Chapter 7

The Internet of Things – Setting the Standards

7.1. Introduction

Although the Internet of Things (IoT) is seen as a vision of what is to come, rather than a technology in and of itself, it reflects trends in both technological innovation and business strategy. It refers to the convergence of previously disparate telecommunication technologies to create an environment with ubiquitous communication capabilities. For the IoT to become a reality, the development of many different types of technology will have to be coordinated, ranging from item labeling and process control to wireless technology and network interconnection.

These requirements are illustrated in Figure 7.1. Product identification refers to the mechanisms by which individual items can be identified and tracked, via for instance traditional bar codes or radio-frequency identification (RFID) tags. Sensor network and home automation technologies that have developed from industrial process control systems make it possible to monitor the ambient environment. Wireless technology is of course a pre-requisite (enabling any

Chapter written by Keith MAINWARING and Lara SRIVASTAVA.

The Internet of Things: Connecting Objects to the Web Edited by Hakima Chaouchi

physical object to become a part of this ubiquitous network) as is network interconnection via the Internet (enabling global access and reach). Although wireless access technology will become prevalent, there will continue to be a role for wired systems such as power line communication (PLC) within the home.

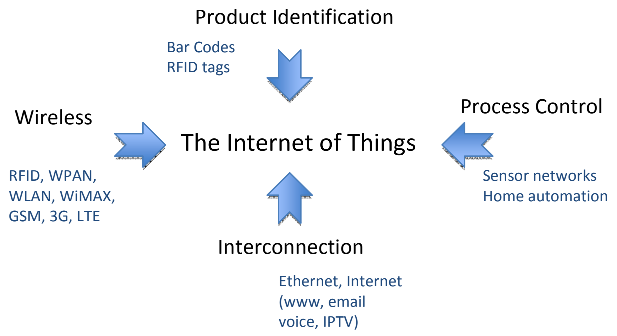


Figure 7.1. *The convergence of product identification, process control, wireless and interconnection technology applications*

The IoT will consist of objects with tags and networked readers, writers, sensors and actuators. The telecommunication systems of today that primarily support interpersonal and person-to-machine interaction will be enhanced with an increasing array of machine-to-machine communications.

This chapter begins by discussing the importance of standardization for the IoT. It then takes a more focused look at the technical specifications for RFID, which, in the early days, had primarily been used in inventory control and logistics applications, but whose field of application is growing steadily everyday [SRI 05, SRI 07]. It continues on by examining how objects are identified and outlines data formats and mechanisms for information access. The future of ubiquitous networking is also discussed with specific reference to wireless sensor networks and home networking. Finally, the challenges arising from the IoT in the context of privacy and data protection are considered.

7.2. Standardizing the IoT

Given the ongoing and emerging convergence of technology areas, a diverse number of organizations from previously separate industry segments are involved in the specification of systems and their standardization. Not surprisingly, this has led to some overlap in activities because these organizations are each working in their own specific area of expertise. The result has been a bewildering array of standards. A 2008 European study on RFID alone noted that more than 250 standards describing RFID-related solutions had been established by around 30 different organizations [CER 08]. In this context, international standardization organizations can play an important role in harmonizing specifications and creating interoperable global standards for the IoT.

The most important organizations setting standards for the IoT are:

– EPCglobal, the Ubiquitous ID Center and ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) in the area of defining identifier formats and short-range radio technology;

– the IEEE 802 standards committee on local and personal area networks; and

– the Internet Engineering Task Force (IETF) for the suite of protocols that provide end-to-end connectivity over the Internet.

The ITU-T (International Telecommunication Union – Telecommunication standardization sector) is also playing a role in harmonizing standards and producing system-level descriptions of ubiquitous networks.

7.2.1. *Why standardize?*

Standards can be used to increase product quality (i.e. meeting performance and safety requirements) and to ensure the interoperability of various components in a system. It is this latter aspect that is of interest in the present context. Standards are particularly valuable in cases where interfaces between components are produced by different companies (whether or not these are physically separate pieces of equipment) or where items of equipment are owned by different organizations. Ideally, standardization should provide mutual benefits for equipment vendors, service providers and their customers, by stimulating the overall growth of a particular market.

In general, significant benefits are to be gained by standardization of:

– the information to be transferred, such as the format of the identifier and the application data;

– the characteristics of the interfaces;

– the protocols for data transfer over the various interfaces; and

– other functions, such as routing and security.

In addition to the standardization of interface specifications and protocols, companies may also be required to follow specific regulations. Examples include those concerned with radio frequency usage (e.g. to ensure the interoperability of equipment) or those concerned with the protection of consumers using the technology (e.g. data protection legislation and guidelines).

7.2.2. *What needs to be standardized?*

The IoT can be viewed as a subset of a future Internet in which communication capabilities will become ubiquitous. However, it is widely acknowledged that the IoT suffers from a fragmentation of standards. For example, EPCglobal, ISO and Japan's Ubiquitous ID Center have defined formats for tag data. At the same time, other organizations have been active in defining local and wide-area network connectivity standards. It is therefore necessary to consider the technology and standards produced in the four areas (see Figure 7.1) that are converging and how these technologies can be integrated in a complete system with end-to-end connectivity. For instance, the standardization of sensor networks is relevant to the broader picture of standardization activities in this area. Home networking also provides an example of how RFID, sensor networks, wireless and fixed (e.g. PLC) communication links and the more familiar applications of the Internet might be integrated. Some of the standards relating to ubiquitous networking in next generation networks are relevant in this context.

Figure 7.2 [ITU 08] provides a good framework in which to consider the various elements of the IoT. It shows the identifiers, interfaces and some of the wide-area network functions involved in connecting "things" to the Internet. In illustrating how the various technologies can be integrated to create an IoT, it reflects the areas of convergence illustrated in Figure 7.1. It can be used as an effective model for analyzing standardization activities in each area.

More specifically, in a typical system an object is assigned a tag with an identifier. In some cases, additional application data can be associated with the object. These application data could, for instance, be provided by a sensor collocated with the tag. The identifier and application data are read over a short-range radio frequency interface, such as RFID, or by a scanner. This interface can also be used to write application data to the tag. ID terminals, such as readers and sensors, will use low-power wireless networks – networks that can be connected to the global Internet.

