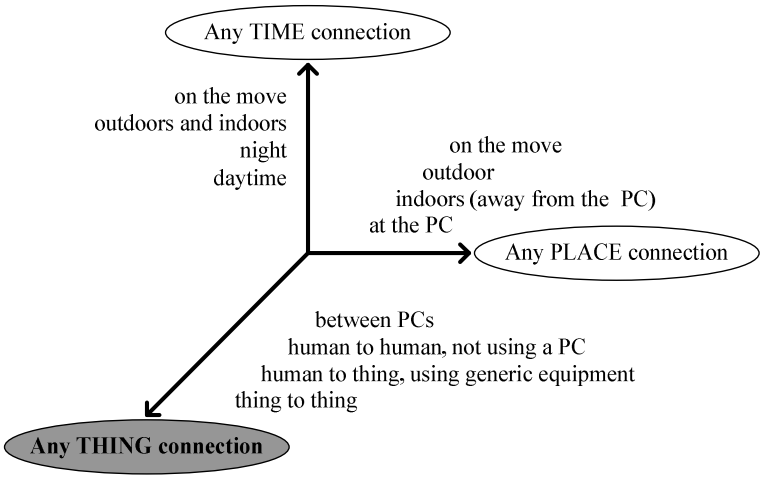

Figure 10 – The new dimension introduced in the Internet of Things **Fehler! Verweisquelle konnte nicht gefunden werden.**

Figure 11 shows the technical overview of IoT.

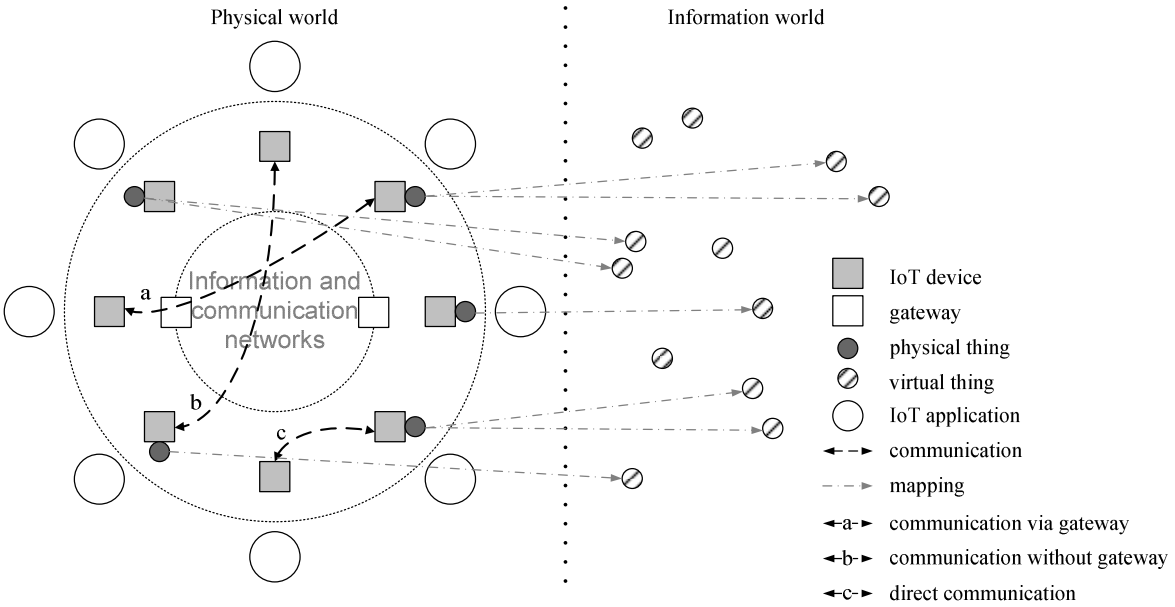

Figure 11 – Technical overview of IoT **Fehler! Verweisquelle konnte nicht gefunden werden.**

Physical things have association with virtual things (mapping), however virtual things can also exist without any associated physical things.

Devices communicate with other devices: they communicate through the network via gateway (case a), through the network without gateway (case b) or directly, that is without using the network (case c). Also, combinations of case a and c, case b and c are possible: for example, devices can communicate with other devices using direct communication in a ad-hoc sensor network (case c) and then communication through the network via ad-hoc sensor network gateway (case a).

The information and communication networks transfer data captured by devices to applications and other devices, as well as instructions from applications to devices. The information and communication networks provide capabilities for reliable and efficient transfer. The IoT network infrastructure may be realized via existing networks, such as conventional TCP/IP-based networks, and/or evolving networks, such as NGN.

ITU-T Y.2060 **Fehler! Verweisquelle konnte nicht gefunden werden.** summarized the fundamental characteristics of IoT as follows:

- Interconnectivity:
  In IoT, any thing will be inter-connected with the global information and communication infrastructure.

- Things-related services:
  The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their corresponding virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information and communication world will change.

- Heterogeneity:
  The devices in the IoT are heterogeneous as based on different hardware platforms and

networks. They can interact with other devices or service platforms through different networks.

- Dynamic changes:
  The state of devices change dynamically, e.g. sleeping and waking up, connected/disconnected etc. as well as the context of devices including location and speed, etc. Moreover, the number of devices can change dynamically.

- Enormous scale:
  The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

Figure 12 shows the IoT reference model. It is composed of four layers as well as management capabilities and security capabilities which are associated with the four layers.

