I. Introduction

A. Internet of Things: Notion

The Internet of Things (IoT)\(^1\) is an emerging global Internet-based information architecture facilitating the exchange of goods and services.\(^2\) The IoT has the purpose of providing an IT-infrastructure facilitating the exchange of “things” in a secure and reliable manner, i.e. its function is to overcome the gap between objects in the physical world and their representation in information systems.\(^3\) The IoT will serve to increase transparency and enhance the efficiency of global supply chain networks.\(^4\)

HALLER/KARNOUSKOS/SCHROTH define the IoT as “a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these ‘smart objects’ over the Internet, query their state and any information associated with them, taking into account security and privacy issues.”\(^5\)

Extending the initial application scope, the IoT might also serve as backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and retrieve information from the Internet to facilitate their adaptive functionality.\(^6\)

Through the IoT, everyday objects (such as cars, refrigerators, umbrellas, etc. as well as more advanced, computer and information services) will be able to interact and communicate.\(^7\) „Things“ do not have to be products of higher technology – any one of the around 50,000 billion objects existing on earth can be introduced in the IoT.\(^8\)

Many good examples have been provided. They include cars warning other cars of traffic jams, a cell phone reminding a person when it was last left next to the

---

1. The term “IoT” has been “invented” by KEVIN ASHTON in a presentation in 1998 (see SANTUCCI, 2).
2. For a general overview see WEBER, Legal Environment, 522–523.
3. HALLER/KARNOUSKOS/SCHROTH, 15.
4. FABIAN, 1.
5. HALLER/KARNOUSKOS/SCHROTH, 15.
6. See in general FABIAN, 1.
7. PREUVENEERS/BERBERS, 288.
keys, a wastebin inquiring its contents about their recyclability, or a medicine cabinet checking the storage life of the medications in it.\textsuperscript{9}

The question has been raised why the IoT does not already exist, considering that the Internet, mobile devices and data carriers exist for quite some time. The answer thereto lies in the fact that persons do not communicate with the tools being already available to their possible extent. Barcodes, GPS, RFID etc. are closed-loop systems that are not yet bound together, but that are systems standing alone.\textsuperscript{10}

\section*{B. Technicity of the Internet of Things}

The IoT is a very complex platform for the connection of things based on objects being tagged for their identification, but also sensors,\textsuperscript{11} actuating elements and other technologies. In this book, the focus is put on the identification of things, which is the most important (while not the only) aspect\textsuperscript{12} of the IoT as far as the involvement of businesses is concerned.

\subsection*{1. Technical Elements}

\subsection*{1.1 Radio-Frequency Identification (RFID)}

\subsubsection*{a) RFID in General}

From a technical point of view, the architecture of the IoT is based on data communication tools, primarily RFID-tagged items (Radio-Frequency Identification). RFID is a technology used to identify, track and locate assets. The RFID technique has been known since at least the Second World War\textsuperscript{13} and has, up to now, been used primarily in new civil application fields.\textsuperscript{14} This technology is gradually replacing the existing bar-codes, not requiring any contact with objects.\textsuperscript{15} As the number of tags produced increases, it is expected their price will decrease.

\begin{itemize}
\item \textsuperscript{9} Mattern, Ubiquitous Computing, 17.
\item \textsuperscript{10} Oral statement of Bert Moore, AIM, Director, Communications and Media Relations at the CASAGRAS Conference in London on October 6–7, 2009.
\item \textsuperscript{11} The use of sensors in the IoT is discussed in chapter V.D. with regard to environmental concerns.
\item \textsuperscript{12} Other aspects are the autonomous operation of objects or the communication between things.
\item \textsuperscript{13} Shih/Sun/Lin, 973.
\item \textsuperscript{14} Such as animal or human identification, anti-counterfeiting, access control and payment; Fabian, 1–2.
\item \textsuperscript{15} Usually, RFID tags can be read from about 20 meters away.
\end{itemize}
RFID is a technology for the automatic identification of objects through wireless radio waves. In general, RFID systems consist of two components: a transponder (RFID tag or chip), attached to the object and serving as data carrier, and a registration device reading the data in the transponder. RFID tags can either be passive (not possessing a battery), active (with an integrated battery including an active transmitter and receiver), or semi-passive (with battery but no transmitter). While RFID seems to be the technology referred to most often when considering the architecture of the IoT, one has to keep in mind that it is not the only technology available. Other tools such as Near Field Communication Technologies, wireless sensors, 2D barcodes or inks with nano-particles could also be used instead of RFID. The employment of other technologies than RFID for the IoT has also been emphasized in responses to the European Commission regarding a working document on the challenges of the IoT.