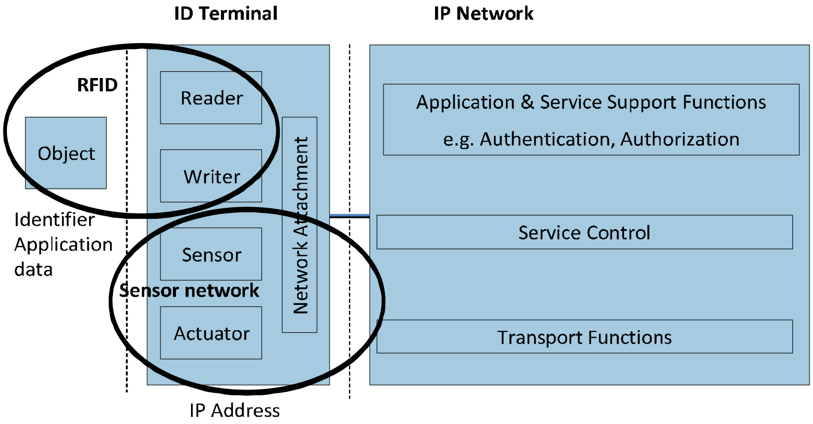


Figure 7.2. *Reference model for the IoT, adapted from reference architecture for tag-based applications in ITU-T recommendation Y.2213*

In summary, therefore, the key areas requiring standardization are as follows: the identification of things, the methods by which information is transferred between things and the devices (ID terminals) that detect or control them the networking of ID terminals, and finally, the method by which ID terminals are connected to the global internet.

7.3. Exploiting the potential of RFID

You could be forgiven for thinking that RFID is synonymous with the IoT as it is vital for identifying objects in real time and for obtaining information about them, be they stationary or mobile. Of course the IoT is much wider in scope than RFID, and involves the interconnection of all sorts of components and devices with different technologies for the creation of a truly ubiquitous networking environment.

7.3.1. *Technical specifications*

RFID enables objects to be tagged, making information stored on these tags readable using short-range wireless technology. This information consists of an identifier and possibly additional application data associated with the object. Information can be written onto the tag, enabling a wide range of tag-based identification services to be offered by a variety of organizations. For instance museums, shops or restaurants can tag objects in their environment to provide further information about them, such as their name, description, price or location. An identifier can be assigned to any entity, such as a physical/logical object, a place or a person. It is stored on an ID tag, such as a barcode, a passive/active RFID tag, a smartcard or an infrared tag.

The specifications for RFID cover the identification of objects, air interface characteristics and data communication protocols. An early application of RFID was for the identification of animals. ISO completed a standard in 1994 that defines the structure of an RFID identification code for animals (ISO 11784). The complementary ISO standard 11785 describes how this tag information is read. The ISO has proceeded to define a complete set of specifications for item management: ISO/IEC standards 15961 through 15963 describe the common data protocol and identifier formats applicable to the ISO/IEC 18000 series of standards that describe the air interfaces at various frequencies. Separate specifications are required for the different frequency bands because the frequency of operation determines the characteristics of the communication capability, e.g. the range of operation or whether transmission is affected by the presence of water.

In addition, ISO 17363 through to 17367 specify supply chain applications (with parts applicable to freight containers, returnable transport items, transport units, product packaging and product tagging) and ISO 18185 describes how RFID can be used to track the movements of freight containers. ISO has also produced performance and conformance test specifications.

In summary, the following ISO/IEC specifications are related to RFID:

– *Animal identification*:

- ISO/IEC 11784 radio-frequency identification of animals – code structure;

- ISO/IEC 11785 radio-frequency identification of animals – technical concept.

– *Item management.*

– Identifiers and data protocol:

- ISO/IEC 15961 data protocol: application interface;

- ISO/IEC 15962 data protocol: data encoding rules and logical memory functions;

- ISO/IEC 15963 unique identification for RF tags.

– Air interfaces.

– ISO/IEC 18000 RFID for item management:

- Part 1: reference architecture and definition of parameters,

- Part 2: <135 kHz;

- Part 3: 13.56 MHz;

- Part 4: 2.45 GHz;

- Part 6: 860 MHz to 960 MHz:

– Type A: pulse interval encoding in the forward link and an adaptive ALOHA collision arbitration algorithm,

– Type B: Manchester encoding in the forward link and an adaptive binary tree collision arbitration algorithm,

– Type C – EPCglobal Class 1 Gen 2;

- Part 7: active air interface at 433 MHz.

– Supply chain applications:

- ISO/IEC 17363 Freight containers;

- ISO/IEC 17364 Returnable transport items;

- ISO/IEC 17365 Transport units;

- ISO/IEC 17366 Product packaging;

- ISO/IEC 17367 Product tagging.

– Testing:

- ISO/IEC 18046 Radio frequency identification device performance test methods;

- ISO/IEC 18047 RFID device conformance test methods.

Another important standards organization in relation to the development of RFID is the Auto-ID Center. The Auto-ID Center was created in 1999 and developed the electronic product codes (EPCs, tag identifiers) that have now been adopted more generally by the industry. EPCglobal is leading the development of industry-driven standards for the EPC to support the use of RFID. EPCglobal has also produced a set of standards for tag data encoding, an air interface protocol operating in the 860 – 960 MHz frequency range, reader protocols as well as information and object name services. An overview of the EPCglobal suite of standards is provided in Figure 7.3.

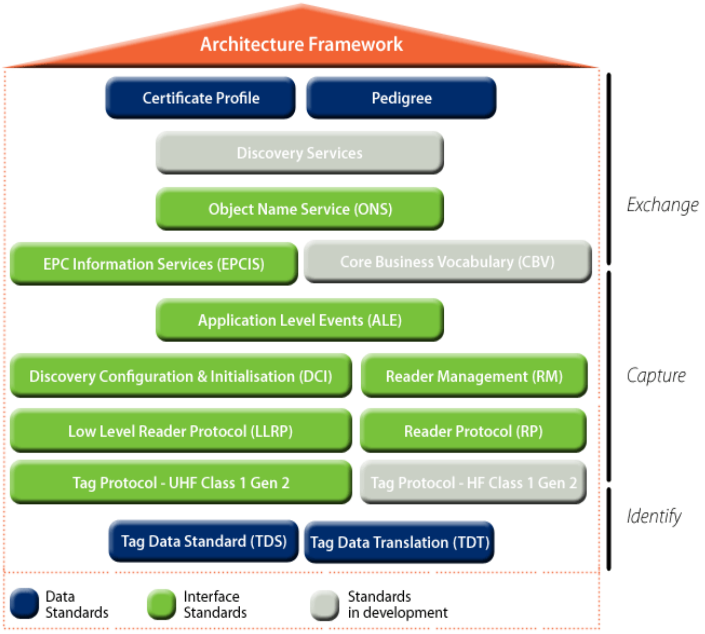

Architecture Framework
Certificate Profile
Pedigree
Discovery Services
Object Name Service (ONS)
EPC Information Services (EPCIS)
Core Business Vocabulary (CBV)
Application Level Events (ALE)
Discovery Configuration & Initialisation (DCI)
Reader Management (RM)
Low Level Reader Protocol (LLRP)
Reader Protocol (RP)
Tag Protocol - UHF Class 1 Gen 2
Tag Protocol - HF Class 1 Gen 2
Tag Data Standard (TDS)
Tag Data Translation (TDT)
Exchange
Capture
Identify
Data Standards
Interface Standards
Standards in development

Figure 7.3. *EPCglobal standards overview*
(Source: http://www.epcglobalinc.org/standards)

The main elements of the EPCglobal suite of standards are as follows:

– The EPC tag data standard defines a number of identification schemes and describes how these data are encoded on tags and also how they are encoded in a form suitable for use within the EPC systems network.