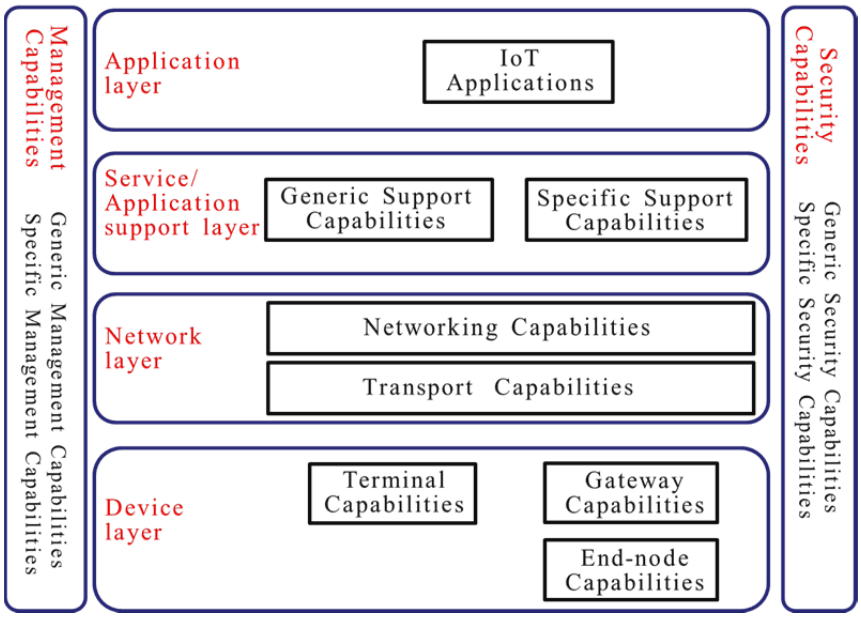

Figure 12 – IoT reference model **Fehler! Verweisquelle konnte nicht gefunden werden.**

- Application layer: it contains IoT applications.

- Service/Application support layer:
  - Generic IoT service/application support capabilities: The generic IoT service/application support capabilities are common capabilities which can be used by different IoT applications, such as data processing, data storage. These capabilities may be also invoked by specific IoT service/application support capabilities, e.g. to build other specific IoT service/application support capabilities.
  - Specific IoT service/application support capabilities: The specific IoT service/application support capabilities are particular capabilities to cater with requirements from diversified applications. In fact, they may consist of various detailed capability groupings, in order to provide different support functions to different IoT applications.

– Network layer:
  - Networking capabilities: They provide relevant control functions of network connectivity, such as access and transport resource control functions, mobility management, Authentication, Authorization and Accounting (AAA), etc.
  - Transport capabilities: They focus on providing connectivity for the transport of IoT service/application specific data information, as well as the transport of IoT-related control and management information.

– Device layer:
  Device layer capabilities can be logically categorized into three kinds of capabilities, i.e. terminal capabilities, end-node capabilities and gateway capabilities. Each device in the device layer needs to support at least one of the following capabilities:
  - Terminal capabilities include but are not limited to:
    - Direct communication with the network layer:
      With terminal capabilities, devices are able to gather and upload information directly (i.e. without using gateway capabilities) to the network layer and can directly receive information (e.g. commands) from the network layer.
  - Gateway capabilities include but are not limited to:
    - Multiple interfaces support:
      For the device layer, the gateway capabilities support devices with end-node capabilities to be connected with the network layer through kinds of wired or wireless technologies, such as Controller Area Network (CAN) bus, ZigBee, Bluetooth, Wi-Fi, etc. To the network layer, the gateway capabilities can communicate through various technologies, such as Public Switched Telephone Network (PSTN), Second Generation/Third Generation (2G/3G), Long Term Evolution (LTE), Ethernet, Digital Subscriber Line (DSL), etc.
    - Protocol conversion:
      There are two situations where IoT gateway capabilities are needed. One situation is when communications at the device layer use different device layer protocols, e.g., ZigBee technology protocols and Bluetooth technology protocols, the other one is when inter-layer communications use different protocols e.g., ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.
  - End node capabilities include but are not limited to:
    - Indirect communication with the network layer:
      End nodes are able to gather and upload information to the network layer indirectly, i.e. through gateway capabilities. On the other side, devices with end-node capability can receive information (e.g. commands) from the network layer.
    - Ad-hoc networking:
      Devices with end node capabilities are able to construct networks in an ad-hoc manner in some scenarios needing increased scalability and quick deployment.
    - Sleeping and waking-up:
      End node capabilities support sleeping and waking-up mechanisms to save energy.

– Management capabilities:
  As same as in traditional communication networks, IoT management capabilities cover the

traditional fault, configuration, accounting, performance, security (FCAPS) classes, i.e. fault management, configuration management, accounting management, performance management and security management.

- Security capabilities:
  - Generic security capabilities are independent of applications.
  - Specific security capabilities are closely coupled with application-specific requirements (e.g., mobile payment, security requirements).

Whether IoT is a concept, a technology or an infrastructure, it is inevitable that IoT encompasses many ICT like Ubiquitous Computing does and IoT is indispensable for supporting Ubiquitous Computing.

6.6. Web Services [8]

A key enabling technology to the use of M2M in the Internet of Things will be so called “Web Services”. The technology, however, has been used as the base for not only M2M applications and services but other ordinary applications and services.

W3C defines Web Services as follows:

- A web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Services Description Language (WSDL)). Other systems interact with the web service in a manner prescribed by its description using Simple Object Access Protocol (SOAP)-messages, typically conveyed using HyperText Transfer Protocol (HTTP) with an eXtensible Mark-up Language (XML) serialization in conjunction with other web-related standards.

Web Services require quite a lot of functionalities, and as a result architecture is indispensable. The web service standardization organizations construct standards by SOA. SOA is an evolutional form of distributed computing and object orientation.

By applying SOA-based standards to service provision, following effects are expected:

- From a business viewpoint:
  - Increased service value;
  - Internationalization; and
  - Expansion to the business automation
- From system development viewpoint:
  - Easy and quick development of service co-ordination and service area expansion;
  - Web Services enable system developers to focus on not "HOW" but "WHAT". "HOW" is covered by standard base tools. This enables quick and easy system software development;
  - Web Services standards have a composable structure, and so promote reusability of software; and
  - Easy connection to a legacy system.

Message standardization is intended to improve system coordination, interoperability and re-use, and so the conditions for Web Services are considered already mature today. In addition, the use of

Web Services will increase the flexibility of services to interoperate and communicate beyond their original sector in areas where the delineation between services and general commercial services converge.

Service collaboration with other sectors is expected to increase mutual effectiveness. Globalization of economy also requires communication across the country, sometimes across the world. All of these collaborations rely on interoperability of services. Interoperability across many sectors can only be achieved based on open international standards.

