Janne Poikolainen

INTERNET OF THINGS - EMERGENCE OF STANDARDS

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2012

ABSTRACT

Poikolainen, Janne

Internet of Things – Emergence of standards

Jyväskylä: University of Jyväskylä, 2012, 34 p.

Information System Science, Bachelor's Thesis

Supervisor: Mazhelis, Oleksiy

Internet of Things is a paradigm referring to the pervasive presence of networked things and objects that are able to interact and cooperate with each other. This paradigm also suggests that in the future these objects also produce large amounts of data to the internet and other network applications. Predictions say that the amount of data produced by things proceeds human produced data in the near future. These visions are grounded in the assumption that the advances in microelectronics, communications and information technology added with diminishing prices of these technologies will bring networking and cooperation capabilities to more and more every day things.

This thesis reviews what the Internet of Things means as a phenomenon, how standards form in this field and challenges for Internet of Things standardization. Since IoT is a global phenomenon standardization plays a key role in the development of IoT. For this reason this thesis focuses to the standardization activities and not only to introducing technologies associated with IoT. First two chapters deal with the phenomenon and technology. But chapters three and four focus on challenges on IoT standardization and some of the IoT standards that already exist.

Keywords: Internet of Things, IoT, RFID, Sensor network, Standards, Standardization issues.

TIIVISTELMÄ

Poikolainen, Janne

Internet of Things – Standardien synty

Jyväskylä: Jyväskylän yliopisto, 2012, 34 s.

Tietojärjestelmätiede, kandidaatintutkielma

Ohjaaja: Mazhelis, Oleksiy

Internet of Things on käsite joka viittaa verkottuvien, yhteistyökyjyjä omaavien tavaroiden ja muiden objektien laajaan läsnäoloon. Käsite ennustaa myös, että jopa aivan lähitulevaisuudessa yhä suurempi osa internettiin ja muihin verkkoihin tuotetusta tiedosta ei ole enää ihmisten tuottamaa. Nämä näkemykset pohjaavat jatkuvalle viestintä- ja kommunikaatioteknologian ja elektroniikan kehitykseen, joka myös laskee hintoja ja tuo verkko- ja yhteistyöominaisuuksia yhä useampiin joka päiväisiin esineisiin.

Tämä tutkielma tarkastelee Internet of Things käsitteen lisäksi alan standardien syntyä ja standardisoinnin haasteita. Koska käsite on maailmanlaajuinen, standardisointi on avain asemassa näiden teknologioiden yleistymisen saavuttamisessa. Tästä syystä tämä tutkielma keskittyy myös alan standardointi toimintaan, erilaisten teknologioiden esittelyn lisäksi. Tutkielman kaksi ensimmäistä kappaletta esittelee itse ilmiötä ja siihen liittyviä teknologioita. Kappale kolme keskittyy standardoinnin haasteisiin ja kappale neljä esittelee jo olemassa olevia standardeja.

Avainsanat: Internet of Things, IoT, RFID, Sensori verkot, Standardit, Standardointi kysymykset.

FIGURES

TABLES

TABLE OF CONTENTS

1 . Introduction

The Internet of Things (IoT) is a concept referring to the pervasive presence of things and objects around us, which are able to interact and cooperate with each other. (Atzori, Iera, & Morabito, 2010)

The IoT vision is grounded in the assumption that advances in microelectronics, communications and information technology remain steady in the foreseeable future. In recent years the integration of processors communication modules and other such components into everyday objects has increased, as a result of their diminishing size, falling price and decreasing energy consumption. (Mattern & Floerkemeier, 2010)

The growth of internet during last three decades from linking just thousand hosts to today's billions has been very fast. Lately, the mobile devices rather than computers are used for connecting to the Internet. The next logical step in this development is to evolve from interconnected computers towards a network of interconnected objects and thus create the Internet of Things. Objects can have their own addresses or be embedded in complex systems as sensors for obtaining environmental information. Sensor networks can record temperature, measure distances or sense presence of people. Data gathered via sensors can then be used to create applications to health care, traffic control, recyclability improvement, commerce, logistics or smart homes to create interactive environments. (Commission of the European Communities, 2009)

The things in IoT are different kinds of physical entities, that possess some characteristics that are of some importance to people. IoT functionalities include for example tracking of parts or packages, monitoring tasks in manufacturing or measurement of temperature in an engine. As a result of these different areas of deployment IoT consists of heterogeneous set of devices and communication strategies. Devices can be personal wearable wireless sensors or they can be integrated to our living environment. (Tarkoma & Katasonov, 2011)

EU – action plan for Europe states three points to highlighting the complex nature of IoT. First IoT should be seen as infrastructure consisting of inde-

pendent systems that is only partly based on existing Internet infrastructure. Second IoT will be implemented in symbiosis with new services. Third is the modes of communication: things-to-person and thing-to-thing. Especially thing-to-thing communication that includes Machine-to-Machine (M2M) communication is expected to grow substantially in the future as connected devices will multiply as much as 99%. (Commission of the European Communities, 2009)

Understanding the definition and basic ideas behind the concept of IoT and its social, economical and technical implications can be challenging. The reason for this fuzziness around the term is caused by the term "Internet of Things" it self. The term is syntactically composed of two terms that push forward differently oriented visions. The first gives a network oriented vision and the second focuses on common framework of generic "objects". The differences in the point of view can be substantial and the different perspectives depend on specific interests of stakeholders, business alliances, research and standardization bodies. Nevertheless when put together the two terms form a semantic meaning of a world-wide network of interconnected objects that are uniquely addressable and communicate using standard protocols. (Atzori et al., 2010)

In the very first "Things oriented" visions the things were very simple items with identifying capabilities. Today's IoT visions are much wider and they consist of much more than solely identification of objects. The capabilities in question include track-ability, sustainability, enhaceability as well as identifiability. The things are not only equipped with wireless communication, memory and elaboration capabilities, but are also capable of autonomous and pro active behavior, context awareness and collaborative communications just to name a few. (Atzori et al., 2010)

The "Internet oriented" vision is composed of the new dimensions being added to the information and communication technologies. The dimensions include communication between people and things and between things themselves. ITU states this new dimension: *"from anytime, anyplace connectivity for anyone, we will now have connectivity for anything"*. (International Telecommunications Union, 2005)

The third IoT vision orientation is the "Semantic oriented" vision. The idea of connectivity to anything rises a potential problems as the number of items in the future Internet is destined to become extremely high. Challenges arise on how to represent, store, interconnect, search and organize these large amounts of information generated by the IoT. One of the suggested solutions for solving the problem is the use of semantic technologies for thing description and reasoning over data. (Atzori et al., 2010)

Another more holistic approach for the phrase was originally adopted in the ITU 2005 report. It suggests that IoT would connect objects in a sensory and intelligent way. The ITU report defines three key functions IoT would combine as technology develops in these fields. These functions are: tagging things (item

identification), feeling things (sensors and wireless sensor networks) and shrinking things (nanotechnology). (Tarkoma et al., 2011)