16 Weber/Willi, 245–246; Mattern, Technische Basis, 55–57; Arioli/Thalmann, 550; see also Kim/Choi/Lee/Lee, 364; Müller/Handy, 3.

17 For RFID tags see Benghozi/Bureau/Massit-Folléa, 95; Hawrylak/Mickle/Cain; Juels, 382.

18 From a technical point of view, Near Field Communication Technologies could be classified as a kind of RFID because they are partly based on the same standards. However, from a political point of view, in particular representatives of Near Field Communication Technologies are opposed to that view in order to prevent the partly negative connotations of RFID with regard to privacy to be transferred to Near Field Communication Technologies.

19 Amcham EU, 4; EPCglobal, Response to the EU Commission Staff Working Document, 2–4; see also Mattern, Techische Basis, 49–50.

20 Amcham EU, 4; EPCglobal, Response to the EU Commission Staff Working Document, 2–4.
The basic RFID Device and Process Architecture is illustrated in the following graph:\(^{21}\)

---

**b) Global RFID Interoperability Forum for Standards (GRIFS)**

The Global RFID Interoperability Forum for Standards (GRIFS) is an EU project lasting from January 2008 to December 2009. The GRIFS is engaged in RFID standardization for physical items. It documents the development of standards, establishes liaisons of existing standards and, most importantly, provides for a forum for standards (this forum should continue even after the end of the project in December 2009).\(^{22}\)

In May 2009, a Memorandum of Understanding (MoU) was effectively launched between key stakeholders (IEC, ISO, ITU and UNECE). This MoU has been established for the facilitation of standards. It does not constitute a change to the existing standards development process and decisions have to be taken by consensus.\(^{23}\)

---

\(^{21}\) Graph taken over from a presentation of Paul Chartier at the CASAGRAS Conference in London on October 6–7, 2009.


1.2 Electronic Product Code (EPC)

The most popular industry proposal for the new IT-infrastructure of the IoT is based on an Electronic Product Code (EPC), introduced by EPCglobal and GS1. EPCglobal is a consortium focused on developing and establishing global standards for RFID, EPC, and the EPCglobal Network.

The EPC is made up of a header, which determines the kind of EPC and how to interpret the other parts of the EPC. Most often, the actual EPC consists of an EPC Manager Number, an Object Class Code and a Serial Number (or a subset thereof). EPCs are unique numbers encoded in an inexpensive RFID tag. EPC tags can store up to 256 bits. Physical objects consequently carry these RFID tags with the EPCs.

While EPCs allow for users to verify the integrity of the ordered object, a “tracking and tracing” of things on their way from the sender to the recipient is not possible. Such result could only be achieved by the sender delivering a file to the recipient including all information on the delivery before sending off the object.

The EPC Network allows many parties to register any information for the objects they are concerned with, thereby creating a process to openly exchange product-related information. This information can consist of EPC-encoded sensor data, historical data or business context. Furthermore, the infrastructure is able to offer and query EPC Information Services (EPCIS) both locally and remotely to subscribers.