6.7. Service Oriented Architecture [8]

Applications and services of Ubiquitous Computing and/or ubiquitous sensor networks (USN) will be based on the Service Oriented Architecture for Web Services-based service provisioning. The SOA provides methods for systems development and integration where systems package functionality as interoperable services. A SOA infrastructure allows different applications to exchange data with one another. Service-orientation aims at a loose coupling of services with operating systems, programming languages and other technologies that underlie applications. SOA separates functions into distinct units, or services, which developers make accessible over a network in order that users can combine and reuse them in the production of applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services.[18]

SOAs build applications out of software services. Services comprise intrinsically unassociated, loosely coupled units of functionality that have no calls to each other embedded in them. Each service implements one action, such as filling out an online application for an account, viewing an online bank-statement, or placing an online booking or airline ticket order. Instead of services embedding calls to each other in their source code, they use defined protocols that describe how one or more services can “talk” to each other. [18]

A software developer, software engineer, or business process expert associates individual SOA objects by using orchestration. In the process of orchestration, a software engineer or process engineer associates relatively large chunks of software functionality (services) in a non-hierarchical arrangement (in contrast to a class hierarchy) by using a special software tool that contains an exhaustive list of all of the services, their characteristics, and a means to record the designer's choices that the designer can manage and the software system can consume and use at run-time. [18]

7. Standardization activities

7.1. ISO/IEC JTC 1

NOTE – The following sub-clauses focus on the standardization activities of JTC 1/WG 7 and SC 31/WG 6. Please refer to ANNEX I for more information about other JTC 1/SCs.

7.1.1. WG 7 – Sensor Networks

In the area of generic solutions for sensor networks, JTC 1/WG 7undertakes standardization activities that support and apply to the technical work of all relevant JTC 1 entities and to other standards organizations. The work scope of JTC 1/WG 7 includes:

- Standardization of terminology.
- Development of a taxonomy.
- Standardization of reference architectures.

- Development of guidelines for interoperability.

In the area of application-oriented sensor networks, JTC 1/WG 7 identifies gaps and commonalities as they may impact standardization activities within the scope of JTC 1. JTC 1/WG 7 pursues the following standardization activities:

- Addressing the technology gaps within the scope of JTC 1 entities.
- Exploiting technology opportunities where it is desirable to provide common approaches to the use of sensor networks across application domains.

JTC 1/WG 7 has 9 on-going work items on sensor networks as follows:

- ISO/IEC DIS 29182 Part 1 – Sensor Network Reference Architecture: General overview and requirements
  - provides the general overview and describes the requirements identified for the reference architecture
- ISO/IEC DIS 29182 Part 2 – Sensor Network Reference Architecture: Vocabulary and terminology
  - provides the definitions of all the terminology and vocabulary used in the sensor network reference architecture
- ISO/IEC CD 29182 Part 3 – Sensor Network Reference Architecture: Reference architecture views
  - provides the reference architecture views, (e.g., business, operational, systems, technical) as well as different presentation of the architecture (e.g., functional, and logical)
- ISO/IEC CD 29182 Part 4 – Sensor Network Reference Architecture: Entity models
  - provides the description of entity models, (e.g., system, subsystem, component models) with their interfaces, functional descriptions, and how they are used in the reference architecture and for implementation
- ISO/IEC CD 29182 Part 5 – Sensor Network Reference Architecture: Interface definitions
  - provides detailed, supportive information on the interfaces among the entity models in the reference architecture
  - includes the data/information descriptions, system level specifications, and so on
- ISO/IEC WD 29182 Part 6 – Sensor Network Reference Architecture: Application profiles
  - provides the application profiles that are derived from studies of use cases, scenarios, etc., for sensor network based applications and services
- ISO/IEC CD 29182 Part 7 – Sensor Network Reference Architecture: Interoperability guidelines
  - provides the design principles for interoperability based on the reference architecture which is developed with interoperability requirements

- ISO/IEC DIS 20005, Services and Interfaces Supporting Collaborative Information Processing (CIP) in Intelligent Sensor Networks
  - specifies services and interfaces supporting collaborative information processing (CIP) in intelligent sensor networks including:
    - CIP functionalities and CIP functional model
    - Common services supporting CIP
    - Common service interfaces to CIP
- ISO/IEC WD 30101, Sensor Network and its Interface for Smart Grid System
  - specifies sensor networks in order to support Smart Grid technologies for power generation, distribution, networks, energy storage, load efficiency, control and communications and associated environmental challenges

7.1.2. SC 31/WG 6 – Mobile Item Identification and Management (MIIM)

NOTE – SC 31 pursues standardization activities on Automatic Identification and Data Capture (AIDC) Techniques such as linear barcodes, 2D codes and RFID. Linear barcodes, 2D codes and RFID are used to identify object, however this report summarizes standardization activities regarding only RFID, especially mobile RFID (named Mobile AIDC). See clause 6.3.

The work scope of JTC 1/SC 31/WG 6 covers the following:

- Standardization of automatic identification and data collection techniques that are anticipated to be connected to wired or wireless networks, including sensor specifications, combining RFID with mobile telephony, and combining optically readable media with mobile telephony

At a glance, the work scope of JTC 1/SC 31/WG 6 is closely related with the technology for supporting Ubiquitous Computing on the applications in the B2C domain including sensor technologies.

Most of WG 6 projects deals with “mobile RFID” and IEEE standards regarding sensor interfaces under PSDO (Partner Standards Developing Organization) as follows:

- ISO/IEC 29143 (2011) – Air interface specification for Mobile RFID interrogator
  - provides an air interface specification for mobile RFID interrogators being part of a passive backscatter system
- ISO/IEC TR 29172 (2011) – Mobile item identification and management – Reference architecture for Mobile AIDC services
  - describes a reference architecture for Mobile AIDC services
- ISO/IEC FDIS 29173 Part 1 – Mobile RFID interrogator device protocol for ISO/IEC 18000-6 Type B and Type C
  - defines an interface protocol between a device driver of a mobile AIDC application platform and a mobile RFID interrogator within a mobile AIDC terminal
- ISO/IEC DIS 29174 Part 1 – UII scheme and encoding format for Mobile AIDC services – Identifier scheme for multimedia information access triggered by tag-based identification

- defines the Identifier (ID) scheme for multimedia information access triggered by tag-based identification, which provides the users with an improved method to access to the multimedia content without typing its address on a keyboard or inputting the name of objects and/or places of relevant information

– ISO/IEC FDIS 29174 Part 2 – UII scheme and encoding format for Mobile AIDC services – Registration procedures
  - specify registration procedures of ID scheme, obligations and requirements of Registration Authority (RA) as managing the ID scheme defined by ISO/IEC 29174-1

– ISO/IEC 29175 (2012) – Application data structure and encoding format for Mobile AIDC services
  - provides identification of user data for the purpose of encoding and identifying user data in Mobile AIDC services using:
    - ISO/IEC 29143 radio frequency (RF) tags,
    - ISO/IEC 18000-63 RF tags, and
    - ISO/IEC 15434-applied optically readable media such as linear bar codes and two-dimensional symbols.