In order to collect and process data from everyday objects and devices, the first required system is identification. Identification is needed to connect the objects to large databases and networks. The system of identification needs to be cost-effective and unobtrusive. The second, embedded intelligence can enhance the data collection capabilities and also the power of the network by moving part of the information processing to the edges of the network. Third miniaturization and nanotechnology give smaller and smaller things the ability to interact and connect. Eventually, even dust sized particles might be tagged and networked. As everyday objects will take on more smart characteristics they may also take on electronic identities that can be queried remotely, or they can be equipped with sensors to detect changes around them. (International Telecommunications Union, 2005)

In the internet of today nearly all information is originally created by humans, by typing text, taking digital pictures or in some other form of recording information. But in the visions of new era of ubiquity humans may become the minority as data generators and receivers as everyday objects start using networks. (Atzori et al., 2010)

There are many IoT technologies that exist today mentioned in the EU – Action plan for Europe: web-enabled mobile phones equipped with cameras or Near-Field Communication, unique serial numbers on pharmaceutical products, smart electrical monitoring systems and intelligent objects used in retail, manufacturing and logistics. (Commission of the European Communities, 2009) In Finland cellular-based energy metering has been widely used by utility companies for a decade. (Tarkoma et al., 2011) These applications use technologies like RFID, Near Field Communication (NFC), 2D barcodes, wireless sensors and actuators, Internet Protocol Version 6 (Ipv6) and ultra wide-band or 3/4G that are regarded as key technologies in future IoT deployments. (Commission of the European Communities, 2009)

Research questions of this thesis are:

- What is Internet of Things?
- How do IoT standards form?
- What are the challenges for IoT standardization?

A brief explanation for the first question is already given in this chapter and following chapters of this thesis are organized as follows. Second chapter "Enabling technologies" describes the technologies that from the IoT infrastructure, third chapter "Emergence of Standards" deals with the challenges in IoT standardization and fourth chapter introduces existing standardization.

2 . Enabling technologies

IoT relies on several enabling technologies that together create a bridge between virtual and physical world. These technologies include identification, sensing, embedded information processing, actuation, communication, addressability, localization and user interfaces. (Commission of the European Communities, 2009)

2.1 Identification

As mentioned in the previous chapter identification is the first functionality needed according to ITU vision of IoT. The existing technology that offers this functionality is the RFID. (International Telecommunications Union, 2005)

The abbreviation RFID stands for radio frequency identification and as the name suggests information is carried by radio waves. The technical procedure is drawn from radio and radar engineering. An RFID system is made up of two components: the transponder and reader. A reader contains a radio frequency module that acts as a transmitter and receiver, a control unit and a coupling element to the transponder. In addition reader usually has some form of interface to forward the received data. The transponder is the data-carrying device of an RFID system. It usually consists of a coupling element and a microchip. Tags are usually passive, i.e., they do not have an on board power supply. (Atzori et al., 2010) The transponder is active only when it is within the interrogation zone of a reader (Finkenzeller, 2003). This is because the power required to activate the transponder is supplied through the coupling unit. The energy is harvested from the query signal transmitted by the reader by electromagnetic induction. (Atzori, Iera, & Morabito, 2010)

Apart from passive RFID tags mentioned there are also tags with a internal power supplies. Internally powered tags are divided to two categories. The

semi passive tags where batteries power the microchip, but transmission is powered with harvested energy. In active tags battery powers the transmission as well. (Atzori, et al., 2010) In addition to different power supplies there are many more factors to differentiate RFID system variants. System features can be differentiated by operation type, amount of data, programmability, data carrier's operating principle, frequency range, data transfer type and response frequency. (Finkenzeller, 2003)

2.2 Sensing and embedded information processing

In co-operation with RFID systems sensor network use have been proposed in several application scenarios of IoT. Sensor networks can augment the awareness of an environment by tracking the status of things. (Atzori et al., 2010) Sensor networks can monitor numerous ambient conditions. Here are some examples: temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of objects, mechanical stress levels. (Estring, Govindan, Heidemann & Kumar 1999)

A sensor network is constructed of densely deployed sensor nodes that are located inside or very close of the measured phenomenon. The position of sensor nodes do not need to be predetermined, but they can be deployed randomly if such demands are dictated by application. These requirements also imply that sensor network protocols and algorithms must posses self-organizing capabilities. Sensor nodes are fitted with an on-board processor, so they are able to carry out simple computations locally. Due to this ability instead of sending raw data, the sensor nodes transmit only the required and partially processed data (Akyildiz, Su, Sankarasubramaniam & Cayirci, 2002) Nodes transmit their data to special nodes called sinks, that are responsible for the fusion of the sensor data. Data reporting is usually done to a small number of sinks, in most cases, only one. (Atzori et al., 2010)

Although the flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment characteristics of sensor networks create many possible application areas for remote sensing, there are equally many problems in several layers of the protocol stack. Such factors include fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. (Akyildiz et al., 2002)

Most current commercial wireless sensor networks (WSN) are based on the IEEE 802.15.4, witch defines a physical and MAC layers for low-power, low bit rate communications in wireless personal area network (WPAN). But since the standard does not include specifications for the higher layers of the protocol stack there are several issues that make seamless integration of sensor nodes to

the internet difficult. Scarcity of IP-addresses poses a problem, because sensor networks may consist of a very large number of nodes. In addition there are issues in energy saving functionalities and physical layer packet sizes. (Atzori et al., 2010)

RFID sensor networks consist of RFID-based sensors with some computing capabilities and RFID readers, which are the sinks that gather the data and also provide power for the network. RFID sensor network advantages compared to WSN systems include: small size, low cost and no lifetime limitations from battery duration. (Atzori et al., 2010)

2.3 Middleware

The middleware is a software layer between hardware and application levels (Bandyopadhyay, D. & Sen, 2011). There are several reasons middleware is required for IoT. First reason is defining and enforcing of common standards is difficult when devices and domain are so diverse as in the case of IoT. But in order to become reality IoT needs to join very heterogeneous components together. Middleware acts as a bond between these different technologies. Second requirement is a demand for abstraction layer for applications of diverse domains. To mitigate this problem middleware provides applications with application programming interfaces to the physical layer communications services. Middleware also hides unnecessary details and diversity of physical level technologies. (Bandyopadhyay, S. Sengupta, Maiti, & Dutta 2011)

These requirements create the need for various functional components that IoT-middleware must support. The components are: interoperation, context detection, device discovery and management, security and privacy and managing data volume. (Bandyopadhyay, S. et al., 2011)

Semantic interoperability is a term that describes communication between providers and requestors, despite the heterogeneous nature of their information structures. Lack of semantic interoperability is the cause of ineffective collaboration and integration. One model of achieving semantic interoperability between heterogeneous information systems is through comprehensive shared information models. Problem with this approach is the models rigidity, that can also be seen as inflexibility. The second way to achieve semantic interoperability is by providing appropriate semantic intermediators to translate the information format to each systems individual needs. (Bandyopadhyay, D. et al., 2011)