– A machine-readable version of the EPC data formats is given in the EPC tag data translation standard. This can be used for validating EPC identifiers and translating between various representations of the data.

– The tag protocol is an ultra-high frequency RFID air interface. A reader sends information to a tag by modulating a radio frequency signal in the 860-960 MHz range. Tags are passive, in that they receive energy from the signal transmitted by the reader. This air interface protocol has been included in the ISO/IEC 18000 series of specifications as Type C in Part 6. A high frequency air interface is also under development.

– The low level reader protocol is used by a client to control a reader at the level of operation of the air protocol. On the other hand the reader protocol provides an interface between application software and readers. Readers discover clients using the procedures specified in the discovery, configuration and initialization standard.

– The reader management standard is used to monitor the operating status of RFID readers. It is based on use of the simple network management protocol defined by the IETF.

– The application layer events standard provides a means for clients to obtain filtered EPC data. This interface provides independence between the infrastructure components that obtain the raw EPC data, the components that process those data and the applications that make use of the data.

– The EPC information services standard allows the sharing of EPC data within and across enterprises.

– The object naming service standard describes how the domain name system (DNS) can be used to obtain information associated with a specific EPC.

– The EPCglobal certificate profile standard describes how entities within the EPC global network can be authenticated. Use is made of the X.509 [ITU 08b] authentication framework and the Internet public key infrastructure profiles defined in RFC 3280 [HOU 02] and RFC 3279 [BAS 02].

– The pedigree standard specifies the means of handling electronic drug “pedigree” documents for use in pharmaceutical supply chain applications.

In addition, other standardization organizations have also produced complementary specifications on RFID applications. For example, the American National Standards Institute has defined an RFID standard for modern healthcare.

7.3.2. *Radio spectrum and electromagnetic compatibility*

Radio spectrum is a valuable economic and social resource. As is the case with all common goods, it must be managed so that unrestricted usage does not lead to its degradation due to interference between users. International agreements on spectrum allocation have been reached at the ITU and national authorities manage frequency usage within countries. Some spectrum is reserved for specific applications, such as mobile telephony, and can only be used by operators that have a license to offer such services, whereas other parts of the radio spectrum can be used without obtaining a license. For example, the 2,400 MHz band, used for wireless personal area networks (WPANs) described below, is standardized for unlicensed use on a near global basis. However, equipment using unlicensed frequencies must often comply with specific regulations, e.g. to minimize interference, in order to be legally marketed.

There are regional variations in the frequency bands used for RFID around the world, in particular in the 860-960 MHz frequency range: China uses 840-845 and 920-925 MHz, Europe 865-868 MHz, US and Canada 902-928 MHz and Japan 952-954 MHz.

Regulations to limit interference with other systems and for the testing of equipment for approval are applied on a regional or national basis. For example, the Radio and Telecommunications Terminal Equipment Directive sets out the relevant rules for Europe. The key requirements cover health and safety protection, electromagnetic compatibility and the effective use of the radio spectrum to avoid harmful interference with other equipment. RFID-specific requirements are contained in the following European Standards produced by the European Telecommunication Standards Institute (ETSI):

– ETSI EN 300 330: Technical characteristics and test methods for radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz;

– ETSI EN 300 220: Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW;

– ETSI EN 302 208: Radio frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W;

– ETSI EN 300 440: Radio equipment to be used in the 1 GHz to 40 GHz frequency range.

7.4. Identification in the IoT

Electronic product codes were first used to identify a type of product, for example at the point of sale, but they can also be used to identify specific items or examples of a product if a sufficient number of addresses are available. In an IoT, any thing can be assigned an identifier – a physical object, person, place or logical object. A number of different identifier formats have been defined for use with RFID and these are described in section 7.4.1.

The term “identifier” is synonymous with the term “name”. A name does not change with location, in contrast to an “address” which is intended to be used to refer to the location of a thing. IP addresses are used to route packets between end-systems. As the most widespread version of the IP in use at the moment, IPv4, has a limited address space, IPv6 with its greatly increased number of addresses will most likely be adopted for the IoT.

IP addresses play two roles: from a network point of view, they act as a locator and from an application point of view they identify hosts for the duration of a communications session. This dual role is seen to be problematic due to increasing demands for mobility and the multi-homing of end-systems. For this reason the Internet Research Task Force (IRTF) and the IETF have developed the host identity protocol (HIP), which defines host identifiers that can perform the identifier role of the IP address, leaving the IP address to act solely as a locator.

These host identifiers could potentially be used as another type of identifier in the IoT. IPv6 and HIP are described below in sections 7.4.2 and 7.4.3 respectively.

7.4.1. *A variety of data formats*

The standards organizations ISO, EPCglobal and the Ubiquitous ID Center have each defined a number of identifiers with different formats suited to a variety of item-based applications. In each case, the definition of the numbering authority has been based on different principles:

– national registration authorities manage animal identification (see Table 7.1);

– EPCglobal acts as the registration authority for the identity space of specific industry sectors worldwide (see Table 7.2);

– several transnational registration authorities are involved in the ISO item management scheme, including EPCglobal (see Table 7.3); and

– the Ubiquitous ID Center acts as an independent registration authority for its “ucode” numbering system.

The EPCglobal tag data standard specifies two aspects:

– how the data are encoded on the tag itself; and

– how the data is encoded as a uniform resource identifier for use within an EPC systems network.

The EPC identifier is defined so as to support various industry-specific coding schemes (or identity types). These identity types are structured as follows:

– *General Identifier (GID)* – General Manager Number (i.e. organizational entity), Object Class (type of thing), Serial Number.

– *Serialized Global Trade Item Number (SGTIN)* – Company Prefix, Item Reference, Serial Number.

– *Serial Shipping Container Code* (SSCC) – Company Prefix, Serial Reference.

– *Serialized Global Location Number (SGLN)* – Company Prefix, Location Reference, GLN Extension.

– *Global Returnable Asset Identifier (GRAI)* – Company Prefix, Asset Type, Serial Number.

– *Global Individual Asset Identifier (GIAI)* – Company Prefix, Individual Asset Reference.

– *Global Document Type Identifier (GDTI)* – Company Prefix, Document Type, Serial Number.

– *Global Service Relation Number (GSRN)* – Company Prefix, Service Reference.