– ISO/IEC 29176 (2011) – Consumer privacy-protection protocol for Mobile RFID services
  - specifies a consumer privacy-protection protocol for mobile RFID services

– ISO/IEC FDIS 29177 – Object Directory Service for Mobile AIDC services
  - specifies the identifier (ID) resolution protocol for multimedia information access triggered by tag-based identification, and
  - is used to retrieve the location and access method of the multimedia information associated with an ID

– ISO/IEC 29178 – Service broker for Mobile AIDC services
  - defines the functions of a service broker supporting service control, MII recognition and MII resolution related functions in Mobile AIDC service architecture that uses MII (ISO/IEC 29174) as an identifier

– ISO/IEC 29179 (2012) – Mobile AIDC application programming interface
  - provides a description of mobile AIDC applications and specifies the functional requirements of mobile AIDC application interfaces, and
  - defines abstract mobile AIDC application interfaces to provide a standardized functional view over various mobile AIDC application platforms

The following standards are IEEE Standards to SC 31/WG 6 under PSDO regarding sensor and sensor network technologies.

– ISO/IEC/IEEE 21450 [IEEE 1451.0] – Smart Transducer Interface for Sensors and Actuators – Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats

– ISO/IEC/IEEE 21451 Part 1 [IEEE 1451.1] – Smart Transducer Interface for Sensors and Actuators – Network Capable Application Processor (NCAP) Information Model

- ISO/IEC/IEEE 21451 Part 2 [IEEE 1451.2] – Smart Transducer Interface for Sensors and Actuators – Transducer to Microprocessor Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats
- ISO/IEC/IEEE 21451 Part 4 [IEEE 1451.4] – Smart Transducer Interface for Sensors and Actuators – Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats
- ISO/IEC/IEEE 802 Part 15.4 [IEEE 802.15.4-2006] – Local and metropolitan area networks – Specific requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless, Personal Area Networks (WPANs)

The standard below is IEEE standard to SC 31/WG 6 under PSDO Joint Development.

- ISO/IEC/IEEE 21451 Part 7 – Standard for a Smart Transducer Interface for Sensors and Actuators – Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats

7.2. ITU-T SGs

7.2.1. SG 13

ITU-T Study Group 13 leads ITU's work on standards for next generation networks (NGN) and future networks. NGN will provide capabilities to support convergence between ICT and other industries such as the vehicle manufacturing industry in support of the networked vehicle.

The standardization activity of SG 13 regarding Ubiquitous Computing may be concentrated on tag-based applications and services, USN, MOC (Machine Oriented Communications), ubiquitous networking and the Internet of Things. Recently, SG 13 started to develop standards for the Internet of Things.

The Recommendations published or under development by SG 13 are as follows:

- ITU-T Y.2213 (2008) NGN service requirements and capabilities for network aspects of applications and services using tag-based identification
  - describes high-level service requirements and NGN capability requirements needed to support applications and services using tag-based identification
- ITU-T Y.2016 (2009) Functional requirements and architecture of the NGN for applications and services using tag-based identification
  - includes functional requirements and architecture of the NGN for the support of applications and services using tag-based identification based on ITU-T Y.2213
- ITU-T Y.2002 (2009) – Overview of ubiquitous networking and of its support in NGN
  - provides an overview of ubiquitous networking and of its support in NGN, and
  - describes objectives and fundamental characteristics of ubiquitous networking and identifies capabilities required for the support of ubiquitous networking in NGN
- ITU-T Y.2060 (2012) – Overview of Internet of Things
  - provides an overview of the Internet of Things, and

  - clarifies concept and scope of IoT, identifies the fundamental characteristics and high level requirements of IoT, and describes the IoT reference model
  - the ecosystem and business models are also provided

- ITU-T Y.2061 (2012) – Requirements for support of machine oriented communication applications in the NGN environment
  - provides an overview of machine oriented communication (MOC) applications, including a description of the MOC ecosystem, key supporting features and some relevant use cases, and
  - analyses service requirements of MOC applications, specifies extended or new NGN capability requirements and MOC device domain capability requirements based on the service requirements, and
  - provides a reference framework for MOC capabilities

- ITU-T Y.2062 (2012) – Framework of object-to-object communication for ubiquitous networking in NGN
  - describes the concept and high-level architectural model of object-to-object communication for ubiquitous networking in NGN and present requirements and mechanism for identification of all objects and providing connectivity to them

- ITU-T Y.2221 (2010) – Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment
  - provides a description and general characteristics of ubiquitous sensor network (USN) and USN applications and services, and
  - analyses the service requirements of USN applications and services, and specifies the extended or new NGN capability requirements based on the service requirements

- ITU-T Y.2026 (2012) – Functional requirements and architecture of the NGN for support of ubiquitous sensor network (USN) applications and services
  - covers extended features of the NGN for support of USN applications and services, and
  - describes functional requirements, a functional architecture and functional entities in order to support the NGN service requirements and capabilities defined in ITU-T Y.2221

7.2.2. SG 16

ITU-T SG 16 is responsible for studies relating to ubiquitous applications ("e-everything", such as e-health and e-business), multimedia capabilities for services and applications for existing and future networks, including NGN and beyond.

The followings are standards developed by ITU-T SG 16, which may be related with Ubiquitous Computing.