Architectures proposed for IoT often follow the service oriented architecture (SOA) approach. The use of SOA principles allows braking down complex systems into ecosystem of simple components. Another benefit from SOA approach is the possibility to software and hardware reuse, because SOA does not

impose a specific technology for service implementation. (Bandyopadhyay, D. et al., 2011)

Advantages of the SOA approach are recognized in many studies on middleware solutions for the IoT. But still a commonly accepted layered architecture for IoT does not exist. This imposes problems for proposed middleware solutions, as a common set of services and an environment for service composition is required for abstracting the device functionalities and communication capabilities. The need of a layered model lead to the definition of a middleware sketch that defines the functionalities addressed in past works dealing with IoT middleware issues. This sketch consists of five layers that are from top to bottom: applications, service composition, service management, object abstraction & objects. In addition the sketch deals with trust, privacy and security management that concerns all layers. (Atzori et al., 2010)

2.4 Communication

IoT applications form an extensive set of demands for communication technology. In other words they create a design space with many dimensions that need to be taken into consideration. These areas include deployment, mobility, cost heterogeneity communication modality, infrastructure, network topology, coverage, connectivity, network size, lifetime and other quality of service requirements. A design space this large complicates IoT application development in several ways. One suggested design to solve this problem is creating designs for minimum capabilities of things. However often a global minimum does not exist and this approach often restricts use of desired capabilities of the design space. These characteristics suggest that heterogeneous systems should be used instead of a single hardware and software platforms. (Sundmaeker, Guillemin, Friess, Woelfflé, 2010) Communication issues are discussed further in the following two chapters with examples of new communication standards currently in development.

3 . Emergence of Standards

In development of standards focuses on designs that should support a wide range of applications. Standards should also serve the requirements different application domains such as variety of industry sectors, society, environment and individual citizens. (Bandyopadhyay, D. et al., 2011) This chapter concentrates on how standards emerge in different areas of IoT and discusses about some fundamental issues of standardization.

3.1 Mandates for standardization

Machine-to-Machine (M2M) standardization efforts in Europe are conducted by The European Telecommunications Standards Institute (ETSI). ETSI has formed a M2M Technical Committee specially to conduct standardization activities relevant to M2M systems and sensor networks. The committee works on development and maintenance of an end-to-end architecture as well as, standardization efforts on sensor network integration, naming addressing, location, QoS, security, charging, management, application and hardware interfaces. (Bandyopadhyay, D. et al., 2011)

European commission has created a mandate to European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and ETSI for development of an open architecture for utility meters. The mandates general objective is to ensure interoperability and raise the customers awareness of actual consumption, in order to allow timely adaptation to their demands. The objective is achieved through ensuring European standards that will enable interoperability of utility meters and it will require interoperability enabling communication protocols to be included in the architecture. This is a major development in shaping the future European standards for smart metering and advanced metering infrastructures. (Daradkeh, Namiot & Sneps-Sneppe 2012)

old technology if standardization is delayed. But on the other hand many competing standards can paralyze markets as users will wait for a dominant technology to emerge. To avoid such a situation, co-ordination between standardizing bodies is necessary and various formal contracts about these matters do exist. (van Kranenburg et al., 2011)

Technical interoperability is another issue that benefits from early adoption of standards. Promotion of interoperability has been recognized as a important factor for the development of IoT (van Kranenburg et al. 2011) An European standards body, ETSI states several definitions that capture the meaning of the term interoperability in their white paper. They all deal with how systems can communicate, exchange data and use information. (van der Veer, 2008)

A contrary approach to early adoptation of standards is to let the community decide the mechanisms that work best, through trial and error. The view suggests that rigid standards development and regulation, does not give enough time for the dominant standard to emerge and artificial standards can be adopted prematurely. An example of this can be found from the history of the internet. ISO established an internet protocol called ISO-IP that was the officially recognized internet protocol. Contrary to ISO-IP TCIP originally developed for the Arpanet, emerged naturally as the dominant protocol for web interaction. ISO-IP standard is considered to have been adopted artificially early and it is incompatible with TCIP, so it only has marginal role today. (van Kranenburg et al. 2011)

3.3 Horizontal solutions

In the infrastructure point of view on IoT one of the biggest challenges relates to shared infrastructure. Different industries that utilize IoT applications, are called verticals. To reach high efficiency and feasibility of many business models, there is a demand in IoT architecture development for horizontal service components that are generic across these different vertical industries (Tarkoma et al., 2011).

A proposal for main application domains of IoT is stated in CERP-IoT cluster book and they are: industry, environment and society. Industry consists of manufacturing, logistics, banking etc. Environment comprises among others of agriculture, recycling and energy management. And finally society deals with governmental issues such as services, society structures and e-inclusion. While these applications domains have different goals their requirements are not significantly different. In reality IoT applications can be associated with sev-

eral rather than single application domain. (Tarkoma et al., 2011; Sundmaeker et al., 2010)

An example of the need for horizontal solutions is the emergence of a variety of communication solutions for specific application domains. This trend is believed to grow even stronger as power-efficient protocols for low-cost communication will enable rapid evolution to number of cost-effective connected devices. This possible development poses a risk that application developments provide limited interoperability. For this reason common standardization and understanding of the IoT domain is needed. Well established vertical solutions that co-exist in many fields such as manufacturing and logistics. But since these solutions are usually developed for highly specialized applications, they are not interoperable with other such solutions. Many technology and system providers also label their solutions as Internet-of-Things technologies, although the more appropriate term would be Intranet-of Things, since the solutions lack the scalability requirements of a future IoT, in both communication- and manageability of devices. (Walewski, 2011)

The Finnish strategic research agenda of IoT has two points of view on vertical applications. First is to analyze existing vertical applications to develop horizontal service enablement architecture and second to investigate potential novel applications enabled by this architecture. Research of the first point of view selects vertical application areas as use scenarios that are studied in detail to understand the commonalities of vertical applications and to identify possible horizontal components for IoT architecture. In the second point of view research focuses on new services and applications enabled by IoT, as these new services and applications will be supported by underlying horizontal components. (Tarkoma et al., 2011)

3.4 Constraints towards global standardization

In IoT standard design there are some special areas that need to be considered ensuring global interoperability. Some areas also have constraints concerning existing regulations. Example of such restriction is permitted frequency bands and power levels for radio frequency communications, that needs to be addressed for all devices that make use of radio spectrum. (Bandyopadhyay, D. et al., 2011)

Different bands of radio spectrum have been allocated for various purposes, such as broadcast communications, mobile telephony, citizen band radio, emergency services communications, wireless internet and short-range radio. Also the frequency band allocations are not identical between different regions of the world (Bandyopadhyay, D. et al., 2011). For example large portions of the

UHF spectrum has been auctioned to cellular phone service providers for high license fees. (Wu, Nystrom, Lin & Yu, 2006)

In the field of IoT, one of the technologies that suffers from complexity caused by different spectrum allocations around the world is RFID. RFID frequencies collide with telecommunications bandwidths in different continents, since North American, Asian and European band widths differ. In United States and Canada RFID systems could be allocated to UHF frequency band from 902 to 928MHz, but outside North America frequency bands around 915Mhz is almost exclusively used for wireless communications. In Europe ETSI has released a 2MHz UHF band for RFID use between 865.6 to 867.6 and Japan's 2Mhz allocation for RFID is between 953 to 954MHz. These differences in RFID bandwidths between different areas add substantial amount of complexity for RFID applications that are intended to have global functionality. For example supply chain management applications where tagged goods must travel across borders. Since conventional RFID tags respond only to a specific UHF frequency range and cannot be read in countries that have different frequency band allocations for RFID use. (Wu et al., 2006)

The next chapter introduces several standards from three different standardization bodies to demonstrate the nature of actual IoT standards.