– *Department of Defense (DoD)* – defined by the United States DoD.

The EPCglobal tag data format consists of a header followed by a number. The header indicates the identity type and the length of the number, as set out in Table 7.2.

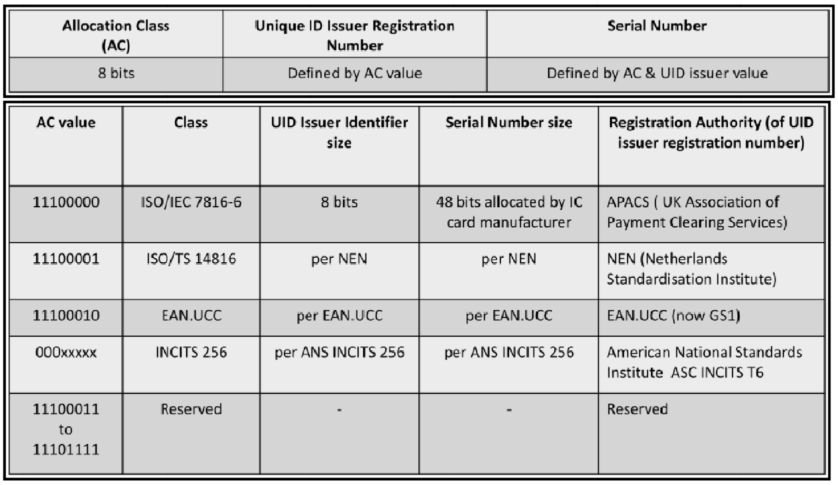
Bit	Information	Combinations	Description
1	Animal (1) or non-animal (0)	2	Signals whether the transponder is application used for animal identification or not
2-4	Retagging counter	8	Indicates that the animal has been retagged with the same number
5-9	User information field	32	Informative content
10-15	Reserved	64	Set to "0"
16	Data block (1) or no data block (0)	2	Signals that additional data are to be received (e.g. physiological data, measured by a device that combines identification and monitoring)
17-26	ISO 3166 country code	1024	Country codes from 900 to 998 may be used to refer to individual manufacturers of transponders
27-64	National ID code	274877906944	Unique within a country

Table 7.1. *Animal identification codes (ISO 11784)*

Header value (hex)	**Identity type and number length**
00	Unprogrammed tag
08	SSCC (Serial Shipping Container Code) – 64 bit
09	SGLN (Serialized Global Location Number) – 64 bit
0A	GRAI (Global Returnable Asset Identifier) – 64 bit
0B	GIAI (Global Individual Asset Identifier) – 64 bit
2C	GDTI (Global Document Type Identifier) – 96 bit
2C	GDTI (Global Document Type Identifier) – 96 bit
2D	GSRN (Global Service Relation Number) – 96 bit
2F	DoD (Department of Defense) – 96 bit
30	SGTIN (Serialized Global Trade Item Number) – 96 bit
31	SSCC – 96 bit
32	SGLN – 96 bit
33	GRAI – 96 bit
34	GIAI – 96 bit
35	GID (General Identifier) – 96 bit
36	SGTIN – 198 bit
37	GRAI – 170 bit
38	GIAI – 202 bit
39	SGLN – 195 bit
3A	GDTI – 113 bit
80 to BF	SGTIN – 64 bit
CE	DoD – 64 bit

Table 7.2. *EPCglobal tag data format [EPC 08]*

Another system for the unique identification of radio frequency tags is described in ISO/IEC 15963. This scheme, in similar fashion to the EPCglobal tag standard, specifies a number of identifier classes. In this case, the allocation class indicates the authority assigning the numbers. Integrated-circuit card manufactures can be registered to assign unique identifiers under the ISO/IEC 7816-6 scheme or the American National Standards Institute INCITS (International Committee for Information Technology Standards) T6 scheme; so can the manufacturers of tags for freight containers and transport applications following the procedures of ISO/TS 14816. EPCglobal identifiers are accommodated within the ISO/IEC 15963 scheme as the EAN.UCC (European Article Numbering – Uniform Code Council) class. EAN is now called GS1, of which EPCglobal is a subsidiary.

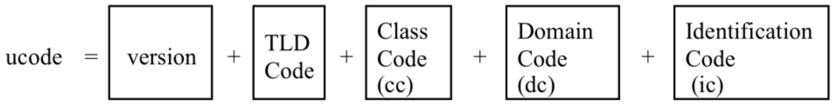


Allocation Class (AC)	Unique ID Issuer Registration Number	Serial Number
8 bits	Defined by AC value	Defined by AC & UID issuer value

AC value	Class	UID Issuer Identifier size	Serial Number size	Registration Authority (of UID issuer registration number)
11100000	ISO/IEC 7816-6	8 bits	48 bits allocated by IC card manufacturer	APACS (UK Association of Payment Clearing Services)
11100001	ISO/TS 14816	per NEN	per NEN	NEN (Netherlands Standardisation Institute)
11100010	EAN.UCC	per EAN.UCC	per EAN.UCC	EAN.UCC (now GS1)
000xxxxx	INCITS 256	per ANS INCITS 256	per ANS INCITS 256	American National Standards Institute ASC INCITS T6
11100011 to 11101111	Reserved	-	-	Reserved

Table 7.3. *ISO/IEC unique ID*

In addition to ISO and EPCglobal, the Ubiquitous ID Centre in Japan has defined a generic identifier called “ucode”, which is not only intended to identify physical objects but also extends to places and digital information. Basic ucodes are 128 bits in length (but can be extended in multiples of 128 bits) and may embed other codes, such as international standard book numbers (ISBNs), IP addresses or E.164 telephone numbers (see Table 7.4). The ucode is simply a number that needs to be assigned a meaning in a relational database. Any individual or group can obtain ucodes from the Ubiquitous ID Center, which acts as the registration authority for these numbers.



ucode (basic 128bit length) structure (can be extended in multiples of 128 bits)

ucode field name and its length

Field Name	Length
Version	4 bit
Top Level Domain Code: TLDc (assigned by Ubiquitous ID Center)	16 bit
Class Code: cc	4 bit
Domain Code: dc	Multiple types
Identification Code: ic	Multiple types

Table 7.4. *Ucode format*

The ITU-T is working on systems for accessing multimedia information triggered by the tag-based identification of things. As part of this work a description of the various ID schemes that could be used for such identification is being produced. The Ubiquitous ID Center has submitted its ucode scheme so that ucode would be assigned an object identifier (OID) registered under the branch {joint-iso-itu-t(2) tag-based(27)} in compliance with ITU-T recommendation X.668 [ITU 08a].