---

24 EPCglobal is a joint venture of GS1 U.S. (formerly Uniform Code Council) and GS1 (formerly EAN International).
26 Fabian, 30.
28 EPCglobal, Object Naming Service (ONS) Version 1.0.1, Appendix A.
29 For the numbers of EPCs that can be generated without duplicates see Fabian, 94–96.
30 EPCglobal, Object Naming Service (ONS) Version 1.0.1, para 4.
31 Dalal, 487.
32 Fabian/Günther/Spiekermann, 1.
33 For security and privacy of the IoT see also below III.
34 Koh/Staake, 17.
35 Fabian/Günther/Spiekermann, 1.
36 Fabian/Günther, Security Challenges, 122.
37 See Fabian, 30–31; to the details of the service orientation and the context-aware computing see Preuveneers/Berbers, 296–299.
1.3 Object Naming Service (ONS)

a) ONS in General

The Object Naming Service (ONS) is a service containing the network addresses of services. Each service available on the ONS contains data about EPCs. Instead of saving all the information on an RFID tag, a supply of the information by distributed servers on the Internet is achievable through linking and cross-linking with the help of the ONS.\(^{38}\) The ONS does not contain actual data about EPCs, but can return a list of network accessible endpoints that pertain to the EPC in question.\(^{39}\) The first ONS was introduced by the (private) company VeriSign, the first European ONS was established by France in 2009.

The ONS is authoritative (linking metadata and services) in the sense that the entity having – centralized – change control over the information about the EPC is the same entity that assigned the EPC to the concerned item.\(^{40}\)

Using the ONS, the architecture can also serve as a backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and receive information from the Internet to facilitate their adaptive functionality.\(^{41}\) The practical operation of the central ONS root has been outsourced to VeriSign, a provider of Internet infrastructure services.

b) ONS and DNS Heritage

The ONS is based on the well-known Domain Name System (DNS), i.e. the DNS-based ONS as hierarchical tree-like architecture\(^{42}\) locates the information sources relevant for a given object. Technically, in order to use the DNS to find information about an item, the item’s EPC must be converted into a format that the DNS can understand, which is the typical, “dot” delimited, left to right form of all domain names.\(^{43}\) In practice, the EPC in the binary form is forwarded to a middleware system. This system converts the EPC to its Uniform Resource Identifier (URI) in order to locate the relevant EPCIS for the searched product. The ONS finally translates the URI into a domain name according a well-defined procedure.\(^{44}\)

\(^{38}\) Fabian, 33.

\(^{39}\) Weber, Legal Environment, 523.

\(^{40}\) EPCglobal, Object Naming Service (ONS) Version 1.0.1, para 4.2.

\(^{41}\) Fabian, 1.

\(^{42}\) Fabian, 33.

\(^{43}\) EPCglobal, Object Naming Service (ONS) Version 1.0.1, para 5.2.

\(^{44}\) Fabian/Günter/Spiekermann, 1.
There are two options that need to be explored. Firstly, the IoT could have an exclusive generic Top-Level Domain (gTLD), e.g. the address .iot. In the Internet, seven gTLDs were created in the beginning: .com for commercial activities, .org for organizations, and .net for networks as three universal top-level domains; .gov for governments, .edu for universities, and .mil for military as three gTLDs for use in the US only, and .int for intergovernmental treaty organizations. \(^{45}\) In the following, the list of gTLDs was enlarged. In particular, each country was given its own name according to the so-called country code Top-Level Domain (ccTLD) such as .de for Germany, .ch for Switzerland, .uk for the United Kingdom and .us for the US. \(^{46}\) On November 15, 2000, the ICANN passed a resolution to introduce seven new gTLDs. \(^{47}\) Since then, six more gTLDs have been introduced. \(^{48}\) However, these extensions have lead to confusion regarding the gTLDs themselves as well as their corresponding dispute resolution policies. \(^{49}\)

With regard to the IoT, commercial pressure against the introduction of an .iot address may emerge from the business sector, which wants to retain e.g. an address .com.

Furthermore, gTLDs relating to a sector and for sector-specific identifiers, resolvers and discovery services could be employed (e.g. the address .aero for organizations in the air transportation sector). \(^{50}\)

Since EPC is encoded into a syntactically correct domain name and then used within the existing DNS infrastructure, the ONS can be considered as subset of the DNS. \(^{51}\) For this reason, however, the ONS will also inherit all of the well-documented DNS weaknesses, such as the limited redundancy in practical implementations and the creation of single points of failure. \(^{52}\)

---

\(^{45}\) For the naming system see Bygrave/Schiavetta/Thunem/Lange/Phillips.