- ITU-T F.744 (2009) – Service description and requirements for ubiquitous sensor network middleware
  - covers USN service description, USN middleware description, use cases of USN services using USN middleware, the functional model for USN middleware and requirements for USN middleware

- ITU-T H.621 (2008) – Architecture of a system for multimedia information access triggered by tag-based identification
  - defines the system architecture for the multimedia information access triggered by tag-based identification on the basis of Recommendation ITU-T F.771, and serves as a technical introduction to subsequent definition of detailed system components and protocols
- ITU-T F.771 (2008) – Service description and requirements for multimedia information access triggered by tag-based identification
  - specifies a high-level functional model, a service description and requirements for multimedia information access triggered by tag-based identification
- ITU-T H.641 (2012) – SNMP-based sensor network management framework
  - describes a sensor network management framework intended to provide integrated management functionalities for heterogeneous sensor networks using the Simple Network Management Protocol (SNMP)
- ITU-T F.OpenUSN (Draft) – Requirements and reference architecture for open USN service framework
  - defines an open USN service framework, and provide requirements, and reference architecture of open USN service framework
  - use of standard interfaces of open USN service framework will ensure USN service reusability, portability across several USN services, as well as accessibility and interoperability by USN application providers and/or developers
- ITU-T F.USN-ALI (Draft) – Requirements and reference structure of automatic location identification capability for USN applications and services
  - enables a device to discover its own location
  - used in various networks such as hybrid mobile networks, internet, low power wireless network (smart gird), and other USN communication systems
- ITU-T H.642.1 (for consent) – Multimedia information access triggered by tag-based identification: Identification scheme
  - defines an identification scheme for multimedia information access triggered by tag-based identification
  - used in the multimedia information system architecture defined in ITU-T H.621, and
  - satisfies the requirements defined in ITU-T F.771
- ITU-T H.642.2 (for consent) – Multimedia information access triggered by tag-based identification: Registration procedures for identifier
  - defines registration procedures of identification scheme defined by ITU-T H.642.1
- ITU-T H.642.3 (for consent) – Identifier resolution protocol for multimedia information access triggered by tag-based identification
  - See ISO/IEC 29177. This is common text with ISO/IEC 29177.

- ITU-T H.IoT-ID (Draft) – Requirements and Common Characteristics of IoT Identifier for IoT Service
  - analyses identifiers in existing technologies and networks for IoT service, and describe the requirements of identifier as IoT identifiers, common characteristics of IoT identifiers, and the general architecture of IoT identifiers
  - describes the requirements and common characteristics of IoT identifier for IoT services
- ITU-T H.IoT-reqs (Draft) – Common service requirements for Internet of Things (IoT) applications and services
  - general overview of Internet of Things applications and services, and;
  - characteristics of Internet of Things applications and services, and;
  - common services requirements for Internet of Things applications and services

7.3. ETSI TC M2M

ETSI TC M2M have responsibility to collect and specify M2M requirements; to develop and maintain an end-to-end overall high level architecture; to identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps; to provide the ETSI main centre of expertise in the area of M2M and to co-ordinate ETSI's M2M activity with that of other standardization groups and fora.

The followings are standards under development by TC M2M.

- TS 102 689 M2M Service Requirements
  - specifies the M2M service requirements aiming at an efficient end-to-end delivery of M2M services including general requirements, management, functional requirements, security, naming, numbering and addressing
- TS 102 690 Functional architecture
  - contains the overall end to end M2M functional architecture, including the identification of the functional entities and the related reference points
- TS 102.921 mIa, dIa and mId interfaces
  - mIa, dIa and mId key reference points of the M2M architecture as identified in TS 102 690
  - protocol/API definition for the Service Capabilities to Service Capabilities communication
  - information model of the protocol/API
  - interaction with/reuse of existing protocols, including the identification of key underlying protocols
- M2M Use cases
  - TR 102 691 Smart Metering
  - TR 102 732 eHealth
  - TR 102 857 Connected consumer

- TR 102 898 Automotive
- TR 102 897 City automation

7.4. 3GPP

3GPP has general objectives on MTC to provide network operators with lower operational costs when offering MTC services; to reduce the impact and efforts handling large MTC groups; to optimize network operations to minimize impact on device battery power usage; and to stimulate new MTC applications by enabling operator to offer services tailored to MTC requirements.

Some standards developed or being developed by 3GPP are shown as follows:

- TR 22.868 Study on Facilitating Machine to Machine Communication in GSM and UMTS
  - specifies charging mechanisms, addressing, types of communication, enhancement for the identified communication model, handling a large number of subscriptions and subscriber data within the network, handling issues of large number of M2M subscriptions for the user of M2M services, and the impact of optimizations for security
- TS 22.368 Service requirements for Machine-Type Communications
  - identify and specify general requirements for machine type communications
  - identify service aspects where network improvements (compared to the current human-to-human oriented services) are needed to cater for the specific nature of machine-type communications
  - specify machine type communication requirements for these service aspects where network improvements are needed for machine type communication
- TR 23.888 System Improvements for Machine-Type Communications
  - architectural enhancements to support a large number of Machine-Type Communication devices in the network;
  - architectural enhancements to fulfil MTC service requirements;
  - support combinations of architectural enhancements for MTC, though not all combinations may by possible
- TR 22.888 Study on Enhancements for MTC
  - network improvements for MTC Device to MTC Device communications via one or more PLMNs
  - possible improvements for MTC Devices that act as a gateway for 'capillary networks' of other devices.
  - network improvements for groups of MTC Devices that are co-located with other MTC Devices
  - improvements on network selection mechanisms and steering of roaming for MTC devices
  - possible enhancements to IMS to support MTC
  - possible improvements for location tracking of MTC Devices
  - service requirements on communications between PLMN and the MTC User/MTC Server (e.g. how the MTC User can set event to be monitored with MTC Monitoring);

- possible service requirements to optimize MTC Devices
- possible New MTC Features to further improve the network for MTC

– TR 22.803 Feasibility Study for Proximity Services (ProSe)
  - use cases and identify potential requirements for an operator network controlled discovery and communications between devices that are in proximity, under continuous network control, and are under a 3GPP network coverage, for:
    - commercial/social use
    - network offloading
    - public Safety
    - integration of current infrastructure services, to assure the consistency of the user experience including reachability and mobility aspects
    - Public Safety, in case of absence of EUTRAN coverage (subject to regional regulation and operator policy, and limited to specific public-safety designated frequency bands and terminals)

7.5. IEEE

IEEE 802.16 (Working Group on Broadband Wireless Access Standards) initiated Machine-to-Machine (M2M) Task Group November 2010. Under M2M Task Group, there are two ongoing projects:

– IEEE 802.16p – IEEE Standard for Air Interface for Broadband Wireless Access Systems Amendment: Enhancements to Support Machine-to-Machine Applications
  - describes enhancements to enable a range of Machine-to-Machine applications in which the device communications require wide area wireless coverage in licensed bands, and are automated rather than human-initiated or human-controlled for purposes such as observation and control
  - specifies IEEE Std 802.16 medium access control (MAC) enhancements and minimal orthogonal frequency division multiple access (OFDMA) physical layer (PHY) modifications in licensed bands to support lower power consumption at the device, support by the base station of significantly larger numbers of devices, efficient support for small burst transmissions, and improved device authentication

– IEEE 802.16b – IEEE Standard for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems - Amendment: Enhancements to Support Machine-to-Machine Applications
  - describes enhancements to enable a range of Machine-to-Machine applications in which the device communications require wide area wireless coverage in licensed bands, and are automated rather than human-initiated or human-controlled for purposes such as observation and control
  - specifies medium access control (MAC) enhancements and minimal WirelessMAN-Advanced physical layer (PHY) modifications in licensed bands to support lower power consumption at the device, support by the base station of significantly larger numbers of devices, efficient support for small burst transmissions, and improved device authentication.

8. Standardization areas and topics

NOTE – This clause suggests standardization areas and topics in Ubiquitous Computing coming from [12] selectively, because of the similarity with Internet of Things. However, it is believed that more feasible standardization areas and topics should be exploited beyond these suggestions.

- Identification
  - identification and authentication that can operate at a global scale
  - includes the management of unique identities for physical objects and devices, and handling of multiple identifiers for people and locations and possible cross-referencing among different identifiers for the same entity and with associated authentication credentials
- Architecture for Ubiquitous Computing
  - open architecture to maximise interoperability among heterogeneous systems and distributed resources including providers and consumers of information and services, whether they be human beings, software, smart objects or devices
  - decentralized autonomic architectures based on peering of nodes
  - architectures moving intelligence at the very edge of the networks, up to users' terminals and things
  - cloud computing technology, event-driven architectures, disconnected operations and synchronization
- Communication
  - billions of connected devices are pushing current communication technologies, networks and services approaches to their limits and require new technological investigations
  - communication to enable information exchange between "things" and between "things" and Internet
  - communication for interaction with humans in the physical world
  - communication and processing to provide data mining and services
  - energy efficient communication with multi frequency protocols, communication spectrum and frequency allocation
  - software defined radios (SDR) to remove need for hardware upgrades when new protocols emerge
- Network
  - architecture needs to be built on top of a network structure that integrates wired and wireless technologies in a transparent and seamless way
  - networks on chip technology considering on chip communication architectures for dynamic configurations design time parameterized architecture with a dynamic routing scheme and a variable number of allowed virtual connections
  - networking technologies (fixed, wireless, mobile etc.)
  - autonomic computing and networking
  - anonymous networking

- IP and post IP technologies

– Data and Signal Processing
  - As an enabler of Ubiquitous Computing, Internet of Things' devices that are operating at the edge are evolving from embedded systems to cyber physical and web enabled "things" that are integrating computation, physical and cognitive processes
  - convergence of physical computing and cognitive devices (wireless sensor networks, mobile phones, embedded systems, embedded computers, micro robots etc.) and the Internet will provide new design opportunities and challenges and requires new research that addresses the data and signal processing technology
  - semantic interoperability, semantic sensor web, data sharing, propagation and collaboration

– Discovery and Search Engine
  - Ubiquitous Computing needs many distributed resources (e.g., sensors and actuators), as well as information sources and repositories
  - necessary to develop technologies for searching and discovering such resources according to their capabilities (e.g., type of sensor / actuator / services offered), their location and/or the information they can provide (e.g., indexed by the unique IDs of objects, transactions etc.)
  - device discovery, distributed repositories

– Security and Privacy
  - During use of Ubiquitous Computing, users need confidence that there is no risk to their security and privacy

– Power and energy efficiency
  - Ubiquitous Computing device may have constrained-power such as battery, therefore energy efficiency has to be achieved. In some cases, energy harvesting/scavenging mechanisms are necessary for Ubiquitous Computing devices
  - electrostatic, piezoelectric and electromagnetic energy conversion schemes

– Software, services and algorithms
  - service discovery and composition
  - data sharing, propagation and collaboration
  - autonomous agent, self-management techniques to overcome increasing complexities and save energy
  - distributed self-adaptive software for self-optimization, self-configuration, self-healing
  - light-weight and open middleware based on interacting components/module abstracting resource and network functions
  - energy efficient micro operating systems
  - software for virtualization
  - algorithms for optimal assignment of resources in pervasive and dynamic environments

– Hardware
  - Nanotechnologies- miniaturization
  - sensor technologies – embedded sensors, actuators
  - solutions bridging nano and micro systems
  - communication – antennas, energy efficient RF front ends
  - Nanoelectronics – Nanoelectronics devices and technologies, self-configuration, self-optimization, self-healing circuit architectures
  - embedded systems - micro energy microprocessors/microcontrollers, hardware acceleration
  - low cost, high performance secure identification/authentication devices
  - low cost manufacturing techniques
  - tamper-resistant technology, side-channel aware designs

9. Clarification of Ubiquitous Computing and Internet of Things

As stated before, the notions of Ubiquitous Computing and Internet of Things are analogical.

Nevertheless, if we approach Ubiquitous Computing and Internet of Things in terms of technology, we are able to be conscious that Ubiquitous Computing is likely to be one of technologies enabling Internet of Things.

Figure 13 depicts how data is transformed into information, knowledge and wisdom in Internet of Things. In this diagram, Ubiquitous Computing provides the capability of gaining and/or transmitting data from the physical world; producing information; exploiting knowledge; and provisioning wisdom to end-users. The more degree of intelligence of things is high, the more diversity of computing by intelligence of things is increasing. That may be how we conceive Ubiquitous Computing enabling Internet of Things.