The ISO/IEC unique ID scheme described earlier is assigned an OID under the branch {iso(1)} of the OID tree. This results in the ISO/IEC (including EPCglobal) and Ubiquitous ID Centre identifier schemes being assigned OID either under the {iso} branch (ISO and EPCglobal) or {joint-iso-itu-t} branch (Ubiquitous ID Centre) and allows the coexistence of the various identification schemes that have different registration authorities. For RFID tags, the OID and ID would be encoded as defined in ISO/IEC 15962.

NOTE: The term "object" in "object identifier" is not being used here as in other parts of this chapter to refer to a "thing" in general. It is instead used in accordance with the definition given in ISO/IEC 15961 as "a well-defined piece of information, definition, or specification which requires a name in order to identify its use in an instance of communication". An OID unambiguously identifies such an object. OIDs are hierarchically organized with the roots of the tree or top "arcs" indicating the organization that is responsible for the definition of the information. The top arcs represent ITU-T, ISO and joint ISO–ITU-T. They are given the numeric values 0, 1 and 2 respectively. The "tag-based" arc in the joint ISO–ITU-T tree is given the numeric value 27.

As mentioned earlier in this chapter, data associated with an object may be stored on a tag along with the ID if the tag has sufficient memory. But another possible means of finding information associated with an ID is to use an ID resolution mechanism, as described in section 7.4.4.

7.4.2. *Locating every thing: IPv6 addresses*

IP addresses provide a locator function and the means for routing traffic between end-systems on the Internet.

IP addresses are assigned by the Internet Assigned Numbers Authority to five Regional Internet Registries:

– APNIC (Asia Pacific Network Information Center) for the Asia-Pacific region;

– AfriNIC for Africa;

– ARIN (American Registry for Internet Numbers) for North America;

– LACNIC for Latin America and the Caribbean; and

– RIPE NCC (Réseaux IP Europeéns – Network Coordination Center) for Europe and the Middle East.

These registries then allocate addresses to Internet service providers who in turn provide them for use by their customers.

The IPv4 address space is limited and the pool of IPv4 addresses available for assignment is predicted to run dry in 2011 – 2012 (see Figure 7.4). This is occurring at a time when the number of devices that require an IP address, such as mobile "phones" and networked sensors, is rapidly increasing.

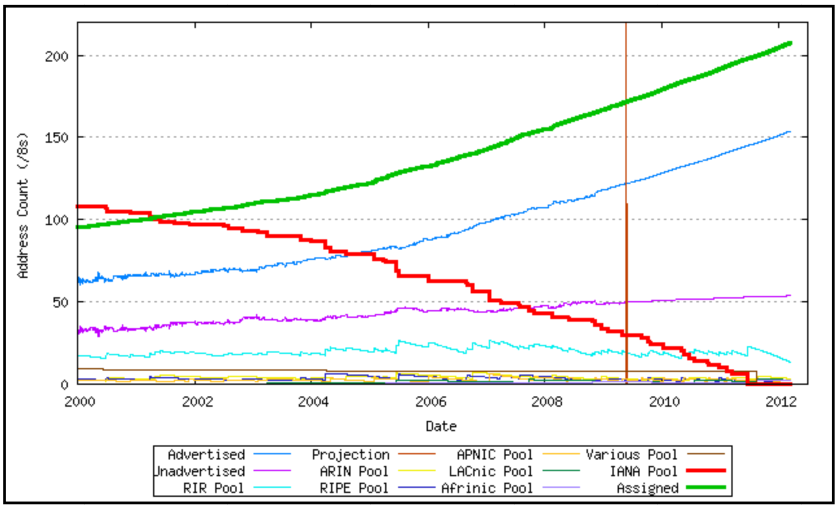


Figure 7.4. *IPv4 address exhaustion (for color version see source: http://www.potaroo.net/ispcol/2009-05/ipv4model.html)*

By extending the length of the address field in the IP header from 32 to 128 bits, IPv6 provides space for 340 billion billion billion billion unique IP addresses. As the number of IPv4 addresses is limited and there are likely to be an enormous number of ID terminals that require IP addresses, the deployment of IPv6 will be vital for the realization the IoT.

The use of IPv6 also has the advantage that the need for translating network addresses (network address translation or NAT) can be avoided. Translation between public IPv4 and private IPv4 addresses allows the creation of additional address space, as the private address domain can overlap the public domain. However, private addresses are not globally unique and thus they cannot be used to route traffic on the public Internet. This restricts certain applications because all communication sessions must be initiated from the private address side of the NAT so that the NAT can establish bindings to public addresses. Home network applications, in particular, can be restricted as sessions must be initiated from within the home network. This makes it difficult to access applications from the public Internet or to perform functions such as remote home consumer appliance diagnostics.

IPv6 is not compatible with IPv4 and so a smooth migration strategy has to be defined. Systems can be implemented that support both protocol versions – so-called dual-stack systems. IPv4 or IPv6 can be tunneled through the other protocol and translation between the address types can be performed. It does seem that IPv4 and IPv6 will have to coexist for a considerable time in the future.

As the IPv6 address space is so large, it is quite feasible to use IPv6 “addresses” as the identifiers of things. However, as the primary function of an IP address is to route traffic to a specific location, it has been argued that it is best to separate the identifier and location (or name and address) functions as the identifier of an object should not change as that object moves and connects to the network at a different location.

7.4.3. *Separating identifiers and locators in IP: the HIP*

From a network point of view, an IP address plays the role of a locator of a host and from an application point of view it plays the role of an identifier of a host for the duration of an association. The HIP provides a mechanism to separate these two roles. The HIP creates a new namespace of host IDs above the IP layer so that the IP address can be used solely as a locator.

The host identity architecture is described in RFC 4423 and the protocol is defined in RFC 5201. Host IDs are cryptographic public keys and can be used to authenticate identities or to provide anonymity. A hash of the full host identity, the 128-bit long host identity tag, is used in HIP payloads.

7.4.4. *Beyond the tag: multimedia information access*

A wide variety of services and applications can be envisaged, once it becomes possible to provide information associated with a tag ID in different forms (text, audio or image). For example, in a museum an ID on a tag attached to a painting could be used to find further information on the painting and the artist. In a grocery store, an ID on a food package could be used to check that the food is safe to eat and not a member of a sample that has been found to be contaminated in some way.

Other areas in which ID-triggered information access could be valuable include medicine/pharmaceuticals, agriculture, libraries, the retail trade, the tourist industry, logistics and supply chain management. ITU-T recommendation F.771 [ITU 08c] describes a number of services that could be based on the use of information associated with tagged objects and the requirements for these services.

A model for accessing the information associated with a tagged object is specified in ITU-T recommendation H.621 [ITU 08d] (see Figure 7.5). Within this model, a multimedia information discovery function can send the ID obtained from an ID tag reader to an ID resolution function, thereby obtaining a pointer (such as a uniform resource locator, or URL) to the appropriate multimedia information manager. As a result, it becomes possible to access the information associated with the tag ID. As the number of IDs is expected to be very large, the ID resolution function is likely to be distributed in a tree structure.