4 . Existing standardization

There are several standardization bodies providing standardization to the field of IoT. In this chapter some examples of such standards are described. This is not in any means a complete list of IoT standards, but a set of some standards provided by some of the more influential standard providers: EPCglobal, ETSI and IETF.

4.1 EPCglobal Standards

EPCglobal is an activity conducted by GS1. GS1 is a non-for-profit standards organization focusing on standards and solutions that improve the efficiency and transparency of supply and demand chains. EPCglobal supports the global adoptation of Electronic Product Code (EPC) and related industry driven standards. To achieve this EPCglobal has created an Architecture Framework that is a collection of interrelated hardware, software and data standards. EPCglobal, its delegates and others also operate a shared network services called EPC Network Services to create all in service together with EPCglobal Standards (Traub et al. 2010).

In the EPCglobal Framework standards define norms for hardware, software and data interfaces. Some of these standards are developed by EPCglobal, but the framework also includes standards developed by other standardization bodies. The function of EPCglobal standards is to provide normative guidance for the behavior of interfaces between components. But innovation in the product implementation is free, as long as they implement EPCglobal interface standards correctly (Traub et al. 2010).

EPCglobal Network services can be considered as a special case of components that implement EPCglobal standards. These services provide services

to all End Users and they can be deployed by EPCglobal, EPCglobal delegated organizations or other third parties (Traub et al. 2010).

The EPCglobal framework activities can be divided into three parts (see Table 1) and while this division is not rigid it can be helpful for understanding of the scope and overall organization. The rest of this chapter describes areas and ratified standards.

TABLE 1 EPCglobal Architecture Framework components. (Traub et al. 2010)

Activity	Standard	Status
Object Exchange	UHF Class 0 Gen 1 Tag Air Interface	Not a EPCglobal standard
	UHF Class 1 Gen 1 Tag Air Interface	Not a EPCglobal standard
	HF Class 1 Gen 1 Tag Air Interface	Not a EPCglobal standard
	UHF Class 1 Gen 2 Tag Air Interface v1.1.0	Ratified
	UHF Class 1 Gen 2 Tag Air Interface v1.2.0	Ratified
	HF Class 1 Tag Air Interface	In Development
Infrastructure	EPC Tag Data Standard	Ratified
	Low Level Reader Protocol	Ratified
	Reader Management	Ratified
	Discovery, Configuration and Initialization (DCI) for Reader Operations	In Development
	Tag Data Translation	Ratified
	Application Level Events (ALE)	Ratified
	EPCIS Capture Interface	Ratified
Data Exchange	EPCIS Data Standard	Ratified
	Core Business Vocabulary	Ratified
	EPCIS Query Interface	Ratified
	ONS	Ratified
	Discovery Services	In Development

4.1.1 Physical Object Exchange

Physical Object Exchange activity provides means for identifying exchanged physical objects with Electronic Product Codes. These objects can be for example trade goods that are shipped and received, in which the receiver will be able to determine the EPCs of the objects and interpret them properly. Other uses can differ from this goods model, but still involve unique identification and tagging of objects (Traub et al. 2010).

Physical Object Exchange standardization actually consist only of UHF (Ultra High Frequency) and HF (High Frequency) Tag Air Interface standards. In this thesis the EPC Tag Data Standard is covered in the next part dealing with EPC Data Exchange activity since it can belong to either one of activities. The point of view in this matter depends on specific applications.

The Air Interface standards consist of four UHF standards in which the latest ratified version is UHF Class 1 Gen 2 Tag Air Interface v1.2.0 standard. In HF standards EPCglobal published an HF Class 1 Gen 1 Tag Air Interface. This is not an actual EPCglobal standard, but it will be superseded by a HF Class 1 Tag Air Interface which is currently in development (Traub et al. 2010).

The Air Interface standards defines the physical and logical requirements for a RFID system. These requirements include frequency ranges, system composition and protocols for communication. For example the first actual chapter of the latest UHF standard document defines conformance issues such as interrogator and tag general conformance requirements, command structure and extensibility. The biggest portion of the standard document is about protocol requirements. It describes protocol overview of physical and tag-identification layers, protocol parameters for signaling and logical operating procedures. The description of operating procedure comprises of two main parts. The first is signaling and the second tag selection, inventory and access. Signaling part deals with operational frequencies, interrogator-to-tag and tag-to-interrogator communications, transmission order, cyclic redundancy check (CRC) and link timing issues. Tag selection, inventory and access part defines tag memory usage. (EPCglobal, 2008)

4.1.2 Infrastructure for Data Capture

EPC data is created by user operations that create EPCs for new objects, follow the movements of objects (by sensing their EPCs) and gather this information to records. EPC data capture needs several major infrastructure components for gathering and recording EPC data. EPCglobal Architecture framework defines interfaces for these components and so provides the means to build EPC systems using interoperable components. (Traub et al. 2010)

The EPC Infrastructure for Data Capture ratified standards include low level reader protocol, reader management, tag data translation, application level events (ALE) and EPC Information Services (EPCIS) capture interface. EPCIS Data standard and business vocabulary are also ratified, but they are described in the next part since they can exist it both Data Exchange or Infrastructure parts depending on application. Standard for Discovery, Configuration, and Initialization (DCI) for Reader Operations is still in development and not ratified yet. As mentioned in the previous part EPC Tag Data Standard can be

perceived to be part of Infrastructure for Data Capture, so it is described here. (Traub et al. 2010)

EPC Tag Data Standard defines the Electronic Product Code and the memory contents of Gen 2 RFID Tags. The Electronic Product Code is designed to be an universal identifier for any physical object. But though a large portion of EPC applications use RFID tags as data carriers, EPC identifiers also exist in non-RFID applications. EPC identifiers can realized in URI form used within information systems, printed human-readable EPC URIs or EPC identifiers derived from bar code data following the procedures in this standard. (GS1, 2011a)

Low Level Reader Protocol (LLRP) specifies an interface between RFID Readers and Clients. The protocol is called low-level because it provides control of RFID air protocol operation timing and access to air protocol command parameters. These abilities are needed since there is a requirement in some RFID systems for explicit knowledge of RFID air protocols and the ability to control readers that implement RFID air protocol communications. The LLRP functionalities include means to command RFID readers, read tags, write tags, execute other protocol-dependent access commands, control forward and reverse radio frequency link operation, retrieval of reader device capabilities, define vendor specific extensions to the protocol and so forth. LLRP is designed to be aware of regulatory requirements in such way that the functions it provides would be applicable worldwide. (EPCglobal, 2010a)