\(^{46}\) Weber, ICANN, 604; for ccTLD governance see Bygrave/Schiavetta/Thunem/Lange/Phillips, 156–159.

\(^{47}\) The addresses .aero for the air-transport industry, .biz for business, .coop for cooperatives, .info for unrestricted use, .museum for museums, .name for registration by individuals and .pro for registration by accountants, lawyers, physicians and the like.

\(^{48}\) The addresses .asia for the Asian community, .cat for the Catalan linguistics and cultural community, .jobs for the international community of human resource managers, .mobi for the mobile content providers and users community, .tel for e-communications address/numbers information and .travel for the travel and tourism community; for an overview of all current gTLDs see Bygrave/Schiavetta/Thunem/Lange/Phillips, 149.

\(^{49}\) Kaufman, 4–6.

\(^{50}\) CASAGRAS, 41.

\(^{51}\) For similarities and differences of the ONS and the DNS see Weber, Legal Environment, 523.

\(^{52}\) For more details see Weber, Legal Environment, 523; Fabian/Günter, Distributed ONS, 1224.
The ONS and the DNS have the following similarities:

- **Structure**: Based on the distributed DNS-tree, both the ONS and the DNS are grounded on the same database structure.
- **Service architecture**: Both the ONS and DNS use the architectural user-server model and the same Internet communication protocols.

The following differences are given between the ONS and the DNS:

- **Standardization processes and bodies**: The ONS uses the standards development process by EPCglobal, a user driven standards process for the development of technical standards, whereas DNS applies the RFC (Requests for Comments) series, a standardization process developed and published by the Internet Engineering Task Force (IETF).
- **Naming schemes**: The domain names in the DNS usually consist of two or more alphanumeric parts (labels) with only a few technical limits, e.g. each label can contain up to 63 octets, but the whole domain name may not exceed 255 octets. The ONS uses the Tag Data Standard, a deterministic choice based on the EPC structure.\(^{53}\)
- **Use models**: The DNS is based on an extensible and multi-purpose Internet-based public infrastructure; the ONS uses a private infrastructure that is specific to RFID-related business activities/partners.

c) **Introduction of Multiple DNS Classes**

Muguet proposes to use various DNS classes, each being an autonomous namespace with its own root servers and its own governance.\(^{54}\) This approach allows for decentralized security systems related to each DNS class, offering participants commercial and political independence.\(^{55}\)

The operation of the IoT could go through several classes in order to present an independent and interoperable IoT. Classes may be established according to the International Classification of Trademarks\(^{56}\) encompassing 45 classes. This Classification was introduced in the Internet because it was deemed necessary to establish harmonized rules governing domain names. The Nice Classification is based upon the respective multilateral treaty, distinguishing between a broad variety of goods and services. Therefore, the classes are suitable to serve as code

---

\(^{53}\) Fabian, 37.

\(^{54}\) Muguet, 3.

\(^{55}\) Muguet, 4.

\(^{56}\) According to the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks of June 15, 1957.
rules.\textsuperscript{57} In the IoT, each label would have a domain name in a DNS class related to its trademark class. Such an approach would not only provide for decentralized power, but also represent a tool against counterfeiting.\textsuperscript{58}

While MUGUET’s proposal allows for decentralized power as well as potentially increased security and product verification, the classification of objects into various classes could, in practice, pose a major logistical problem and require extensive resources. The introduction of classes increases the complexity of the IoT and therefore makes it more exposed to failures. Furthermore, the proposal still operates with only one root, which does not alleviate the problem of a “single point of failure”.