The ID resolution function could be based on use of the Internet DNS that usually provides the IP address corresponding to a URL. The object naming service described by EPCglobal uses DNS mechanisms to find information associated with electronic product codes.

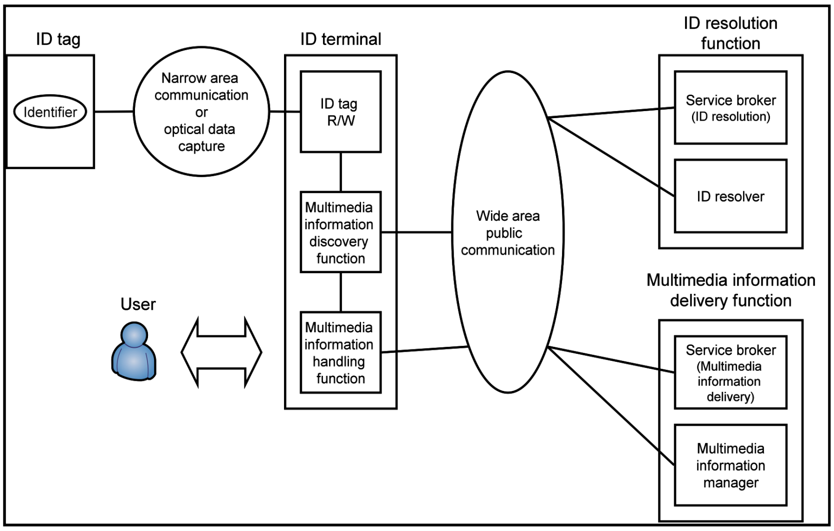

ID tag
Identifier
Narrow area communication or optical data capture
ID terminal
ID tag R/W
Multimedia information discovery function
Multimedia information handling function
User
Wide area public communication
ID resolution function
Service broker (ID resolution)
ID resolver
Multimedia information delivery function
Service broker (Multimedia information delivery)
Multimedia information manager

Figure 7.5. *Functional architecture for multimedia information access triggered by tag-based identification (ITU-T recommendation H.621) [ITU 08c]*

7.5. Promoting ubiquitous networking: any where, any when, any what

The IoT can be seen as a subset of a ubiquitous networking environment in which wireless and wired broadband networks provide all types of communication capabilities. It will meet a variety of person-to-person, person-to-machine and machine-to-machine communication requirements and in which sensors and RFID readers will increasingly be deployed.

Sensor networks have been used in industrial process control and would in many cases benefit from local or wide area network interconnection to perform control, maintenance and data collection operations. In addition, there are a large number of potential environmental monitoring applications for sensor networks that can increase security and also play a role in combating climate change. There is also growing convergence in the home where music, television, games, Internet access, telephony, alarm and home automation systems could feasibility be integrated and benefit from the use of wireless technology and wide-area network connectivity.

7.5.1. *Wireless sensor networks*

Wireless sensor networks consist of individual sensors monitoring environmental conditions, such as temperature, vibration, sound, pressure, motion or the presence of chemical pollutants. They can be employed in a great range of areas including industrial process monitoring and control, healthcare applications, traffic control and home automation. Each node in a sensor network consists of one or more sensors, a radio transceiver, a microprocessor and a power source. Sensor network components need to be of low cost and consume little power. Nodal resources in terms of memory, processor and power are severely constrained, for example to 32 K flash memory, 8-bit microprocessor and two AA batteries. Sensor networks consist of a great number of nodes, of which many may be “sleeping” at any time, which cannot be accessed with any predictability.

The IEEE has produced a specification of a wireless medium access control (MAC) and physical layer for low-rate WPANs suitable for use in wireless sensor networks (IEEE 802.15.4 [IEE 06]). A new MAC specification for this application was defined, as it was necessary to cut overheads in the data link layer protocol. The specification supports data rates of 20, 40, 100 and 250 Kbit/s over a range of up to 10 meters, and operates in the 868/915 MHz and 2,450 MHz bands. Some guidance on the regulatory conditions for use of these frequencies around the world is provided in Annex F of the IEEE 802.15.4 specification [IEE 06].

The IETF has addressed the issue of running the IP over IEEE 802.15.4 networks. The use of IP has the advantage of facilitating wide-area communication without having to employ protocol conversion gateways between sensor networks and the Internet. The IP model is often described as an hourglass in which IP forms the waist. Above IP are the protocols that meet the requirements of applications, such as web browsing and email, and below are the protocols that adapt the application data for transfer over specific media (see Figure 7.6). IP provides information transfer from end-system to end-system. IPv6 was chosen for running over WPANs, rather than the currently most widespread version of the IP, IPv4, as the number of IPv4 addresses is limited and there are likely to be an enormous number of sensors that require IP addresses.

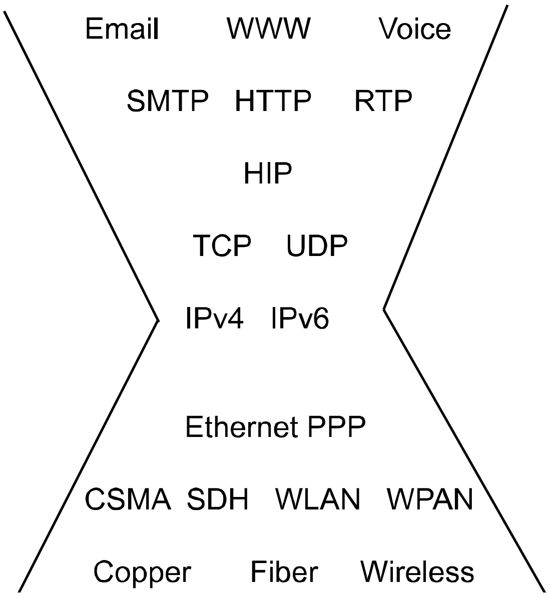


Figure 7.6. *The hourglass model of Internet protocols*

As IPv6 packets are much larger (minimum 1,280 octets) than the maximum payload of an IEEE 802.15.4 frame (102 octets), it is necessary to perform IPv6 header compression and to fragment IPv6 packets for transfer over 802.15.4 networks. The IPv6 header compression, fragmentation and reassembly procedures are specified in IETF RFC 4944 [MON 07].

The means by which wireless sensor networks are implemented provide a generic example of how any type of ID terminal, such as RFID readers and writers, could be networked. The characteristics of wireless sensor networks are such, however, that the routing protocols currently used on the Internet are not suitable for use in this environment. Therefore the IETF has undertaken work to optimize a routing protocol for use in sensor networks. The routing requirements for such "low-power and lossy networks" are discussed in RFC 5548 [DOH 09]. The mechanism defined by the Routing Over Low-power and Lossy networks (ROLL) working group of the IETF is intended to provide an end-to-end IP-based solution to communication over low-power WLAN, Bluetooth or PLC links in addition to IEEE 802.15.4 networks.