Reader Management (RM) standard defines wire protocol for monitoring the operating status and health of EPCglobal compliant tag readers. The RM protocol is used in interaction of management software and devices capable of interfacing with tags, that can be referred as Reader and Host. This standard focuses only on the protocol required to monitor the health of the reader and the actual collection of tag data between Reader and Host is defined in the EPCglobal Reader Protocol. (EPCglobal, 2007a)

EPC Tag Data Standard (TDS) provides machine readable framework for EPC validation and translation. It is created to help EPC identifier implementation to future applications that may be adopted by additional industry sectors or use additional EPC identifier schemes and to indicate how existing coding systems should be embedded within the EPC. TDS also describes how to translate between the three representations of EPC: binary format and two URI formats. The first URI format is for tag encoding and the other for pure identity. TDS describes human readable encoding and decoding rules for each these coding schemes. (GS1, 2011)

Application Level Events (ALE) is an interface for clients to interact with filtered and consolidated EPC and related data from variety of sources. Most EPC processing systems have some level of processing to reduce the volume of data coming from EPC data sources such as RFID readers. Ale interface

provides independence between raw EPC data acquirement of the infrastructure components, filtration and counting data of the architectural components and data usage of applications. This division of functionalities allows changes in one area without required changes in others. It also provides the possibility to specify what kind of data and operations are needed, without limiting possible implementation strategies or internal interfaces within a specific software applications. (EPCglobal, 2009)

EPC Information Services (EPCIS) Capture Interface is the first of the EPCIS interfaces when following the division used in this thesis. The Capture Interface is an interface for real time delivering of events from Capturing Applications to consumers including Repositories, Accessing Applications and trading partners. The other two EPCIS interfaces Query Control and Callback Interface are described in the Data Exchange chapter. (EPCglobal, 2007b)

4.1.3 Data Exchange

EPC Data Exchange standards provide the means for users to share EPC data to different groups, access to EPC Network services and other shared services that facilitate these exchanges. The benefit for end users comes from increasing visibility to global scale movement of physical objects. (Traub et al. 2010)

The first two Data Exchange standards EPCIS Data Standard and Core Business Vocabulary were mentioned already in the previous part, since they can belong to Infrastructure or Data Exchange. EPCIS Query Interface was also mentioned in the previous part since it's function relates to EPCIS Capture Interface. Other Data Exchange Standard include Pedigree Standard, EPCglobal Certificate Profile and Object Naming Service (ONS). Discovery Services also belong to this part, but is still in development at the time this thesis is written and for this reason it is not included. (Traub et al. 2010)

EPCIS Data Standard framework elements has two layers: Abstract Data Model Layer and Data Definition Layer. The Abstract Data Model Layer specifies generic structure of EPCIS data and general requirements and rules for creating data definitions in the Data Definition Layer. The Data Definition Layer specifies the abstract structure and meaning of the data exchanged through EPCIS. (EPCglobal, 2007b)

The EPCIS Query Interface defines where EPCIS Accessing Application can requests EPCIS data and how the data is delivered. EPCIS data requested from EPCIS Repository or EPCIS Capturing Applications, in which the Query Interface specifies the exact location. The Query Interface also provides the means for mutual authentication and delivers authentication results between the the two parties. (Traub et al. 2010) This Interface consists of two individual interfaces called EPCIS Query Control Interface and EPCIS Query Callback In-

terface that are collectively called the EPCIS Query Interface. (EPCglobal, 2007b)

EPCglobal Pedigree Standard specifies an architecture for maintenance and exchange of electronic pedigree documents. A pedigree is a certified record that contains product- , transaction-, distributor -and recipient information of a prescription drug. These documents are used in pharmaceutical supply chains to ensure that only authentic products are distributed through the supply chains and so help the battle against drug counterfeiting. The standard specifies two XML Schema documents. First is Schema for standard electronic pedigree format and second a standard electronic envelope format for packaging multiple pedigree documents for exchange. Schemas are designed to allow multiple interpretations of US and international pedigree laws and it includes a version mechanism to allow for future changes. (EPCglobal, 2007c)

Certificate Profile Standards function is to ensure secure usage EPCglobal network without compromising broad interoperability and rapid deployment. This is achieved through issuance and usage of X.509 certificate in the EPCglobal Network. The profiles are based on two IETF standards. First of the two is Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List, specified in RFC3280. The second profile is Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List, specified in RFC 3279. These profiles are chosen for the EPCglobal Network because they have been well implemented, deployed and tested in many existing environments. (EPCglobal, 2010b)

Object Name Service (ONS) is a mechanism to access data related to EPC. This data can be for example product or service data. ONS does not contain any actual data about the EPC, only network addresses to services that for the data in question. ONS is an authoritative entity in the sense that it assigns data to EPCs and has change control over EPC information. ONS uses Internets Domain Name System (DNS) for resolving EPC information, which means that when the EPC is converted to a domain-name the result must be a valid DNS Resource. (EPCglobal, 2008b)

4.2 ETSI Standards

Machine to Machine (M2M) is a leading paradigm towards IoT, but very little standardization for it can be found. Instead multiplicity of current solutions use standard Internet, Web and Cellular technologies. (Atzori, Iera, & Morabito, 2010)

As a classical definition, Machine-to-Machine (M2M) refers to common wireless and wired technologies that allow systems and devices to communic-

ate with each other. M2M captures events using devices such as sensors or meters to capture different events. Events can relate to quantities of products in stock or a phenomenon such as temperature or humidity. This data is then relayed through a network to an application. Application translates this data into meaningful information. In IoT clusters of devices form M2M networks that are connected to its infrastructure which is the traditional "Internet of people". (Daradkeh et al., 2012)

ETSI has published several standards concerning M2M. In table 2 there is a list of standards with their standard numbers, titles and scopes.

TABLE 2 List of ETSI Machine-to-Machine Communication standards

Standard No	Title	Scope
TS 102 689	M2M Service requirements	Describes the end to end system requirements in terms of capabilities for supporting M2M communication services.
TS 102 690	Functional architecture	Describes the M2M functional architecture to deliver M2M services to applications.
TR 102 691	Smart Metering Use Cases	Technical Report that collects the use cases which have been identified for the Smart Metering application.
DTR/M2M-00004	M2M definitions	Record of all M2M specific definitions in order to ensure consistent use of terminology across all M2M standards. Scheduled publication: 20.7.2012
TS 102 921	mIa, dIa and mId interfaces	Specification of mIa, dIa and mId interfaces as for ETSI TS 102 690, in terms of protocols/API, the data model and the encoding.