1.4 EPC Discovery Service

The EPC Discovery Services are another locator of EPC-related data. Unlike ONS, however, an EPC Discovery Services may not only contain pointers to the entity that originally assigned the EPC code, but any entity. Thus, EPC Discovery Services are not universally authoritative for the data they have about an EPC. Nevertheless, it is anticipated that various EPC Discovery-Services, in a competitive relationship, will be established, some of them with a scope limited e.g. geographically or according to objects.\textsuperscript{59}

1.5 Graphic Overview

The finding of information using an RFID tagged object can – in very simple terms – be demonstrated in a graph:

\textsuperscript{57} Weber, More harmonization in the DNS, 454–455.
\textsuperscript{58} MUGUET, 5.
\textsuperscript{59} EPCglobal, Object Naming Service (ONS) Version 1.0.1, para 4.2.
2. Decentralized and Interoperable Internet of Things

2.1 Introduction

As the IoT is based on the Internet, the framework of the Internet shall be examined and serve as a basis of understanding for the establishment of the IoT. The currently used Internet model, maintained by the Internet Corporation of Assigned Names and Numbers (ICANN), a US-domiciled private entity, is hierarchically structured as a single authoritative root with complete interoperability based on common standards. In this context, the question whether a single- or a multi-root architecture would be preferable merits further elaboration.

The fact that the concentration of the de jure control over the root name space is in the hands of a single non-governmental entity is subject to constant criticism, since, for example, a unique root does not meet geopolitical concerns. Therefore, structural changes are of fundamental importance. Furthermore, a unipolar ONS could be controlled or blocked by a single country or a group of countries based on political or economic reasons. Even if no single server would contain the complete ONS directory and if each server would be responsible for one or more domains but no two servers for the same domain, a fully centralized root system does not seem to be appropriate.

Therefore, an independently managed decentralized multiple-root system being interoperable and covering data in a distributed way needs to be developed for the future IoT, although multiple identifier authorities imply a significant and sustained effort of global cooperation. The need therefore can be slightly limited through the introduction of common standards that apply to all identifier authorities. Nevertheless, continuous dialogue between all authorities regarding current events and possible improvements of the system is indispensable to preserve the globality and uniformity of the IoT.

Nevertheless, the implementation of a multi-root system does not exclude that a close cooperation between EPCglobal/GS1 and the domain name registries is applied; by sharing experiences and by putting together combined efforts it should be possible to realize better and more stable solutions. Furthermore, a multipolar
ONS (MONS) allows for the distribution of control between the participating parties.\textsuperscript{65}

2.2 Replicated Multipolar ONS

One possible scenario of replicated MONS consists of an ONS root running on six locally distributed servers. These servers would all be operated by the company VeriSign; this concept herewith differs from the existing DNS where root name servers are operated by various entities.

A second setting would be to replicate the ONS root between various independent servers. These servers would have to synchronize the instances of the root ONS, which could be achieved by EPCglobal distributing a master copy. In order to delimit the number of incoming requests, each server would be responsible to cover a certain area of the Internet Protocol (IP) topology and respond only to requests originating from that area. These individual servers can consequently provide their services in parallel to the root ONS operated by VeriSign.

Both scenarios of the multiple replicated ONS would enhance availability. However, the establishment of an according structure might not be globally accessible due to a high load of data and result in an unstructured patchwork of areas with ONS root redundancy.\textsuperscript{66}

2.3 Regional Multipolar ONS

In particular European scholars call for a root system on a regional basis, representing the whole of the Internet community within the organizational structures. Correspondingly, democratic legitimacy\textsuperscript{67} is only considered as being achievable through various root systems.\textsuperscript{68}

Evdokimov/Fabian/Günther have addressed the possibility of regional MONS. Regional MONS would allow reducing the size of the root zone file and the frequency of its updates. The authoritative region for membership could be determined by a company’s registration address or the address of the regional GS1 department that issued the company prefix. While regional MONS are a promising approach, the delegation of queries from one regional ONS to another constitutes an additional resolution step. This step asks for an extension of the existing EPC scheme. To encounter this problem, the first three digits of the company pre-

\textsuperscript{65} Evdokimov/Fabian/Günther, 7.

\textsuperscript{66} Evdokimov/Fabian/Günther, 7–9.

\textsuperscript{67} See below IV.B.