7.5.2. *Networking the home*

Sensors, actuators and RFID will be increasingly used in the home. Sensors will perform such functions as monitoring energy and water consumption, detecting motion or the presence of smoke, and may even be used to monitor the health of its inhabitants in the provision of telehomecare services [SRI 09]. Actuators will be used to control lighting, heating and other systems. Even today, sensors in the home are often connected to wide-area networks using telephone lines, mobile communications (telephony or SMS) or the Internet, in order to provide alarms to caregivers or the emergency services. There are also home automation systems that use both sensors and RFID, for instance for opening gates and garage doors.

In fact, the home provides a microcosm of a ubiquitous networking environment with telephones, personal computers, audiovisual entertainment, gaming consoles and security systems that are increasingly being connected to the Internet and used on-line. For example, digital television programming may be taken off air and viewed on a home computer, delivered over an IP network (IP TV) in a similar fashion to cable or satellite TV, or accessed over the Internet. There is tremendous potential in integrating many of these applications.

A number of standardization and industry organizations are addressing different bits of the home networking puzzle, such as: the Multimedia over Cable Alliance; Universal Plug and Play; Digital Living Networking Alliance; WiFi Alliance; IEEE; CableLabs;

ITU-T; ETSI; the Digital Video Broadcasting project; Broadband Forum; and HomePlug Alliance.

A range of wireless technologies are used within the home, such as WLAN (IEEE 802.11), Bluetooth, Zigbee and Z-Wave. There is also a potential for the adoption of PLC, in which the electricity cables within the home are used to provide a broadband home network. The ITU-T has produced a specification for generic home network transport architecture in ITU-T recommendation G.9970 [ITU 08d]. A physical layer specification for a transceiver capable of operating at rates of up to 1 Gbit/s over telephone wiring, coaxial cable or power line wiring is provided in ITU-T recommendation G.9960 [ITU 09]. In this architecture, G.9960 domains are interconnected with each other and with other "alien" domains based on different technologies, such Ethernet and WLAN, with inter-domain bridges.

7.5.3. *Next generation networks*

The ITU-T and other standardization organizations, such as ETSI and the Alliance for Telecommunications Industry Solutions, have developed the concept of next generation networks in which fixed and mobile voice, data and video services converge on an IP-based network infrastructure. This architecture has been extended in ITU-T recommendation Y.2002 [ITU 05] in order to accommodate ubiquitous networking. The aim is to provide seamless communication capabilities between people, objects and persons, and objects irrespective of location. Figure 7.7 shows the next generation network model enhanced to support the interconnection of things.

Next generation networks is a system-level specification that makes use of the components produced not only by the ITU-T but by many other organizations, such as the IEEE and IETF. The standardization of ubiquitous networking will involve a number of organizations that define various system components as well as organizations that will paint a broader conceptual canvas.

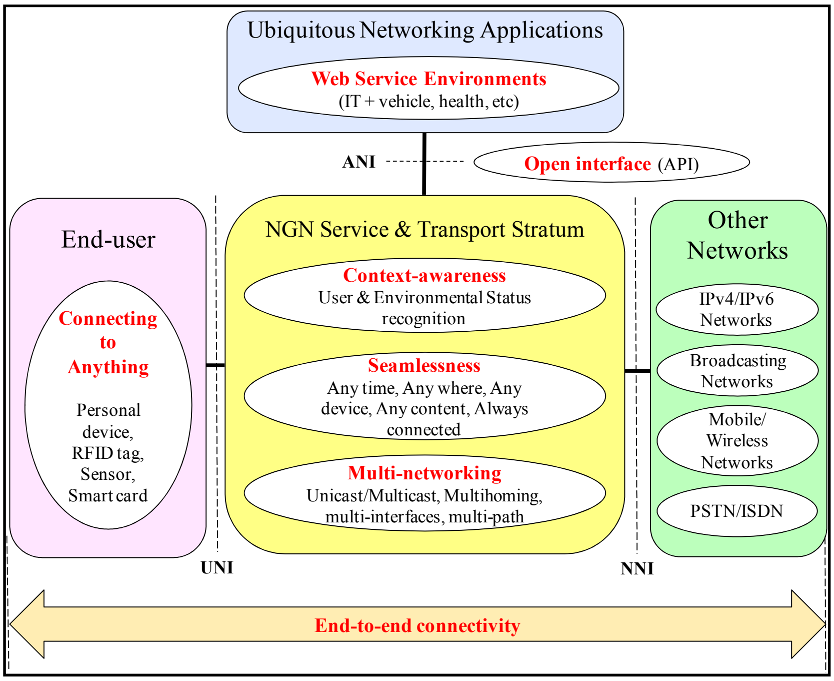

Ubiquitous Networking Applications
Web Service Environments
(IT + vehicle, health, etc)
ANI
Open interface (API)
End-user
Connecting to Anything
Personal device, RFID tag, Sensor, Smart card
NGN Service & Transport Stratum
Context-awareness
User & Environmental Status recognition
Seamlessness
Any time, Any where, Any device, Any content, Always connected
Multi-networking
Unicast/Multicast, Multihoming, multi-interfaces, multi-path
Other Networks
IPv4/IPv6 Networks
Broadcasting Networks
Mobile/ Wireless Networks
PSTN/ISDN
UNI
NNI
End-to-end connectivity

Figure 7.7. *High level model of ubiquitous networking in next generation networks (ANI: application network interface; UNI: user–network interface; NNI: network–network interface) [ITU 05]*

The Internet is of course constantly evolving and the future Internet may be based on a different architecture from the Internet of today. However, in either case it is widely acknowledged that the future Internet will have to accommodate not only connectivity between personal devices, computers and networks but also between everyday objects.

7.6. Safeguarding data and consumer privacy

The widespread use of RFID and the deployment of ubiquitous sensor networks will of course lead to an enormous amount of data being captured by commercial and state enterprises. This presents the risk of associating data, including location information, with a person, and concerns have been raised about the appropriate use and possible misuse of such data [SRI 07]. Privacy in itself is by no means a new issue and the right to privacy is recognized in a number of international conventions. Article 12 of the United Nations Declaration of Human Rights states that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Similarly the European Convention for the Protection of Human Rights and Fundamental Freedoms states that:

> "Everyone has the right to respect for his private and family life, his home and his correspondence."