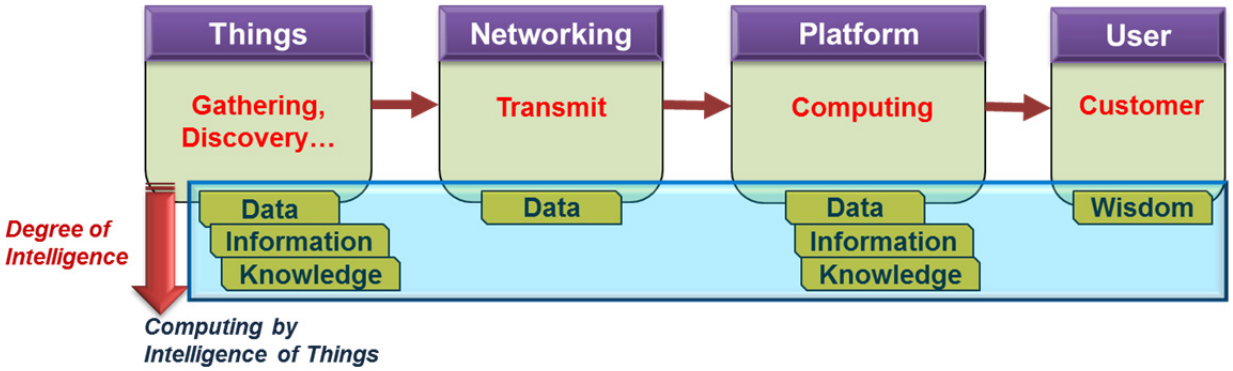

Figure 13 – Ubiquitous Computing enabling Internet of Things

10. Recommendation to JTC 1

This work recommends to JTC 1 to establish pertinent relationships with relevant SDOs and consortia to investigate the status of the work continuously on Ubiquitous Computing/Internet of Things.

In conclusion, SWG on Planning:

- **notes** that at least one WG and many SCs in JTC 1 are related with Ubiquitous Computing/Internet of Things, and;
- **recommends** the acceptance of the following Draft Resolution to JTC 1:

  JTC 1 recognizes the importance of Ubiquitous Computing/Internet of Things (UC/IoT) as a trend that will shape the definition of many standards in the ICT sector, and notes a growing interest in this area among a number of standards setting organizations. The vision for Ubiquitous Computing/Internet of Things (UC/IoT) is relevant to the mission of JTC 1 and intersects with the scope of a number of JTC 1/SCs, WGs and SWGs. Therefore, JTC 1 establishes a Special Working Group on Ubiquitous Computing/Internet of Things (UC/IoT).

  The SWG will have the following Terms of Reference:

  1. Identify market requirements and standardization gaps for UC/IoT;
  2. Encourage JTC 1 SCs and WGs to address the need for ISO/IEC standards for UC/IoT and facilitate cooperation across JTC 1 entities;
  3. Promote JTC 1 developed standards for UC/IoT and encourage them to be recognized and utilized by industry and other standards setting organizations;
  4. Facilitate the coordination of JTC 1 UC/IoT activities with IEC, ISO, ITU and other organizations that are developing standards for UC/IoT;
  5. Periodically report results and recommendations to JTC 1 SWG Planning; and
  6. Provide a written report of activities and recommendations to JTC 1 in advance of the 2013 JTC 1 Plenary meeting.

  Membership in the SWG UC/IoT is open to:

  1. JTC 1 National Bodies, JTC 1 Liaisons and approved JTC 1 PAS Submitters;
  2. JTC 1 SCs, JTC 1 WGs, relevant ISO and IEC TCs;
  3. Members of ISO and IEC central offices; and
  4. Invited standards setting organizations that are engaged in UC/IoT standardization as approved by SWG UC/IoT.

Appendix I

The mapping table between WGs, SCs and issues of Ubiquitous Computing/Internet of Things

NOTE – This section is initially produced based on subcommittees/working groups information from JTC 1 web pages. It is recommended that each WG and SC should fill out their technical relationships with Ubiquitous Computing/Internet of Things.

I.1 JTC 1/WG 7 (Sensor networks)

JTC 1 N 10770 reads for its business plan,

- *"In the area of generic solutions for sensor networks, undertake standardization activities that support and can be applied to the technical work of all relevant JTC 1 entities and to other standards organizations. This includes activities in sensor networks such as the following:*
  - *Standardization of terminology*
  - *Development of a taxonomy*
  - *Standardization of reference architectures*
  - *Development of guidelines for interoperability*
- *In the area of application - oriented sensor networks, identify gaps and commonalities that may impact standardization activities within the scope of JTC 1. Further, share this information with relevant entities within and outside of JTC 1. Unless better pursued within another JTC 1 entity, the following standardization activities may be pursued as projects by this Working Group:*
  - *Addressing the technology gaps within the scope of JTC 1 entities*
  - *Exploiting technology opportunities where it is desirable to provide common approaches to the use of sensor networks across application domains*
- *In order to foster communication and sharing of information between groups working in the field of sensor networks:*
  - *Seek liaison relationships with all relevant JTC 1 SCs/WGs*
  - *Seek liaison relationships with other organizations outside JTC 1 including but not limited to: relevant ISO TCs, IEC TCs and ITU-T SGs, IEEE 1451, IEEE 1588, IEEE P2030, IEEE 802.15,Open Geospatial Consortium, ZigBee Alliance, IETF 6LoWPAN, IETF ROLL WG, ETSI, IPSO Alliance, EPCglobal, ISA 100, LONMARK, KNX Association, Zwave Alliance*
  - *Consider the possibility of conducting joint projects with relevant ITU-T SG*
  - *Seek input from relevant research projects and consortia"*

Along with the work scope of JTC 1/WG 7, it has covered the following work topics which are shown to help understand how the work scope may be interpreted in terms of work items:

- Sensor Network Reference Architecture (SNRA) – Part 1: General overview and requirements

- Sensor Network Reference Architecture (SNRA) – Part 2: Vocabulary/Terminology
- Sensor Network Reference Architecture (SNRA) – Part 3: Reference architecture views
- Sensor Network Reference Architecture (SNRA) – Part 4: Entity models
- Sensor Network Reference Architecture (SNRA) – Part 5: Interface definitions
- Sensor Network Reference Architecture (SNRA) – Part 6: Application profiles
- Sensor Network Reference Architecture (SNRA) – Part 7: Interoperability guidelines
- Services and Interfaces Supporting Collaborative Information Processing in Intelligent Sensor Networks
- Sensor Network and its Interface for Smart Grid System
- Generic Sensor Network Application Interface

I.2 JTC 1/SC 6 (Telecommunications and Information Exchange Between Systems)