4.2.1 M2M service requirements

ETSI standard document TS 102 689 describes M2M service requirements to enable consistent and cost-effective communication for wide-range of ubiquitous applications. The scope of the document lists requirements for efficient end-to-end delivery of M2M services. This standard, together with the architecture specification, forms the basis for detailed technical specifications for M2M communications. (ETSI 2010a)

The document contains the following five clauses. First: general requirements, that describes features for communication necessary for the correct establishment of M2M communications. Second: management, specifications for required management models for malfunction detection, configuration, accounting, etc. Third: functional requirements for M2M services, describing functional requirements for M2M data collection & reporting, remote control operations, etc. Fourth: security, requirements for M2M device authentication, data

integrity, privacy etc. And fifth: naming, numbering and addressing schemes specific to M2M. (ETSI 2012a)

4.2.2 M2M functional architecture

ETSI M2M functional architecture standard TS 102 690 is an overall end-to-end architecture, including identification of the functional entities and related reference points. The functional architecture is designed to use an underlying IP-network, that can be provided by 3G or other IP capable networks. The use of any available IP capable network is not intentionally excluded from the document. (ETSI 2011a)

The high level architecture for M2M includes a device and gateway domain and network domain. The device and gateway domain consists of M2M Device, M2M Area Network and M2M Gateway. M2M devices can connect to the network domain via M2M Gateway as a proxy or directly using the access network. Using direct connectivity networking procedures, such as registration, authentication, authorization, management and provisioning are performed by M2M device it self. The M2M device may also provide service to other devices connected to it that are hidden from the network domain. If Gateway as a network proxy approach is used, the gateway performs networking procedures towards the network domain. It may also run applications that collect and treat information from sensors. M2M area network provides connectivity between M2M devices and M2M gateways. M2M area networking technologies include personal area networks such as IEEE 802.15.1, Zigbee, Bluetooth, IETF ROLL, ISA100.11a or local networks such as PLC, M-BUS, Wireless M-BUS and KNX. (ETSI 2011a)

The Network Domain is composed of Access Network, Core Network, M2M Service Capabilities and M2M applications. The Access network creates the means for the M2M Device and Gateway Domains to communicate with the Core Network. The Access Network technologies include for example xDSL, HFC, satellite, GERAN, UTRAN, eUTRAN, W-LAN and WiMAX. The Core Network provides at minimum IP connectivity, but potentially other connectivity means as well, such as service and network control functions, interconnection with other networks and roaming. Different core networks can also offer different feature sets. Examples of Core Network technologies are 3GPP, TISPAN and 3GPP2 core networks. M2M Service Capabilities provide functions that are shared by different applications, expose functions through a set of open interfaces, use Core Network functionalities and simplify and optimize application development and deployment through hiding network specificities. Finally M2M Applications run the service logic and use M2M Service Capabilities accessible through an open interface. (ETSI 2011a)

4.2.3 Smart Metering Use Cases

ETSI standard document TR 102 691 collects the use cases, which have been identified for the Smart Metering M2M application. As mentioned before in the Emergence of Standards chapter this work was commissioned by an EU mandate. The documented use cases identify actors and information flows and thus form the basis of future work on M2M on Smart Metering. The Use Cases describe a system from the user point of view describing what the actor achieves from interacting with the system. These Use Cases are then used for deriving requirements on the system. Each Use Case is described in the same manner using the same structure. (ETSI 2010b)

4.2.4 mIa, dIa and mId Interfaces

ETSI standard document TS 102 921 contains the specification for mIa, dIa and mId reference points of the M2M architecture as identified in Functional Architecture document. Main aspects of these specifications are described in terms of protocols/API, definition of resources and sub-resources using the APIs data model and coding. (ETSI 2012)

4.3 IETF Standards

Internet Engineering Task force (IETF) is the open recognized International Standards Organization (ISO) in charge of standardizing the IP protocol. IETF is organized into working groups that work on several areas including routing, transport and security. Three IETF working groups are currently working on standards for IP protocol for smart objects: 6LowPAN (Ipv6 over IEEE 802.15.4), ROLL (Routing Over Low power and Lossy networks) and Constrained RESTful Environments (CoRE) working group (working on CoAP protocol) (Dunkels & Vasseur, 2009).

To promote the Internet Protocol as the network technology for Smart Objects and support for IETF standardization work in this field, IPSO (IP for Smart Objects) Alliance was formed in 2008 by 25 founding companies. (Atzori et al., 2010) It is stated in IPSO whitepaper that IP has proven to be flexible, scalable, efficient and open based networking technology and it can meet the requirements of highly constrained smart object networks. This added with the progress in low-cost embedded devices is the reason why IPSO believes IP is the technology that makes IoT a reality. (Dunkels et al., 2009)

4.3.1 6LowPAN

Low-Power wireless personal area network (LoWPAN) devices conform to the IEEE 802.15.4-2003 standard by the IEEE. Device characteristics include short range, low bit rate, low power and low cost. These properties enable LowPAN network to be simple low cost wireless communication network for applications with limited power and relaxed throughput requirements. Typically LoWPAN devices work together to connect the physical environment to the real world applications such as wireless sensors. (Kushalnagar, Montenegro, & Schumacher, 2009)

The benefits from utilizing IP networks includes flattening the naming and addressing hierarchy in addition to simplifying the connectivity model. This means that complex gateways are not required to translate between proprietary protocols and standard IP, but they can be replaced with much simpler bridges and routers. Also the tools and knowledge of developers for commissioning, configuring, managing and debugging IP based protocols are readily established. (Mulligan, 2007)

6LowPAN has become the standard for low-rate wireless personal area networks (LR-WPAN). 6LowPAN is short for Ipv6 over IEEE802.15.4, which means Ipv6 is used as an interconnection scheme in the network layer of IEEE802.15.4 equipment. 6LowPAN is expected to have a large adoption in different application areas due to its cheapness and practicality. Almost any equipments that benefit from low price, low-rate, low power and dense deployment characteristics, could be realized by 6LowPAN technology, especially in the industrial wireless domain (Ma & Luo, 2008).

4.3.2 RPL

Low-power and Lossy Networks (LLNs) consist of nodes with constraints concerning processing power, memory and in many cases also energy. In many cases nodes are not mains powered but battery operated or energy scavenging. LNN characteristics offer many challenges to routing solutions, concerning network links and traffic. Nodes are interconnected by lossy links that support only low data rates, are unstable and have relatively low packet delivery rates. Network traffic patterns are usually point-to-multipoint, rather than point-to-point and networks may consist of thousands of nodes (Winter et al., 2012).

Routing Over Low power and Lossy networks (ROLL) working group was created by IETF to standardize a routing protocol for networks of highly energy constrained and static wireless sensors transmitting very small quantities of data. (Watteyne, Molinaro, Richichi & Dohler, 2011) ROLL working group has defined application-specific routing requirements for Ipv6 Routing Protocol for LLNs (RPL). Specific applications are specified in RFC5867 (Building Auto-

mation), RFC5826 (Home Automation), RFC5673 (Industrial) and RFC5548 (Urban). Although RPL is specified according to the requirements of these application requirements, it's use is not meant to be any way limited to these applications (Winter et al., 2012).