The EU has adopted directives on data protection (Directive 95/46/EC [EUP 95]) and the protection of privacy in telecommunications (Directive 2002/58/EC [EUP 02]) that are intended to form the basis of harmonized national laws addressing privacy within EU Member States. The directive on data protection from 1995 follows the principle that it is necessary for a citizen to consent to providing information in full knowledge of the use to which this information will be put. It states that "sensitive data" relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual preference should not be processed. These principles apply to the Internet and have been interpreted rigorously in some countries. In Sweden for example, the personal data law originally prohibited any data on a person being released on web pages (with the exception of journalism, art and literature) without the explicit consent of that person. This included not just information, such as a person's name, identity number, address or photograph, but also any information that could be used to identify an individual, such as their occupation or town of residence. This law has been revised and relaxed to allow reference to a person in unstructured material as long as it is not offensive and does not violate that person's integrity. However, this indicates that there is considerable leeway in the interpretation of the EU Directive and that some of the changes that are being made to the regulation of communications are being made due to the difficulty of enforcing the regulations rather than due to changes in the principles to be applied. The enormous volumes of data that will be collected in different legal jurisdictions in the future will stress the system of imposition of existing data protection legislation.

The EU directive on data protection in principle forbids the sending of personal data to other countries that do not ensure adequate protection of privacy. Publishing data on the Internet (as long as the law is followed), however, is not considered to be sending information to another country, even though access is global.

The Directive "concerning the processing of personal data and the protection of privacy in the telecommunications sector" [EUP 02] requires Member States to guarantee the confidentiality of communications by adopting national regulations to make any unauthorized listening, tapping, storage or other kinds of interception or surveillance illegal. Telephone callers must be given the option of not having their identity revealed if the calling-line identification service is offered. Conversely, subscribers to this service must have the opportunity to reject incoming calls from individuals who have blocked their calling-line identification. Individuals are entitled to be omitted from printed or electronic telecommunication directories.

These EU directives do not apply when public security, defense or criminal law enforcement are taken into consideration, however. A state may be able to get away with violating the principles of personal data protection on the grounds of national security. There is clearly a trade-off between the wish to maintain personal integrity with the need to secure our environment, avoid being a victim of crime and apprehend criminals. In most countries it is only lawfully permissible to intercept communication by court order on suspicion of serious crime. Countries are, however, sometimes tempted to relax these restrictions on the basis of potential threats to national security.

The European Commission published a recommendation on the impacts of RFID on privacy and data protection in May 2009 [COM

09]. This recommendation recognizes the applicability of the directives described above concerning the protection of personal data (Directive 95/46/EC) and the processing of personal data (Directive 2002/58/EC) to the use of RFID applications that process personal information. It goes on to recommend that privacy and data protection impact assessments be performed for RFID applications and that operators should publish information associated with the use of these applications. This published information should include a statement of what information is to be processed, whether the location is monitored, and the privacy and data protection risks. For retail applications, it is recommended that point-of-sale tags be removed or deactivated unless the consumer gives explicit consent to keep the tags operational.

7.7. Conclusions

The IoT represents a future vision of ubiquitous connectivity. Connecting sensor networks and RFID readers/writers to the Internet greatly increases the potential range of applications and the flexibility, usefulness and scope of the network. Although there is much ongoing standardization activity in the various aspects of the IoT, the convergence of previously separate industry sectors has led to some overlap and confusion. This situation may well present an important opportunity for international standardization organizations to play a greater role in providing solutions for end-to-end communications in an IP-based IoT.

7.8. Bibliography

[BAS 02] BASSHAM L., POLK W., HOUSLEY R., *Request for Comments 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, 2002.

[CER 08] CE RFID, *Coordinating European Efforts for Promoting the European RFID Value Chain – Report on RFID Standards and Radio Regulations*, CE RFID, 2008.

[COM 09] COMMISSION OF THE EUROPEAN COMMUNITIES, *Commission Recommendation of 12.5.2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-frequency Identification*, CEC, 2009. (Available at: http://www.ifap.ru/ofdocs/eu/eu0001.pdf, accessed February 23, 2010.)

[DOH 09] DOHLER M., WATTEYNE T., WINTER T., BARTHEL D., *IETF Request for Comments 5548: Routing requirements for urban low-power and lossy networks*, IETF, 2009. (Available at: http://tools.ietf.org/html/rfc5548, accessed February 23, 2010.)

[EPC 08] EPCGLOBAL, *Tag Data Standards Version 1.4*, EPCglobal, June 2008.

[EUP 95] EU PARLIAMENT, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*. EU Parliament, 1995. (Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, accessed February 23, 2010.)

[EUP 02] EU PARLIAMENT, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* (Directive on privacy and electronic communications). EU Parliament, 2002. (Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF, accessed February 23, 2010.)

[HOU 02] HOUSLEY R., *Request for Comments 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, 2002. (Available at: http://www.ietf.org/rfc/rfc3280.txt, accessed February 23, 2010.)

[IEE 06] IEEE, *IEEE 802.15.4 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE, 2006.

[ITU 05] ITU-T, *ITU-T Recommendation Y.2002: Overview of Ubiquitous Networking and its Support in NGN*, ITU-T, 2005.

[ITU 08] ITU-T, *ITU-T Recommendation Y.2213: NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*, ITU, 2008.

[ITU 08a] ITU-T, *ITU-T Recommendation X.668/ISO/IEC 9834-9: OID Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*, ISO/IEC, 2008.

[ITU 08b] ITU-T, *ITU-T Recommendation X.509: The Directory: Public-key and attribute certificate frameworks*, ITU, 2008.

[ITU 08c] ITU-T, *ITU-T Recommendation F.771: Service Description and Requirements for Multimedia Information Access Triggered by Tag-based Identification*, ITU-T, 2008.

[ITU 08d] ITU-T, *ITU-T Recommendation H.621: Architecture of a System for Multimedia Information Access Triggered by Tag-based Identification*, ITU-T, 2008. (Available at: http://itu.int/rec/T-REC-H.621, accessed February 23, 2010.)

[ITU 08e] ITU-T, *ITU-T Recommendation G.9970: Generic Home Network Transport Architecture,* ITU-T, 2008.

[ITU 09] ITU-T, *ITU-T Recommendation G.9960: Unified High-speed Wire-line Based Home Network Transceivers – Foundation*, ITU-T, 2009.

[MON 07] MONTENEGRO G., *Request for Comments 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, IETF, 2007. (Available at: http://www.rfc-archive.org/getrfc.php?rfc=4944, accessed February 23, 2010.)

[SRI 05] SRIVASTAVA L., *ITU Internet Reports: The Internet of Things*, ITU, 2005. (Available at www.itu.int/internetofthings, accessed February 23, 2010.)

[SRI 07] SRIVASTAVA L., “RFID: ubiquity for humanity”, *INFO*, vol. 9, no. 1, p. 4-14, 2007.

[SRI 09] SRIVASTAVA L., *Wireless Independent Living for a Greying Population*, River Publishers, 2009.