JTC 1 N 10858 reads for its business plan, *"Standardization in the field of telecommunications dealing with the exchange of information between open systems including system functions, procedures, parameters, and equipment, as well as the conditions for their use. This standardization includes both the lower layers that support the physical, data link, network, and transport protocols and services as well as the upper layers that support the application protocols and services including but not limited to Directory and ASN.1. A vital aspect of this work is done in effective cooperation with ITU-T and other worldwide and regional standardization bodies including IEEE, IETF, and Ecma International."*

Along with the work scope of JTC 1/SC 6, it has covered the following work topics which are shown to help understand how the work scope may be interpreted in terms of work items:

- Near Field Communication (NFC)
- Magnetic Field Area Network (MFAN)
- CSMA/CD MAC and PHY
- Wireless MAC control
- PHY/MAC specifications for short-range wireless low-rate applications in ISM band
- Multicast Session Management Protocol
- High Rate Ultra Wideband for Multimedia Services within 10 m range
- IS-IS routing protocols
- Connection-mode Transport Protocol
- Quality of Service (QoS)
- Enhanced communications transport service and protocol
- Group management protocol

- Relayed Multicast Protocol
- X.400 messaging
- X.500 directory services
- ASN.1

I.3 JTC 1/SC 17 (Cards and Personal Identification)

JTC 1 N 10854 reads for its business plan, *"Standardization in the area of: a) identification and related documents, b) cards, and c) devices associated with their use in inter-industry applications and international interchange."*
Along with the work scope of JTC 1/SC 6, it has covered the following work topics which are shown to help understand how the work scope may be interpreted in terms of work items:

- Physical characteristics and test methods for ID cards
- Integrated circuit cards with contacts
- Contactless integrated circuit cards
- Machine readable travel documents such as visa and passport
- Issuer Identification Numbers (IINs)/Application Provider Identifiers (RIDs)
- Motor vehicle driver license and related documents
- Application of biometrics to cards and personal identification

I.4 JTC 1/SC 25 (Interconnection of IT equipment)

JTC 1 N 10865 reads for its business plan, *"Standardization of microprocessor systems; and of interfaces, protocols and associated interconnecting media for information technology equipment, generally for commercial and residential environments, for embedded and distributed computing environments, storage systems, and other input/output components.*

Development of standards for telecommunication networks and interfaces to telecommunication networks is excluded."

Along with the work scope of JTC 1/SC 25, it has covered the following work topics which are shown to help understand how the work scope may be interpreted in terms of work items:

- Fibre Distributed Data Interface (FDDI)
- Small Computer System Interface (SCSI)
- Fibre Channel
- Intelligent Peripheral Interface
- High Performance Parallel Interface (HIPPI)
- Home Electronic System Interfaces
- Home network security

- WiBEEM wireless communications for home networks
- Microprocessor systems
- Storage management
- Customer premises cabling

I.5 JTC 1/SC 28 (Office equipment)

JTC 1 N 10812 reads for its business plan, *"Standardization of basic characteristics, test methods and other related items, excluding such interfaces as user system interfaces, communication interfaces and protocols, of office equipment and products such as Printers, Copying Equipment, Digital scanners, Facsimile equipment and systems composed of combinations of office equipment."*

Along with the work scope of JTC 1/SC 28, it is developing the following work topics which are shown to help understand how the work scope may be interpreted in terms of work items:

- Measurement of Image quality attributes for hardcopy output
- Test chart and method for measuring printer resolutions
- Cartridge Characterization
- Method for measuring digital copying Productivity
- Copying machines and Multi-function devices
- Determination of chemical emission rates from electronic equipment

I.6 JTC 1/SC 31 (Automatic Identification and Data Capture Techniques)

JTC 1 N 10845 reads for its business plan, *"Standardization of data formats, data syntax, data structures, data encoding, and technologies for the process of automatic identification and data capture (AIDC) and of associated devices utilized in inter-industry applications and international business interchanges. AIDC serves many different applications (e.g., product/item identification, point-of-purchase/use, track and trace, product distribution) in such market sectors as retail sales, health care, supply chain, transportation, and many areas of the manufacturing and service industries, where reliable, fast and automated data input with reduced errors improves operational efficiency with a positive impact on financial returns."*

SC 31 has handled linear bar codes, two-dimensional symbologies, Radio Frequency Identification (RFID), RTLS (Real Time Locating Systems) and unique identifiers. Along with the work scope of JTC 1/SC 31, more specifically, it has covered the following work topics which are shown to help understand how the work scope may be interpreted in terms of work items:

- Linear bar code print quality
- Data Matrix and QR Code 2005
- EAN/UPC
- GS1 Application Identifiers and ASC MH10 Data Identifiers

- Unique identifiers for transport units, individual items, returnable transport items, product groupings, and grouping of transport units
- RFID Application Interface Protocols
- RFID Air Interface
- Real Time Locating Systems
- Mobile item identification and management
- Smart Transducer Interface for Sensors and Actuators

Table 1 – WGs/SCs' relation with UC/IoT

(This table does not show the complete relation of WGs/SCs with UC/IoT)

WG/SC No	The title of WGs/SCs	Relation to Ubiquitous Computing/Internet of Things
WG 6	Corporate Governance of IT	N/A
WG 7	Sensor networks	Sensor networks/M2M
SC 2	Coded character sets	N/A
SC 6	Telecommunications and information exchange between systems	Network/Transport
SC 7	Software and systems engineering	N/A
SC 17	Cards and personal identification	Personal identification
SC 22	Programming languages, their environments and system software interfaces	N/A
SC 23	Digitally Recorded Media for Information Interchange and Storage	N/A
SC 24	Computer graphics, image processing and environmental data representation	N/A
SC 25	Interconnection of information technology equipment	Hardware (User device)
SC 27	IT Security techniques	Security/Privacy
SC 28	Office equipment	Computing by office device
SC 29	Coding of audio, picture, multimedia and hypermedia information	N/A
SC 31	Automatic identification and data capture techniques	RFID/Identification of Things
SC 32	Data management and interchange	N/A
SC 34	Document description and processing languages	N/A
SC 35	User interfaces	User interfaces to mobile device

SC 36	Information technology for learning, education and training	N/A
SC 37	Biometrics	Identification by biometrics
SC 38	Distributed application platforms and services (DAPS)	Cloud computing/SOA
SC 39	Sustainability for and by Information Technology	Power and energy efficiency