RPL designs include several special characteristics compared to other routing protocols. Here are some examples. Multiple concurrent RPL instances can be present in a single network and each instance may serve different constraints or performance criteria. Packet processing and forwarding is separated from routing optimization, for minimizing energy or latency or satisfying constraints. Neighbor Unreachability Detection (NUD) and Bidirectional Forwarding Detection (BFD), for verifying bidirectional links is needed in RPL operations.

4.3.3 CoAP

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol that realizes the Representational State Transfer (REST) architecture. CoAP is designed to be used in most constrained networks between constrained nodes, such as sensors and actuators. In addition CoAP can be translated to Hypertext Transfer Protocol (HTTP) for linking constrained nodes and nodes on the Internet. CoAP application areas include different forms of M2M communication in construction, health care, transportation or any other area utilizing sensor and actuator devices for monitoring and interacting with the environment (Jimenez, Lopez-Vega, Mäenpää & Camarillo, 2012).

CoAP provides a method/response interaction model between application endpoints, supports built-in resource discovery, includes key web concepts, multicast support, low overhead and translates to HTTP for web integration purposes. The protocol is also kept simple enough to be utilized in constrained environments. The main features of CoAP include: constrained web protocol for M2M, UDP binding, asynchronous messaging, low header overhead, low parsing complexity, URI support, content-type support, simple proxy capabilities, caching capabilities, stateless HTTP mapping and security binding to Datagram Transport Layer Security (DTLS). (Shelby, Hartke, Bormann & Frank, 2012)

CoAP interaction model is similar to HTTP client/server model, except that CoAP implementation acts in both client and server roles. A CoAP and HTTP requests are equivalent. In both protocols request is set by a client to request an action defined by a method code on a resource on a server that is identified by a Universal Resource Identifier (URI). The server then replies with a response code and resource representation. But unlike HTTP, CoAP interchange is asynchronous over a datagram oriented transport such as User Datagram Protocol (UDP). Interchange uses layer of messages that support optional

reliability. CoAP message types are Confirmable, Non-Confirmable, Acknowledgment and Reset, that are transparent to the request/response interactions in basic exchanges. CoAP can be logically realized as a two-layer approach, where messaging layer deals in asynchronous interactions with UDP and request/response layer deals with interactions using method and response codes. (Shelby et al., 2012)

4.4 Chapter summary

A summary of the standards discussed in this chapter is provided in Table 3. The table shows which of the standards are considered to be horizontal and if they are early or late standards. Based on this information some conclusions can be done about the nature of these standards. The next chapter deals with some of these conclusions.

TABLE 3 Overview of existing standards

Organization	**Std description**	**Nature**	**Early vs. late**	**Status**
EPCglobal	Electronic Product Code	Vertical	Early	Ratified and in production use
ETSI	M2M Standards	Horizontal	Early/late	Communications: publication 2011 Functional architecture: publication 2011 Smart metering Use cases: publication 2010 M2M definitions: Stable draft 2012 mIa, dIa and mId interfaces: publication 2012
IETF	IP Protocol for Smart Objects	Horizontal	Late	6LowPAN: Proposed Standard RPL: Proposed Standard CoAP: in development

5 . Conclusions

IoT is a fairly new concept as the term was first introduced only little over ten years ago and it has been gaining more and more popularity in academia and industry since then. As a vision IoT is very powerful, since it is so ubiquitous, all-embracing and because of the magnitude of consequences it's future materialization might have. And yet there are still many puzzles to solve before these visions will become reality.

There are also differences of the visions of many stakeholders as discussed in the introduction chapter. For example more things oriented vision predict the use of Intranet of Things solutions that would be translated to the Internet through gateways. More internet based visions, promote the view that IP communication should be used across the line. These views can also be seen in the existing and upcoming standards discussed in existing standardization chapter. EPCglobal and ETSI standards can be seen as more things oriented as they both deploy architectures that use a gateway between the application and internet domains. As IETF standards clearly emphasize a very internet based view, as they state that complex gateways are not needed between proprietary protocols and standard IP.

In the view of early versus late standardization the examples given on existing standards in this thesis are also different. IETF standardization can be considered as late standards, since their aim is to integrate IoT functionalities seamlessly as possible to existing internet infrastructure. ETSI M2M standards on the other hand do not describe any strict normative rules for technology, but system requirements and architecture for a communication, so they are some where in the middle with the early vs. late standardization issue. The EPCglobal standards the describe the use of technologies normatively, so they fall more into early standardization.

While EPCglobal standards are the only standards mentioned in this thesis that are actually in production use and have wide adoptation, they are also the only example of vertical standards. Even though they have some expandab-

ility, they are tailored to supply chain management and other very similar forms of applications. EPCglobal standards are also the only one of these standards that actually define a whole infrastructure for application deployment. ETSI and IETF standards do not specify whole infrastructures. ETSI M2M standards specify an architecture and requirements for a M2M communication, but they do not have limitations to the application domain or even the technologies used. IETF standards are network standards suited to any prospective use and they also do not have any restrictive nature for application domain. For this reason ETSI and IETF standards are perfect examples of the up and coming horizontal standards.

Another source of different views on the development of IoT technologies and standards is caused by different interests of stakeholders in different parts of the world. China is focusing more on smart city concepts and is demanding for earlier standardization. The United States on the other hand has emphasizes more of it's efforts on sensor networks. History knows many examples where overlapping technology standards have produced a lack of interoperability. One good example of this is Japanese 2G mobile phone technology that is incompatible with it's European counterparts. Global differences can also be caused by differences of current technologies as discussed in challenges for global standardization chapter. Global differences need to be solved through common standardization. But in many cases there will probably be a need for flexibility in standards that take account and finds solutions for these differences.

For the research question of this thesis there are some points that can be regarded as results. Common standardization and understanding of the IoT domain is crucial for the realization of the paradigm. IoT standards can emerge from new technology standards or they can be mandated to fulfill the needs of future technologies. But perhaps the biggest effect on cost effectiveness and faster real life deployment of these technologies could be achieved through more horizontal standardization.

Further research in this area is not hard to find. Any of the presented standards and their possible application domains propose enough research questions for a thesis.

REFERENCES

Akyildiz, I.F. Su, W. Sankarasubramaniam, Y. Cayirci, E. 2002, Wireless sensor networks: a survey, Computer Networks 15 March 2002: (Volume 38, Issue 4) p. 393-422. Web of Science 2002.

Atzori, L. , Iera, A. & Morabito G. 2010, The Internet of things: A survey, Computer Networks 28 October 2010: (Volume 54, Issue 15) p. 2787-2805, Web of Science, 2010.

Bandyopadhyay, D. Sen, J. 2011, Internet of Things: Applications and Challenges in Technology and Standardization, Wireless Personal Communications 58: (1) p. 49-69, Web of Science, 2011.

Bandyopadhyay, S. Sengupta, M. Maiti, S. & Dutta S. 2011, A Survey of Middleware for Internet of Things, Communications in Computer and Information Science 162 CCIS: () p. 288-296.

Commission of the European Communities (2009). Internet of Things – An action plan for Europe. http://eur-lex.europa.eu/LexUriServ/site/en/com/2009/com2009_0278en01.pdf

Daradkeh, Y. Namiot, D. Sneps-Sneppe, M., M2M Standards: Possible Extensions for Open API from ETSI, EuroJournals Publishing Inc, 2012.