\textsuperscript{68} Benhamou, Governance Perspective, 269.
fix that identify the country could be used, or a regional prefix would need to be established. As a region’s MONS root will be perceived as the root of the whole hierarchy by a resolver, the structure of regional MONS can be called a relative hierarchy, allowing for the implementation of the regional MONS within the DNS. In addition, this system has the advantage that each region could determine its own resolution architectures for subsystems below the root zone, thereby allowing for a modularity of the ONS.69

The establishment of regional roots has also been proposed by the French government to the EU in 2008. The French government wanted the EU to establish its own root for the Internet of Things, as an alternative to the ONS created by EPC-global. The technology of the proposed root would not differentiate from the ONS – both systems rely on the DNS – but would have a different registry and use the top level domain “.eu” instead of “.com”. In the opinion of the French government, the Internet of the future asks for areas administered by regions (and not globally).70

2.4 Referral Systems

Afilias, a large provider of global domain name registry services supporting over 14 million domains across 15 top level domains71, published a White Paper on “Finding your Way in the Internet of Things” in September 2008. Afilias therein submits an architectural approach to ONS for creating a decentralized and interoperable IoT root system focusing on five main issues,72 namely identifier collisions, backward compatibility, unilateral control authority, assurance of practicality, openness to competition in the provision of services and setting of priorities towards trust/security.73

In practice, identifier authorities could set up referral systems under any top level domain, thereby establishing ONS operations. To satisfy the requirement of interoperability, these identifier authorities would need to cooperate and coordinate the look up of their identifiers in global supply chains.74

In the EPC that has been transformed into a DNS format, a “dot” constitutes a delegation step, and thus a pointer to a subsequent zone.75 Accordingly, the Inter-

---

69 Evdokimov/Fabian/Günthter, 9–14.
71 See http://www.afilias.info/.
72 Afilias White Paper, 2.
73 Weber, Legal Environment, 525.
74 Afilias White Paper, 5.
75 EPCglobal, Object Naming Service (ONS) Version 1.0.1, para 6.1.
net Service Provider (ISP) would look up the DNS service at the root servers for one “dot” part and get referred to the next DNS service from there. This process is repeated until the answer is a referral to an electronic system such as EPCIS or an EPC Discovery Service which can provide the requested information.\textsuperscript{76}

Using such an example of supply chains, Afilias proposes an ONS model with local control and global interoperability, notwithstanding the fact that the IoT will be broader than just supply chain elements thereof. Different DNS operators are employed at each level of DNS resolution. In addition, the traffic volume can be disbursed at the lower, distributed levels of DNS delegation, i.e. the multitude of root servers already existing in the DNS will be used to search for information through an EPC and the ONS.\textsuperscript{77}

\section*{2.5 Assessment of the Various Approaches}

All of the three approaches to a multipolar ONS mentioned above\textsuperscript{78} aim at diversifying the control over the IoT and distributing the volume of data. A split-up according to regions is the solution most often asked for by stakeholders and the doctrine. However, the suggestion made by Afilias seems more promising.

While a central root continues to exist at the top level, control is referred to lower instances at a local level. Herewith, global interoperability can be assured, but referrals are still able to administrate the IoT within their own level (of course having to follow the principles set by the central root). Such a distribution of control goes in hand with the disbursement of traffic volume, without impairing global accessibility or an unclear fragmentation of attribution of queries. Furthermore, this system is compatible with the existing DNS and can be built on it.

An additional point in the decision on a particular system is the length of the information path. Short information paths increase the robustness of the system and thereby increase security.\textsuperscript{79} A central root with referrals to instances at lower levels do not create excessively long information paths for users and are therefore suitable for the creation of a safe IoT.

\textsuperscript{76} For examples see Afilias White Paper, 5–13.
\textsuperscript{77} Afilias White Paper, 14–15.
\textsuperscript{78} See above I.B.2.1–2.4.
\textsuperscript{79} For the security of the IoT see also below III.
Internet of Things
Legal Perspectives
Weber, R.H.; Weber, R.
2010, XXIV, 135 p., Hardcover
ISBN: 978-3-642-11709-1