Dunkels, A. Vasseur, J.P. , IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #1, September 2008, http://www.ipso-alliance.org

Estrin, D. Govindan, R. Heidemann, J. Kumar, S. Next century challenges: scalable coordination in sensor networks, Mobile computing and networking: Proceedings of the 5th annual ACM/IEEE international conference, (MobiCom '99), 1999, pp.263-270, Association for Computing Machinery, 1999.

EPCglobal, 2007a, Reader Management Version 1.0.1. http://www.gs1.org/gsmp/kc/epcglobal/rm/rm_1_0_1-standard-20070531.pdf

EPCglobal, 2007b EPC Information Services (EPCIS) Version 1.0.1. http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_0_1-standard-20070921.pdf

EPCglobal, 2007c, Pedigree Ratified Standard Version 1.0. http://www.gs1.org/gsmp/kc/epcglobal/pedigree/pedigree_1_0-standard-20070105.pdf

EPCglobal, 2008a, EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version

1.2.0. http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf

EPCglobal, 2008b, EPCglobal Object Name Service (ONS) Version 1.0.1. http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_1_0_1-standard-20080529.pdf

EPCglobal, 2009 The Application Level Events (ALE) Specification, Version 1.1.1 Part I: Core Specification EPCglobal Ratified Standard. http://www.gs1.org/gsmp/kc/epcglobal/ale/ale_1_1_1-standard-core-20090313.pdf

EPCglobal, 2010a, Low Level Reader Protocol (LLRP) Version 1.1. http://www.gs1.org/gsmp/kc/epcglobal/llrp/llrp_1_1-standard-20101013.pdf

EPCglobal, 2010b, EPCglobal Certificate Profile Specification Version 2.0. http://www.gs1.org/gsmp/kc/epcglobal/cert/cert_2_0-standard-20100610.pdf

ETSI, 2010a, Machine-to-Machine communications (M2M); M2M service requirements, European Telecommunications Standards Institute 2010. http://pda.etsi.org/exchangefolder/ts_102689v010101p.pdf

ETSI, 2011, Machine-to-Machine communications (M2M); Functional architecture, European Telecommunications Standards Institute 2011. http://pda.etsi.org/exchangefolder/ts_102690v010101p.pdf

ETSI, 2010b, Machine-to-Machine communications (M2M); Smart Metering Use Cases, European Telecommunications Standards Institute 2010b. http://pda.etsi.org/exchangefolder/tr_102691v010101p.pdf

ETSI, 2012, Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces, European Telecommunications Standards Institute 2012. http://pda.etsi.org/exchangefolder/ts_102921v010101p.pdf

Finkenzeller, K. 2003, RFID Handbook, John Wiley & Sons Inc, 2003.

GS1, 2011a, GS1 EPC Tag Data Standard 1.6. http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf

GS1, 2011b, GS1 EPCglobal Tag Data Translation (TDT) 1.6. http://www.gs1.org/gsmp/kc/epcglobal/tdt/tdt_1_6_RatifiedStd-20111012-i2.pdf

IEEE C80216-10_0002r7, "Machine to Machine (M2M) Communication Study Report," IEEE802.16 Contribution, May, 2010. http://www.ieee802.org/16/ppc/docs/80216ppc-10_0002r7.doc

International Telecommunications Union, 2005, The Internet of Things, ITU, 2005. http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

Jimenez, J. Lopez-Vega, J. Maenpaa, J. Camarillo, G. 2012, A Constrained Application Protocol (CoAP) Usage for REsource LOcation And Discovery (RELOAD), P2PSIP Internet-Draft, February 2012. http://tools.ietf.org/pdf/draft-jimenez-p2psip-coap-reload-01.pdf

Kushalnagar, N., Montenegro, G., & Schumacher C. (August 2009). IPv6 over Lo-Power Wireless Personal Area Networks (6LoWPANs): Overview, assumptions, problem statement, and goals, IETF RFC 4919. http://tools.ietf.org/html/rfc4919

Ma, X. Luo, W. , The analysis of 6LowPAN technology, Proceedings - 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, PACIIA 2008, p. 963-966, IEEE, 2008.

Mattern, F. & Floerkemeier, C. , Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 6462 LNCS: () p. 242-259, Springer Berlin / Heidelberg 2010

Mulligan, G. 2007, The 6LoWPAN Architecture, Proceedings of the 4th Workshop on Embedded Networked Sensors, EmNets 2007: () p. 78-82, Association for Computing Machinery, 2007.

Shelby, Z. Hartke, K. Bormann, C. Frank, B. 2012, Constrained Application Protocol (CoAP), IETF CoRe working group, 2012. http://datatracker.ietf.org/doc/draft-ietf-core-coap/

Sundmaeker, H. Guillemin, P. Friess, P. Woelfflé, S. 2010, Vision and Challenges for Realizing the Internet of Things. IERC cluster book. IERC, 2010.

Tarkoma, S. Katasonov, A. 2011, Internet of Things Strategic Research Agenda (IoT-SRA) Finnish Strategic Center for Science, Technology 2011.

Traub, K. Armenio, F. Barthel H. Dietrich, P. Duker, J. Floerkemeier, C. Garrett J. Harrison, M. Hogan, B. Mitsugi, J. Preishuber-Pfluegl, J. Ryaboy, O. Sarma, S. Suen, K. Williams, J. 2010, The EPCglobal Architecture Framework EPCglobal Final Version 1.4. http://www.gs1.org/gsmp/kc/epcglobal/architecture/architecture_1_4-framework-20101215.pdf

van Kranenburg, R. , Caprio, D. , Anzelmo, E. , Dodson, S. , Bassi, A. , Ratto, M. Internet of Things, 1st Berlin Symposium on Internet and Society Oct 26-28.2011

van der Veer, H. Wiles A. (2008), ETSI White Paper No.3 Achieving Technical Interoperability – ETSI approach. Third edition. , ETSI 2008. http://www.etsi.org/WebSite/document/whitepapers/IOP%20whitepaper%20Edition%203%20final.pdf

Walewski, J. 2011, Initial architectural reference model for the IoT - v0.9 , IoT-A , 2011 http://www.iot-a.eu/public/public-documents/documents-1/1/1/d1.2/at_download/file

Watteyne, T. Molinaro, A. Richichi, M. G. Dohler, M. , 2011, From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols,

IEEE Communications Surveys & Tutorials 20111001 13(4): p.688, IEEE 2011

Winter, T., Thubert, P. Brandt, A. Hui, J. Kelsey, R. Levis, P. Pister, K. Vasseur, JP. Alexander, R. 2012, RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, IETF ROLL working group RFC6550, 2012. https://tools.ietf.org/html/rfc6550

Wu, NC. Nystrom, MA. Lin, TR. Yu, HC. 2006, Challenges to global RFID adoption, Technovation, 2006, Vol.26(12), pp.1317-1323, Elsevier, 2005.